WHITEPAPER

Ransomware

Prevención y Respuesta a Incidentes

Evandro César Vilas Boas
Guilherme Pedro Aquino

CxSC Telecom
Centro de Segurança Cibernética

Inatel

Índice

Introducción

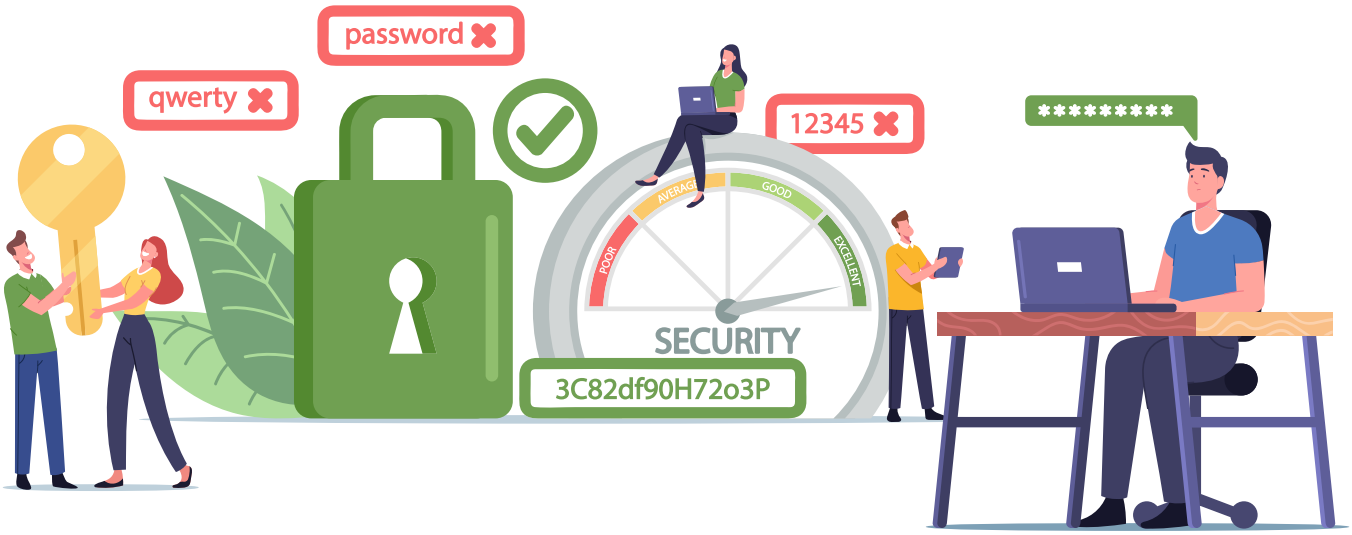
El avance tecnológico de los medios digitales ha permitido ofrecer soluciones asequibles a la población en general, lo que se ha traducido en un aumento considerable del número de personas conectadas. En consecuencia, las organizaciones con fines de lucro comenzaron a explorar los canales de comunicación digital como una forma de redefinir el negocio y expandir su base de clientes. Organizaciones gubernamentales e instituciones sin fines de lucro también han utilizado este estándar de comunicación para digitalizar procesos y facilitar el acceso a los servicios. Algunos sectores de la economía se han beneficiado de la expansión de la conectividad para introducir soluciones disruptivas y totalmente digitalizadas como las fintechs Nubank, Banco Inter y varias otras.

La migración de procesos o actividades rutinarias del entorno físico al digital, no solo transformó los servicios y negocios, sino que también motivó la propagación de delitos cibernéticos.

En este contexto, existe un mayor flujo digital de información sensible al negocio y datos personales procedentes de actividades como el trabajo, las compras en línea, las operaciones financieras, el registro de sitios web, entre otras. Esta información y datos personales se han convertido en valiosos activos digitales. Por lo tanto, la migración de procesos o actividades rutinarias del entorno físico al digital, no solo transformó los servicios y negocios, sino que también motivó la propagación de delitos cibernéticos. Así, se hace necesario proporcionar medios para el tráfico, manipulación y almacenamiento seguro de estos activos por redes y sistemas de telecomunicaciones, introduciendo el concepto de ciberseguridad.

La ciberseguridad proporciona medios para prevenir ciberataques de cualquier naturaleza. Así como, define marcos de respuesta a posibles ataques que una empresa o institución puede sufrir para mitigar los daños. Existen numerosas técnicas de **ciberataque** destinadas a acceder, capturar o dañar sistemas e información. En algunos casos, estos ataques tienen como objetivo extorsionar a la víctima – persona física a jurídica.

Ninguna organización es totalmente segura, ya que los enfoques y metodologías de ciberataques evolucionan continuamente para eludir las medidas de seguridad preventivas. Sin embargo, las buenas prácticas en la prevención de ciberataques, combinadas con el uso de programas para proteger los sistemas – por ejemplo, ***firewalls*** y **sistemas de monitorización de red** – permiten identificar intentos de intrusión o mitigar los riesgos causados por un posible ataque.



Recientemente, las empresas e instituciones se han enfrentado a un escenario de migración del trabajo presencial al trabajo remoto en respuesta a las medidas preventivas de la COVID-19. La mayoría de estas organizaciones no estaban preparadas para el escenario de acceso remoto a sus redes corporativas. Una vez más, se requerían mayores niveles de seguridad cibernética de las empresas con una rápida adaptación de sus redes para el uso remoto de los empleados, con el objetivo de proteger sus activos digitales. En Brasil, las empresas e instituciones enfrentaron un segundo reto relacionado con la adecuación de sus procesos a la **Ley General de Protección de Datos**, sancionada por el Gobierno Federal y vigente desde agosto de 2021.

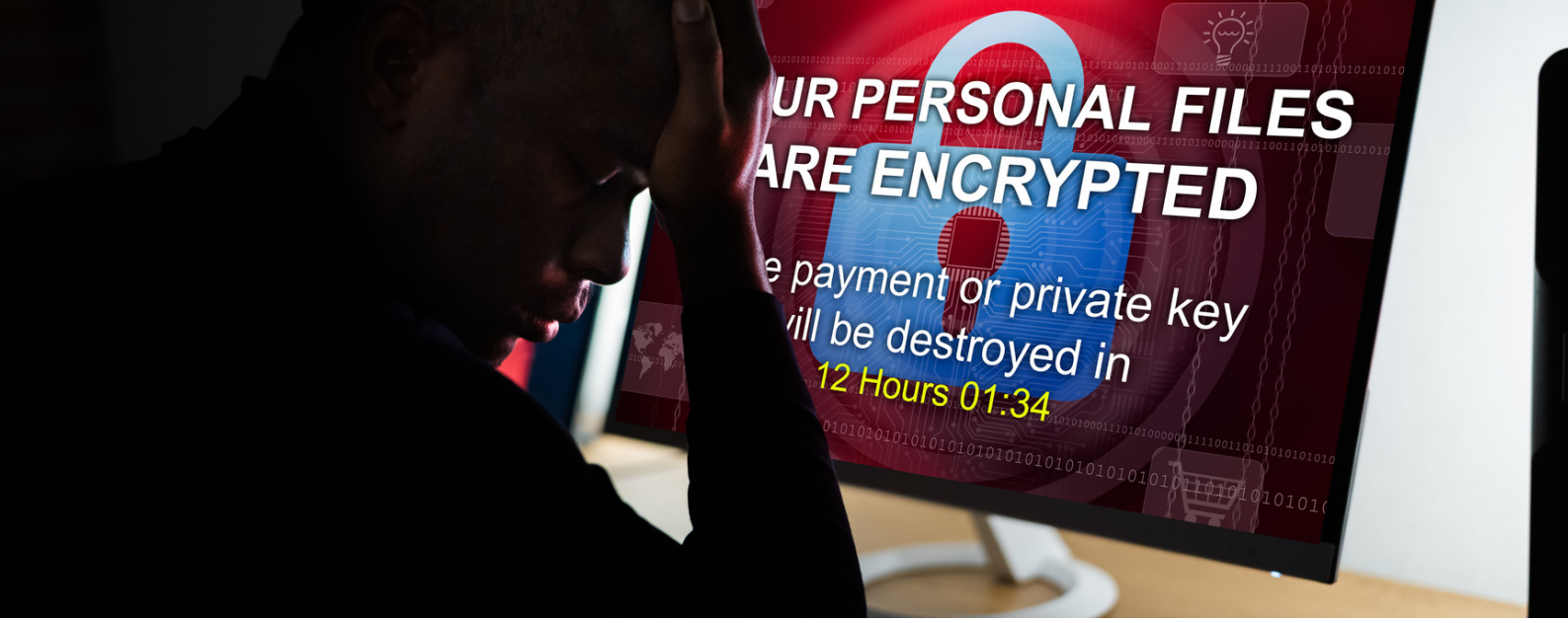
El mundo digital experimentó grandes ataques cibernéticos en **2021.** Estos incluyen la explotación de vulnerabilidades de día cero en servidores de **Microsoft Exchange**, el programa de monitoreo de red Orion TI de **SolarWinds** y la biblioteca de código abierto **Log4j** del Apache *Loggin Services Project*. que sirvió como puerta de enlace para actores maliciosos en un gran número de redes.

Zero-day es una vulnerabilidad desconocida para desarrolladores y usuarios y que está presente en un programa o aplicación. Estas vulnerabilidades se pueden explotar para aprovechar los ataques cibernéticos.

Estos ataques contribuyeron a un aumento en el número de delitos cibernéticos registrados en 2021. Según los datos publicados por **SonicWall** en su informe anual de ciberamenazas, ha habido un aumento en el número de incidentes que involucran intentos de intrusión, ataques de *criptojacking*, ataques de *ransomware* y amenazas cifradas. Entre estas variantes, los ataques de *ransomware* han experimentado un aumento significativo del 105% solo este año.

Por otro lado, los ataques de *ransomware* se clasificaron como la segunda mayor amenaza desde el punto de vista de los encuestados en cuanto al nivel de preocupación por los tipos de ciberataques. **Otros estudios** muestran que Brasil es el cuarto país en términos de número de ataques de *ransomware*.

La empresa de seguridad cibernética BLACKFOG mantiene en su **sitio web** una evaluación del estado de los ataques de *ransomware* para el año 2022, enumerando los ataques para cada mes. Empresas como Toyota, Samsung, Panasonic y Vodafone son entre otras que han reportado algún tipo de incidente con ataques de *ransomware*.



Ransomware

El *ransomware* es un tipo de – de ***malware*** acrónimo de *malicious software*, de español, programas maliciosos – entre otros como *spyware*, *adware* y *botnets*. En general, el *malware* es un programa diseñado intencionadamente para causar daños a los sistemas y dispositivos en los que se instala o proporcionar una ventaja a terceros sobre dichos dispositivos. La naturaleza del *malware* define el nivel de agresividad y potencial de daño. En particular, el *ransomware* es considerado el más agresivo entre las variantes de *malware*.

El *ransomware* es un código malicioso que invade sistemas o dispositivos para secuestrarlos bloqueando el acceso o capturando y encriptando datos, cuya recuperación exige el pago de un rescate al atacante.

Básicamente, este código malicioso invade un sistema o dispositivo para secuestrarlo bloqueando el acceso o para capturar y cifrar los datos almacenados. A continuación, se produce la solicitud de canje del sistema, dispositivo o información condicionada a una contribución financiera. Cuando hay una retención de información, la solicitud de canje incluye amenazas de revelar la información en las vías públicas si no se cumple el pago requerido. Los métodos de pago están dirigidos a mecanismos que hacen imposible el seguimiento, y se verifican las solicitudes de pago en **criptomonedas**, como Bitcoin.

Impactos financieros

Los ataques de *ransomware* se clasifican como delitos de extorsión y desencadenan varios **factores que afectan financieramente a una empresa**. Inicialmente, existe la demanda de rescate, cuyos números son generalmente altos. No se recomienda el pago, ya que no hay garantía para la organización de que el ataque terminará, lo que resulta en más intentos de extorsión. Además, existe la posibilidad de que se dañen los datos.

El ataque puede hacer que las vías de negocio de la empresa no estén disponibles, causando pérdidas por la interrupción. Por otro lado, el tiempo necesario para recuperar sistemas y datos por parte del equipo de TI dificulta el retorno a las actividades de los empleados, lo que afecta a los resultados.

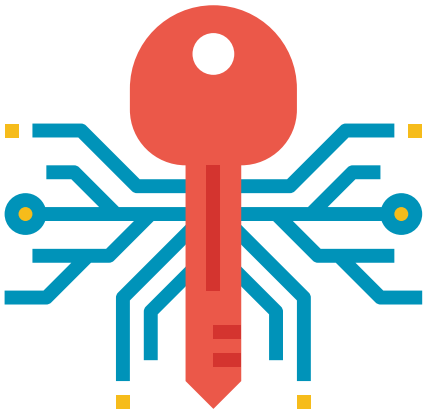
Los ataques de *ransomware* se clasifican como delitos de extorsión y desencadenan varios factores que afectan financieramente a una empresa.

El informe del incidente debe hacerse a la autoridad responsable de gestionar las normas de protección de datos del país. La evaluación del siniestro puede dar lugar a una sanción pecuniaria con las cantidades estipuladas por la legislación. En Brasil, esta autoridad corresponde a la Autoridad Nacional de Protección de Datos (**ANPD**).

El potencial de explotación económica de los ataques de *ransomware* fue reconocido por más de 30 países en 2020 en una reunión virtual. Brasil y otros países, liderados por el gobierno de Estados Unidos, han iniciado la Iniciativa Internacional para combatir el *ransomware*.

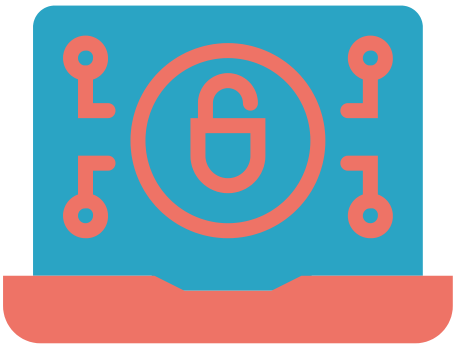
Tipos y métodos de extorsión

Hay varios tipos de *ransomware* que se pueden clasificar ampliamente basado en el proceso de secuestro del sistema, dispositivo o información. Los que emplean cifrado se llaman *Crypto ransomware,* mientras que otros que bloquean los accesos se definen como *Locker ransomware*.



Crypto ransomware **utiliza algoritmos de cifrado para cifrar archivos e información importante, lo que hace que no estén disponibles para el acceso de los usuarios. El proceso de descifrado exige el pago de una cantidad de rescate para recuperar la información.**

Locker ransomware **actúa de manera diferente a *Crypto ransomware*, empleando mecanismos que capturan el dispositivo de la víctima. En consecuencia, recuperar el acceso exige el pago de un rescate.**



En cuanto al proceso de extorsión, las técnicas recientes implican la **doble** extorsión y también la **triple** extorsión. La doble extorsión incluye la demanda de rescate por los datos y la amenaza de filtrar datos e información de las víctimas – persona física a jurídica – si no se paga una segunda cantidad. Este enfoque ha demostrado ser una práctica rentable entre los atacantes en la explotación de ataques de *ransomware*. La triple extorsión surgió a principios de 2021 como una nueva forma de beneficiarse de las solicitudes de rescate. Además de enviar una demanda de rescate, esta técnica implica extorsionar a los clientes de la organización afectada o usar una tercera forma de ataque, como la denegación de servicio como motivación.

Recientemente, un nuevo enfoque relacionado con los tipos de *ransomware* se refiere a su comercialización como servicio: *Ransomware as a Service* – **RaaS**. Los *hackers* dedicados a la programación de *ransomware* los almacenan en sitios *darkweb* y venden suscripciones a otros ciberdelincuentes en un modelo similar al *Software as a Service* – SaaS. La firma permite al criminal explotar el *ransomware* para ejecutar ataques y obtener ganancias a través de la extorsión. Parte del rescate se transfiere al creador del *ransomware* como se establece en un contrato en el momento de la firma.

Evolución del *ransomware* en un clic

La primera aparición de un *malware* clasificado como *ransomware* se remonta a 1989, llamado el **AIDS Trojan**. Este *ransomware* fue creado por el biólogo Joseph Popp y difundido a través de un disquete en la *World Health Organization's AIDS Conference*. Cuando se instala en una máquina, el *ransomware* contaba el número de veces que una máquina había sido reiniciada y después de noventa arranques ocultaría los directorios mediante el cifrado o el bloqueo del acceso a los nombres de los archivos en la unidad de archivos (C:). Recuperó su acceso pagando la suma de U$189.00 a una cuenta identificada como PC Cyborg Corporation.

En 2004, el *ransomware* **GPCode** se extendió a través de correos electrónicos de spam y se camufló como un formulario de solicitud de empleo. Este *ransomware* es un caballo de Troya que cifra los datos del usuario con el algoritmo RSA, seguido de una demanda de rescate. GPCode ha sufrido mutaciones rápidas a lo largo de los años, empleando métodos de cifrado sofisticados como el cifrado asimétrico.

En 2006, surgió otro *ransomware* tipo troyano, apodado **Archievus**. Este *ransomware* fue el primero en utilizar cifrado RSA avanzado, lo que dificulta descifrar los archivos secuestrados. La propagación de este *malware* utilizó enlaces de sitios web y correos electrónicos de spam.

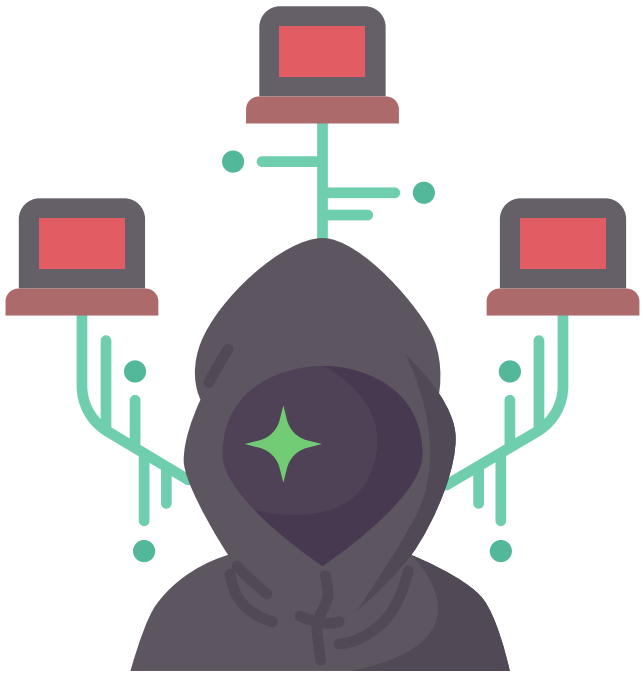
En 2013, el troyano ***Crypto Locker*** en su forma original, extorsionó alrededor de 3 millones de dólares a sus víctimas. Se ha convertido en un modelo de *ransomware* para muchos *hackers*, resultando en variantes que lo han sucedido a lo largo de los años. Este *ransomware* también empleó cifrado asimétrico RSA con claves de 2048 bits de longitud.

En 2017, el ataque de *ransomware* **WannaCry** alcanzó una escala global con pérdidas estimadas de 4.000 millones de dólares. Este *ransomware* explotó una vulnerabilidad en los sistemas operativos Microsoft Windows utilizando un *hack* conocido como EternalBlue. Aunque Microsoft lanzó una actualización para corregir la vulnerabilidad, la falta de conocimiento sobre la importancia de actualizar programas y sistemas se convirtió en una laguna para WannaCry para contaminar los equipos de 230,000. Paralelamente al avance de las criptomonedas, los delincuentes solicitaron pagos iniciales de $300 en Bitcoins.

El ataque del *ransomware* WannaCry alcanzó una escala global con pérdidas estimadas en 4 mil millones de dólares. El *ransomware* aprovechó la vulnerabilidad conocida como EternalBlue en los sistemas operativos Microsoft Windows.

El *ransomware* **Petya** surgió en paralelo con WannaCry y también explotó la vulnerabilidad EternalBlue. Este *malware* ha demostrado ser eficaz para infectar sistemas y dispositivos, incluyendo aquellos actualizados con la vulnerabilidad EternalBlue. Básicamente, Petya actúa sobre el registro de arranque maestro comprometiendo el sistema operativo infectado. En 2017, el *ransomware* **Bad Rabbit** se extendió por los países europeos a través de mensajes de actualización falsos de *Adobe Flash Player*. Los usuarios que aceptaron la actualización fueron infectados por el virus, cuyo valor de rescate fue de R$ 1 mil en Bitcoin.

Recientemente, los ataques de *ransomware* utilizando el enfoque RaaS han surgido como una forma de escalar para propagar virus rápidamente, potenciando la extorsión. En 2019, el *ransomware* **REvil** fue detectado explotando la vulnerabilidad del servidor *WebLogic* de **Oracle**. En 2021, este mismo *ransomware* explotó una vulnerabilidad en los sistemas de **Kaseya**, dirigida a proveedores de administración de seguridad de varias empresas clientes. El rescate de los sistemas implicó una solicitud de 70 millones de dólares. Todavía en 2021, este mismo *ransomware* estaba vinculado a los ciberataques sufridos por las sucursales de la compañía **JBS**, que sucumbieron a la extorsión al pagar alrededor de $11 millones en Bitcoin.



Los ataques recientes informan del uso de RaaS conocidos como **Egregor** y **Conti**. **Barnes & Nobles** es considerada la principal víctima de los ataques de Egregor. Mientras tanto, el *ransomware* **Conti** se clasificó como el segundo mayor número de víctimas en 2021, utilizando varios métodos para irrumpir en las redes corporativas.

Un nuevo tipo de *ransomware* programado en el lenguaje *Rust* ha reclamado ataques recientes, siendo llamado **BlackCat**. Mediante el uso de la compilación cruzada, BlackCat puede dirigirse a los sistemas operativos Microsoft Windows y Linux. Este nuevo *ransomware* es visto como un sucesor del *ransomware* **BlackMatter** y REvil debido a las técnicas similares empleadas en la ejecución de ataques.

Ataque Ransomware

El ciclo de vida de un ataque de *ransomware* comprende un conjunto de acciones que se pueden segmentar en ocho pasos:

- Reconocimiento;
- Preparación;
- Acceso inicial;
- Instalación;
- Descubrimiento;
- Movimientos laterales;
- Recopilación y exfiltración de datos;
- Cifrado, bloqueo de acceso y extorsión.

Los tres principales vectores de entrada explotados en los ataques de *ransomware* son: la difusión de *malware*, el uso de credenciales para el acceso remoto y la exploración y explotación de vulnerabilidades en las interfaces de los servidores con Internet.

Reconocimiento

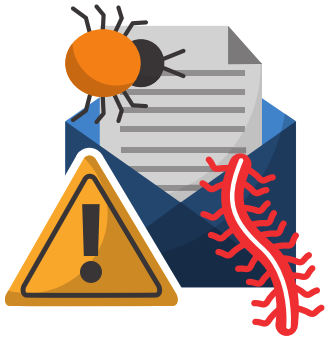
El paso de reconocimiento consiste en explorar **vectores de entrada** para recopilar información sobre la organización objetivo. En esta fase, el atacante realiza una encuesta de información sobre los empleados de la organización mediante la recopilación de correos electrónicos o el análisis de perfiles de redes sociales. Otra posibilidad es explotar la red corporativa desde el punto de vista de las interfaces con Internet para mapear vulnerabilidades.

Preparación

La información recopilada en la fase de reconocimiento se utiliza para definir estrategias para insertar *ransomware* en la red corporativa. Si eliges usar técnicas de **Ingeniería Social**, el atacante prepara el *ransomware* para disfrazarte a través de correos electrónicos que parecen fiables, insertarlo en archivos descargables potenciales – pdf, word, excel – o en sitios web comprometidos. Por otro lado, un atacante podría explotar las vulnerabilidades encontradas en la fase de reconocimiento. Luego, se trazan las herramientas necesarias para ejecutar la invasión.

Acceso inicial

La obtención de acceso a la red o dispositivo de destino comienza con la ejecución del enfoque definido en la etapa de preparación para la entrega de *ransomware*. La entrega debe incluir la ejecución de alguna acción requerida – descargar programas o archivos sospechosos de correos electrónicos de *phishing* – por la víctima para liberar el *ransomware* en la red o la explotación exitosa de una vulnerabilidad.



Esta fase es un punto importante a ser reconocido por las organizaciones, especialmente cuando la entrega se realiza a través de técnicas de ingeniería social. Las prácticas comunes de ingeniería social se consideran eficaces para la propagación de *ransomware* y métodos de intrusión fáciles.

Estos enfoques implican el envío de correos electrónicos de *phishing* con archivos adjuntos o la descarga e instalación de programas de sitios web comprometidos. Además, las superficies de los ataques de *phishing* están evolucionando para aplicaciones de mensajería de texto y *chat*.

Spear phishing también está dirigido a empleados de alto nivel con el objetivo de obtener información confidencial haciéndose pasar por empleados legítimos de la organización.

Por otro lado, el escenario de trabajo remoto ha llevado a un aumento en el número de servidores RDP – ***Remote Desktop Protocol*** – como una forma de proporcionar conexión corporativa a los empleados. Pronto, los atacantes comenzaron a emplear ataques de fuerza bruta contra servicios RDP, redes privadas virtuales y cuentas de usuario. Otros vectores de entrada consideran explotar vulnerabilidades en versiones obsoletas de sistemas operativos, programas o aplicaciones.

Instalación

La entrega exitosa de *ransomware* permite al atacante acceder primero a la red y la instalación de código malicioso para iniciar el proceso de infección. El *ransomware* se instala como un binario, abriendo una ***backdoor*** para comunicarse con un servidor de comando y control, así como cargando los archivos necesarios para las siguientes fases.

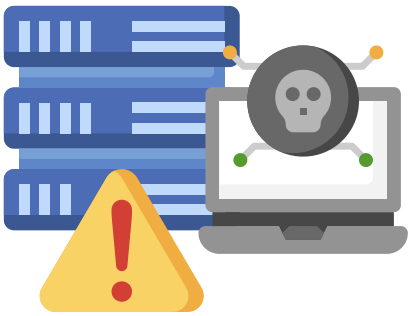
Este paso también incluye la ejecución de procedimientos para ocultar la entrada, asegurar la reinfección del dispositivo y protegerlo de ataques de otros *ransomware.*

Descubierto

Al completar los procedimientos inherentes al paso de instalación, el atacante inicia el reconocimiento del entorno a través del descubrimiento de información, la recopilación de credenciales, la escalada de privilegios, el análisis y la enumeración y la recopilación de datos.

La colección de credenciales emplea herramientas específicas para enumerar las credenciales de usuario. Este procedimiento permite la escalada de privilegios mediante la selección de credenciales de usuarios con privilegios de administrador local o de dominio. El reconocimiento de red a través de la exploración y la enumeración permite al atacante obtener una visión de la red en su conjunto para realizar movimientos laterales. La recopilación de datos es la primera etapa en la búsqueda de datos valiosos que se pueden utilizar en el proceso de negociación.

Movimientos laterales



El mapeo de red a través de herramientas de escaneo y enumeración permite al atacante realizar movimientos laterales. En esta etapa, el objetivo es ampliar el acceso más allá del dispositivo o aplicación inicialmente comprometidos en función del conocimiento de la red a otras máquinas y servicios.

El **movimiento lateral** proporciona un medio para que el atacante busque datos confidenciales y otros activos digitales valiosos, al tiempo que evita la detección y garantiza el acceso persistente a la red. La detección de movimientos laterales es difícil, ya que el análisis de tráfico interpreta las acciones como normales.

Recopilación y exfiltración de datos

El uso de técnicas de doble o triple extorsión introduce la fase de recolección y **exfiltración de datos**. En esta etapa, el atacante tiene como objetivo transferir datos a sus propias copias de seguridad, mientras realiza acciones que podrían comprometer el proceso de restauración de la víctima. Algunos enfoques consideran alterar las rutinas de copia de seguridad y manipular el proceso. Además, introduzca fallas en el programa de copia de seguridad para comprometer el proceso de restauración. La exfiltración de datos se realiza normalmente a través del mismo canal de comunicación establecido en el proceso de instalación.

Cifrado, bloqueo de acceso y extorsión

El último paso en la implementación de un ataque de *ransomware* se refiere a liberar los procesos de cifrado y/o bloquear el acceso a los sistemas y repositorios de datos explotados en los pasos anteriores. A continuación, se anuncia el ataque y se demanda un rescate contra la amenaza de hacer inviables los sistemas y dispositivos, exponer los datos al dominio público o destruirlos.

Gestión de riesgos de Ransomware

La gestión de riesgos de ciberseguridad es un conjunto de prácticas dedicadas a proporcionar soluciones para la seguridad de los activos digitales dentro de una organización. Los enfoques son amplios debido a los diversos ciberataques que una empresa o institución expone al utilizar medios digitales para el desarrollo de su negocio.

Hay actividades dedicadas al reconocimiento integral y detallado de la infraestructura de red. Métodos y buenas prácticas enfocadas en la prevención de incidentes. Mientras tanto, otras acciones permiten detectar la ocurrencia de eventos que suponen un riesgo o violan la seguridad cibernética. En caso de incidencias, existen enfoques que permiten implementar soluciones para mitigar errores y guiar a la organización en el proceso de recuperación.

En este documento, se centra en establecer un conjunto de actividades dirigidas a la gestión de riesgos en *ransomware*. Sin embargo, se hace hincapié en que algunos enfoques pueden generalizarse a una gestión más amplia. El conjunto de acciones en discusión se organiza siguiendo el marco de gestión de riesgos de *ransomware* desarrollado por **NIST** – *National Institute of Standards and Technology* – que los agrupa en:

- Identificación;
- Prevención;
- Detección;
- Respuesta a incidentes;
- Recuperación.

Identificación

La identificación es una fase inicial para la implementación de medidas de gestión de la ciberseguridad con enfoque en *ransomware*. Dado que este *malware* tiene como objetivo explotar vulnerabilidades en la infraestructura de red y acceder a activos digitales críticos, es necesario mapear la arquitectura de red y servicio. Esta acción proporciona una visión general de la infraestructura de la organización y es útil para identificar y remediar posibles vulnerabilidades.

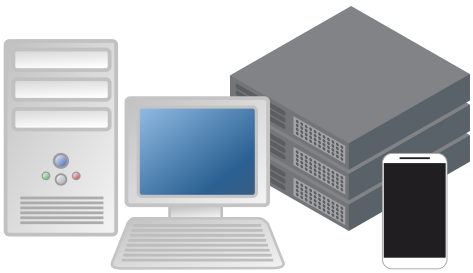
La identificación proporciona una documentación de la infraestructura de la empresa o institución y es útil para mapear y corregir posibles vulnerabilidades.

En caso de incidentes, la información documentada apoya la investigación, permitiendo determinar de forma rápida y precisa posibles violaciones en la implementación de la seguridad. Así como los daños causados por el incidente. En general, las acciones dirigidas a la identificación se organizan en:

- Documentación de *hardware*;
- Documentación de programas, servicios y aplicaciones;
- Documentación de datos e información;
- documentación de servicios externos;
- Documentación de roles y responsabilidades.

Documentación de *hardware*

La organización debe preparar documentación sobre todo el equipo utilizado para prestar los servicios y aplicaciones necesarios para el desarrollo de su negocio. La documentación debe contener las funcionalidades del equipo, su aplicación en el contexto de la infraestructura y la ubicación. Esta información ayuda al personal de TI a implementar procedimientos de respuesta a incidentes, como el aislamiento de los dominios afectados.



Documentación de programas, servicios y aplicaciones

Del mismo modo, los programas, servicios y aplicaciones deben mapearse. La encuesta debe incluir información básica como la versión, la última actualización, el dispositivo host y, especialmente, vulnerabilidades documentadas y sin corregir. En caso de actualizaciones programadas, se deberá añadir información a la documentación que contempla las mejoras y correcciones indicadas por el proveedor. Esta información permite que el equipo de TI tome medidas estratégicas en la gestión de alarmas de ataque masivo mediante la explotación de vulnerabilidades en un programa determinado. Durante la respuesta a un incidente, se pueden identificar programas, servicios o aplicaciones comprometidos y se puede apoyar la investigación forense digital.

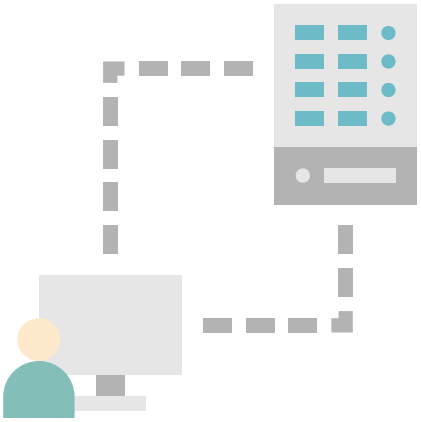
Documentación de datos e información

La organización debe preparar un documento detallado sobre los tipos de datos que recopila, maneja y almacena, así como información inherente al desarrollo de líneas de negocio. La documentación incluirá los medios de recogida, los procedimientos de manipulación y la forma y el lugar de almacenamiento, incluidas las posibles copias de seguridad.

Esta encuesta permite a la organización mapear el nivel de criticidad de los datos e información para el negocio, apoyándola en la implementación de niveles de seguridad adecuados. Una vez más, la información es útil en los períodos de respuesta a incidentes, lo que le permite definir el alcance del ataque.

Documentación de servicios externos

En la realización de sus actividades rutinarias, una organización necesita acceder a servicios que apoyen el desarrollo de su negocio. Este enfoque requiere que la red de la empresa establezca conexiones externas con otras redes o servidores.



Por lo tanto, se hace importante mapear los tipos de conexiones externas, la implementación de capas de seguridad apropiadas y, especialmente, el nivel de seguridad del proveedor de servicios externo. Algunos ataques de *ransomware* comienzan explotando agujeros de seguridad en conexiones externas y/o **infraestructura de proveedor** de servicios.

Documentación de funciones y responsabilidades

La composición del personal y la relación entre sus respectivas funciones y los procesos de la empresa o institución debe documentarse en términos de buenas prácticas y políticas relacionadas con el tratamiento de datos y el acceso a la información confidencial.

Por lo tanto, el empleado debe tener acceso a políticas de seguridad relacionadas con su ocupación organizativa, siendo avalado por el equipo de TI. El documento permite apoyar los métodos de prevención relacionados con la educación de los empleados a través de acciones específicas.

Prevención y Detección

Existen varias acciones que pueden emplearse dentro de una empresa o institución para la prevención de ataques de *ransomware*, que van desde la educación de los empleados en ciberseguridad hasta la implementación de soluciones tecnológicas. Estas acciones le permiten crear etapas de protección en diferentes etapas durante un intento de intrusión de ataque de *ransomware.*

La prevención de ataques de *ransomware* incluye tanto la educación de los empleados como la implementación de soluciones tecnológicas.

Por otro lado, existen herramientas dedicadas a detectar posibles incidentes de ciberseguridad, considerando factores como el análisis del tráfico. En esta sección, estas acciones se presentan con el fin de proporcionar información útil para una buena gestión del equipo de TI.

Educar a los colaboradores

En ciberseguridad, el vínculo humano es el más débil y más fácil de romper. Por lo tanto, los atacantes emplean diferentes formas de ingeniería social para entrar e instalarse en una red. Como se mencionó anteriormente, los correos electrónicos de phishing con archivos adjuntos y aparentemente confiables llevan al destinatario a abrirlo y descargar el archivo adjunto.

Por otro lado, la falta de conocimiento por parte de los colaboradores puede llevarles a sitios comprometidos o maliciosos en la práctica de su oficio a la hora de buscar información o herramientas necesarias. Descargas de programas inadecuadas abren puertas para que el *ransomware* se instale en el dispositivo de la empresa e inicie el proceso de contaminación de la red.

Por lo tanto, es importante invertir en la educación de los empleados en buenas prácticas de ciberseguridad como medio para prevenir ataques de *ransomware*. Se sugiere aumentar la conciencia de los empleados sobre los efectos de un ataque de *ransomware* y cómo pueden estar facilitando agentes para el atacante. Este proceso se puede realizar a través de la difusión de contenidos educativos de ciberseguridad o a través de cursos cortos.

Además, es importante mantener a los empleados alertas, reforzando los riesgos de exposición al navegar por la web. De esta manera, el equipo de TI debe diseñar pruebas de ingeniería social y aplicarlas a los empleados. Los resultados deben recopilarse y utilizarse como demostración de la importancia de la educación en ciberseguridad. Las pruebas deben discutirse con los empleados para demostrar cómo identificar correos electrónicos sospechosos y, especialmente, cómo informarlos al equipo de TI.

Aplicar filtros de tráfico

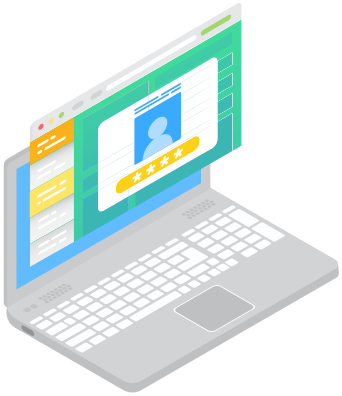
La aplicación de **tecnologías de filtrado de tráfico** web a equipos y dispositivos corporativos le permite crear una barrera para la entrada de *ransomware*. Las URL y sitios web son evaluados y filtrados, evitando que el usuario acceda a aquellos definidos como sospechosos o categorizados como maliciosos.

Los filtros de tráfico web funcionan de dos maneras diferentes para verificar una URL o sitio web y determinar si se debe realizar el bloqueo de contenido. Puede utilizar factores como la calidad del sitio, la consulta en listas conocidas que categorizan las páginas web según el género y el contenido.

La herramienta también puede realizar una evaluación del contenido de la página web para distinguir entre bloqueo o no de acuerdo con los parámetros configurados. Por lo general, estas herramientas utilizan bases de datos que enumeran las URL de diferentes dominios y la posible asociación con *malware*, *phishing* y otros tipos de ataques.

Restringir privilegios de acceso

Al realizar tareas relacionadas con el comercio, se debe realizar una asignación concisa en la que los empleados realmente exijan privilegios de administrador sobre los equipos y dispositivos conectados a la red corporativa. Las credenciales con privilegios de administrador deben reducirse a la menor cantidad posible para limitar la capacidad del atacante para realizar movimientos laterales, cifrar archivos o bloquear el acceso a los dispositivos.

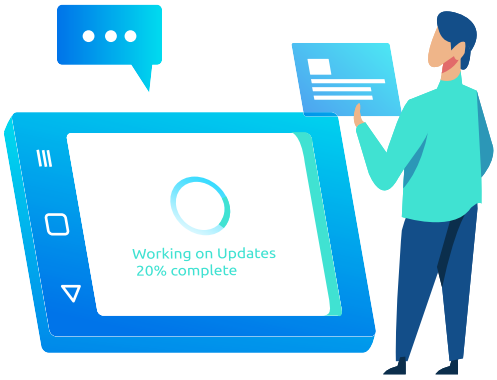


Proporcionar privilegios de administrador a los empleados innecesariamente plantea un riesgo de ciberseguridad para la empresa o institución. Al navegar por la web con tal privilegio, el empleado puede exponerse a ataques de ingeniería social, entregando información valiosa a un atacante potencial. Además de descargar e instalar programas maliciosos y aplicaciones que configuran puertas de enlace para *ransomware*.

Por lo tanto, se recomienda limitar los privilegios de acceso de los colaboradores a la hora de realizar tareas rutinarias como navegar por la web, abrir documentos y aplicaciones, entre otras. De esta manera, si las credenciales de acceso de un empleado se ven comprometidas y se usan para una intrusión de un ataque de *ransomware*, la ejecución se producirá en un equipo o dispositivo con limitaciones de acceso.

Actualizar sistemas operativos, programas y aplicaciones

La explotación de vulnerabilidades en sistemas operativos, programas y aplicaciones representa un vector de entrada importante para el *ransomware* en una red.



Como hemos comentado anteriormente, algunos ataques de *ransomware* han explotado estas vulnerabilidades para acelerar y escalar el proceso de propagación de *malware*, comprometiendo una gran cantidad de máquinas.

Por lo tanto, es importante que el equipo de TI siga las recomendaciones de actualizaciones solicitadas por los sistemas operativos, programas y aplicaciones utilizados para el desarrollo del negocio de la organización. Al verificar una solicitud de actualización, el personal de TI debe realizar las actualizaciones de forma remota – recomendadas. O informar y pedir a los empleados que las ejecuten inmediatamente, asegurando que se corrijan las posibles vulnerabilidades.

Esta práctica elimina la posibilidad de que un ordenador o dispositivo se contamine bajo la prerrogativa de que todas las máquinas en la red estén actualizadas a nivel de sistema operativo, programas o aplicaciones alojadas.

Supervise la red

El uso de programas de monitoreo de red integrados con un *firewall* es un mecanismo para prevenir ransomware u otros ataques. Por lo general, el primer paso en los ataques cibernéticos implica el escaneo de actividades en la red.

De este modo, el sistema de monitorización puede identificar y aislar automáticamente el dispositivo analizado de un atacante, desconectarlo de Internet e informar de la actividad al equipo de TI de la empresa para su revisión. Esta práctica puede poner fin a un posible ataque, evitando que el dispositivo identificado infecte otras máquinas.

Aplique las políticas de contraseñas y reduzca el acceso remoto

Deben implementarse políticas estrictas de elaboración de contraseñas para evitar intrusiones a través de ataques de fuerza bruta. Obligar a los empleados a cambiar periódicamente las contraseñas y establecer políticas que les impidan reutilizar las contraseñas de períodos anteriores.

En caso de acceso remoto a la red corporativa, se debe evaluar periódicamente la necesidad de que los empleados tengan acceso remoto de acuerdo con la actividad. Con el retorno parcial de algunos empleados a las oficinas, el acceso remoto debe eliminarse inmediatamente, reduciendo la posibilidad de intrusión por parte de las VPN.

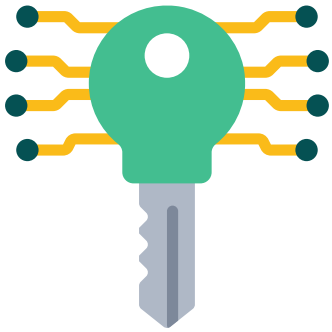
Implementar rutinas de *backup*

Realizar copias de seguridad periódicas de sistemas, datos e infraestructura y realizar pruebas de procedimientos de restauración de vez en cuando es un procedimiento eficaz para los ataques de *ransomware*. Esta práctica permite a la organización tener alternativas para restaurar las partes afectadas durante el ataque, eliminando la necesidad de pagar el rescate.

Las copias de seguridad permiten al personal de TI restaurar las máquinas a las versiones anteriores al proceso de infección. Por lo tanto, se recomienda mantener las versiones del mismo sistema en diferentes intervalos de tiempo. Por ejemplo, una copia de seguridad de intervalos de 30 días y una copia de seguridad de intervalos de 60 días. Esta práctica evita restaurar versiones contaminadas cada pocas semanas, lo que desencadena un proceso de restauración largo e ineficaz por retrabajo.

Además de la opción de mantenimiento de copias de seguridad sin conexión, una práctica posible pero inusual, el almacenamiento de copias de seguridad puede incluir ubicaciones separadas y distribuidas. De esta manera, las soluciones en la nube se utilizan en diferentes áreas de disponibilidad del mismo proveedor – diferentes centros de datos. O, incluso, en las nubes de varios proveedores, una estrategia conocida como multinube. De esta manera, evita que el ransomware obtenga acceso rápido a todas las ubicaciones de almacenamiento y practique el cifrado o la destrucción de copias de seguridad para eliminar las fuentes de restauración como una forma de reforzar la demanda de rescate.

Cifrar datos



Las copias de seguridad periódicas son importantes para ayudar a la organización a recuperarse de un ataque de *ransomware* mientras evita pagar el rescate. Sin embargo, la sensibilidad de los datos puede ser un factor decisivo para pagar el rescate bajo amenaza de exposición al dominio público.

Por lo tanto, es importante realizar un mapeo adecuado de los datos e información manejada por la empresa, enumerar su nivel de sensibilidad e implementar mecanismos de cifrado. Es de destacar que las claves de cifrado implicadas en el proceso deben almacenarse en lugares de acceso restringido y diferentes de aquellos donde se encuentran los datos.

Segmentar la red

La segmentación de servicios externos es una práctica óptima cuando se estructura una red informática. Este proceso garantiza que el acceso a y desde estos servicios está restringido. Además, el acceso remoto debe ser evaluado por un sistema de supervisión de red e incluir autenticación de dos factores.

Los segmentos de red deben configurarse de manera que el tráfico de información entre ellos se limite a servicios específicos y se monitorice por el dispositivo de segmentación apropiado. Estas políticas de tráfico deben hacerse para que el ataque y la infección por un *ransomware* en un segmento no afecte a otros o a toda la red. Por lo tanto, se recomienda que los servidores críticos estén aislados por sus propios segmentos en lugar de agruparlos en un solo segmento de red. La criticidad del servicio también se puede usar para delimitar segmentos, aislando redes internas de aquellas expuestas a Internet, por ejemplo. En los dominios de estaciones de trabajo, las máquinas deben configurarse para evitar el flujo de datos entre sí.

Todas las máquinas que requieren conectividad a Internet deben configurarse para usar un servidor central en una red perimetral – también llamada *Demilitarized Zone*, **DMZ** – en lugar de adquirir una dirección IP directa. Las máquinas que necesitan realizar búsquedas en la web deben estar aisladas del contacto directo con otras máquinas o dispositivos que no tienen esta funcionalidad, evitando que sus vulnerabilidades sean explotadas.

Explorar y corregir vulnerabilidades

La presencia de vulnerabilidades en una red es algo intrínseco, ya que los sistemas operativos, programas y aplicaciones pasan por procesos de actualización. Además, los elementos de red se configuran y reconfiguran de acuerdo con las demandas diarias.

En cuanto a las actualizaciones, cabe recordar que tienen dos propósitos en el ciclo de vida de un sistema operativo, programa o aplicación: ofrecer una mejor experiencia al usuario final o corregir posibles vulnerabilidades. La configuración de los elementos de red está vinculada a la acción humana, que puede exponer indebidamente los puertos de comunicación a Internet.

El proceso de actualización, independientemente de su propósito, puede traer consigo una nueva vulnerabilidad, cuyo conocimiento de su existencia proviene, al principio, de ciberdelincuentes, lo que resulta en vulnerabilidades de "día cero". Los atacantes pueden explotarlos para propagar ataques de *ransomware* en redes que tienen equipos y dispositivos que ejecutan el sistema operativo, programa o aplicación con la vulnerabilidad identificada.

Por lo tanto, el análisis proactivo de vulnerabilidad permite al personal de TI identificar violaciones de políticas de acceso o dispositivos vulnerables. Este proceso implica la ejecución de pruebas de intrusión – ***Pentest*** – por profesionales experimentados conocidos como ***Ethical Hacker***. Las pruebas le permiten identificar posibles vulnerabilidades y corregirlas.

Planificar y formar al equipo

Es importante reforzar: ¡ninguna empresa o institución es totalmente inmune a los ciberataques! La evolución de la tecnología es una calle de doble sentido. Por un lado, las soluciones defensivas mejoran con el objetivo de reducir las superficies de ataque. Por otro lado, las soluciones ofensivas evolucionan mejorando las técnicas existentes y creando nuevos enfoques de ataque.

Por lo tanto, la mejor prevención es el desarrollo de un buen plan de respuesta y recuperación ante incidentes que impliquen un ataque de *ransomware*. Debería elaborarse un manual de apoyo accesible a los responsables de la gestión de la seguridad dentro de la empresa o institución. Este manual debe revisarse y actualizarse periódicamente.

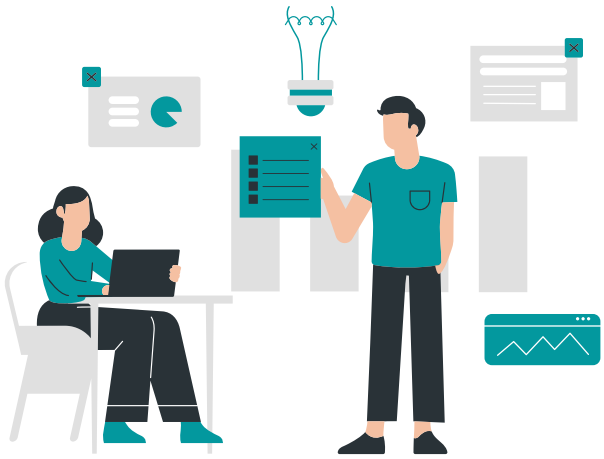
El plan de acción está destinado a proporcionar organización y calma durante un ataque de *ransomware*. Para ello, se espera que el plan defina las actividades y se encargue de ejecutarlas, evitando confusiones. Por lo tanto, el plan de acción debe contener la identificación de las partes interesadas para ejecutar y gestionar la respuesta a los incidentes. En este contexto, incluyen personal de TI, personal de relaciones públicas, equipos de sistemas/aplicaciones y asistencia jurídica.

Algunas observaciones importantes sobre el proceso de redacción del plan de acción incluyen aspectos de comunicación, sistemas de datos críticos y selección de métodos de restauración. El plan debería dar prioridad a los sistemas de datos críticos para proporcionar acciones coordinadas de recuperación desde el nivel más crítico al menos prioritario. Asimismo, debe contener medios de comunicación seguros que no se vean comprometidos o no estén disponibles durante el ataque, como el correo electrónico corporativo o el sistema telefónico.

Este proceso debe identificar sistemas y servicios críticos para las líneas de negocio de la empresa o institución y mapear sus respectivas interacciones con otros sistemas y servicios para establecer estrategias de recuperación ordenadas. Se recomienda prioridad en los servicios de infraestructura de red como los directorios activos – por ejemplo, DNS y DHCP.

Asimismo, el plan debería incluir un mapeo conciso de los datos tratados por la empresa. Este paso permite a la empresa identificar el tipo de datos comprometidos durante un ataque y su criticidad para el negocio. En consecuencia, se pueden proteger los datos no infectados y establecer métodos para recuperar los objetivos del ataque.

La estrategia de recuperación y restauración de sistemas y servicios en un escenario de ataque debe incluirse en el plan de acción. La ejecución del plan debe incluir procesos de recuperación y restauración que mejor se ajusten al propósito según la naturaleza del ataque. Por ejemplo, la recuperación de máquinas a través de copias de seguridad seguras puede resultar en la pérdida de archivos o datos no infectados o cifrados entre la fecha de su copia de seguridad y el ataque. Por lo tanto, las estrategias de recuperación a nivel de archivo o base de datos pueden ser un mejor enfoque. Para ataques amplios, se recomienda la recuperación masiva. Un punto clave en el proceso de recuperación es la automatización para minimizar los errores humanos, así como acelerar el proceso.



Finalmente, un buen plan requiere pruebas periódicas, evaluación de resultados y correcciones. Las pruebas le permiten identificar puntos de cuello de botella y volver a trabajar para garantizar una ejecución completa en respuesta a un incidente real. Las simulaciones permiten que los recursos humanos involucrados ejecuten sus habilidades y responsabilidades, proporcionando mayor confianza en incidentes reales. Se recomienda que el entorno de prueba sea lo más realista posible y planificado de manera que no perturbe el negocio de la empresa o institución.

Soporte en forense digital

En casos de incidencias es importante que la empresa o institución cuente con el apoyo de otras empresas que prestan servicios en análisis ***forense digital.*** Por lo tanto, se recomienda contratar a un proveedor de servicios forenses digitales para soporte inmediato en escenarios de ataque o sospecha de ataque.

Esta provisión de servicio permite una respuesta rápida en la determinación de la magnitud del ataque a la red y su neutralización. Además, se puede obtener apoyo técnico experto en la determinación de puntos estratégicamente seguros para los procesos de recuperación.

Aplicar métodos de detección

Hay tres técnicas utilizadas para detectar un ataque de *ransomware*: seguimiento de firmas, análisis de comportamiento y engaño. El seguimiento de firmas implica identificar la firma del *ransomware* comparando una muestra de su hash con otros hashs conocidos. Este enfoque permite un análisis rápido de los archivos sospechosos y la definición de su naturaleza maliciosa. Generalmente, los programas antivirus emplean esta técnica.

De hecho, los primeros antivirus utilizaron un análisis reactivo considerando la investigación previa por acción humana o programa autónomo en el análisis del tipo de *ransomware* y el seguimiento de su firma. En este punto, vale la pena recordar que cada *ransomware* tiene su propia firma. Por lo tanto, este enfoque tenía una laguna con respecto a los *ransomware* "día cero" que aún no habían sido evaluados previamente.

Esta brecha llevó a los atacantes a actualizar los tipos de *ransomware* para adaptar su firma bajo diferentes formas de codificación. En respuesta, los programas antivirus han implementado técnicas complejas para el seguimiento de firmas al considerar familias de *malware* a través de soluciones heurísticas.

Posteriormente, los códigos de *ransomware* evolucionaron sus tácticas para evadir los sistemas antivirus, utilizando el concepto de polimorfismo. El polimorfismo permite que el *ransomware* disimule su firma de una manera que evita el seguimiento y la detección de programas antivirus. Los atacantes utilizan el enfoque de "empaquetado y cifrado" para modificar el *ransomware* a nivel binario.

El polimorfismo ha asegurado la efectividad de los ataques de *ransomware*, como muestra **Webroot**, cuyas cifras revelan que el 97% del *ransomware* detectado en computadoras y dispositivos son únicos. A pesar de la introducción del polimorfismo, el rastreo de firmas es una primera línea de defensa y puede ayudar a identificar *ransomware* conocido.

El análisis de comportamiento le permite utilizar una base histórica para evaluar nuevas actividades en una red. Se puede emplear en el análisis de la ejecución de archivos o tareas relacionadas, permitiendo identificar actividades anormales tales como una copia excesiva de archivos por unidad de tiempo. Otra posibilidad es mapear la creación de archivos con excesiva entropía, lo que indica la instalación de *ransomware* en período de incubación. El análisis de tráfico también le permite definir actividades sospechosas en la red como un aumento del tráfico dirigido a un servidor en particular.

Un enfoque más activo considera la creación de repositorios de archivos que no son accesibles por los empleados de la empresa en general, pero que bajo ataque se convierten en una oportunidad fácil. Por lo tanto, la supervisión del acceso a los servidores falsos puede alertar sobre la posibilidad de un posible ataque de *ransomware*.

Respuesta y recuperación

En el caso de un ataque de *ransomware*, hay un conjunto de medidas que se deben seguir para proporcionar una respuesta efectiva y recuperación al incidente. Algunas de las prácticas que se discutirán en esta sección forman parte o deben definirse previamente en el plan de respuesta y recuperación a incidentes, recomendado como metodología preventiva. En general, puede enumerar las acciones en:

- Validación del ataque
- Establecer el alcance del ataque
- Aislar los sistemas infectados y preservar la evidencia
- Reportar el ataque a todos los involucrados y a las autoridades
- Evaluar y neutralizar el ataque
- Restaurar sistemas y datos
- Evaluación y aprendizaje post-recuperación

La validación de ataques debe ser el primer paso en un proceso de respuesta a incidentes de ciberseguridad.

Validación del ataque

La validación del ataque debe ser el primer paso en un proceso de respuesta a un incidente de ciberseguridad. Esta actividad pretende definir de hecho cuál fue la naturaleza del ataque para que se tomen los procedimientos necesarios.

En esta sección se describen las actividades para responder y recuperarse de un incidente de *ransomware*. Por lo tanto, si el ataque se valida e identifica como *ransomware*, los siguientes pasos son válidos para la ejecución.

Cabe señalar que los ataques de *ransomware* suelen ser reportados por los colaboradores cuando se encuentran con mensajes de rescate típicos o encuentron archivos supuestamente cifrados. Estos eventos requieren la atención del equipo de TI, que debe iniciar un proceso de revisión sin solicitar la confirmación de un ataque. Porque, los mensajes encontrados pueden ser falsos o el archivo cifrado puede provenir de un proceso que ocurrió en el pasado.

Si se sospecha la presencia de *ransomware*, se debe iniciar una etapa de evaluación de la etapa de infección. Si el *ransomware* se identifica en las primeras etapas, es posible eliminarlo y aislar la máquina infectada sin requerir una respuesta amplia al incidente. Sin embargo, es importante realizar análisis preventivos en todas las máquinas que comparten el dominio de red. En caso de que se haya infectado más de una máquina, debe llevarse a cabo la ejecución completa del plan de acción preparado.

Establecer el alcance del ataque

La confirmación del ataque debe hacerse delimitando el alcance del ataque a la red. Esta acción es extremadamente importante para ayudar al equipo de TI en la ejecución de los procesos de mitigación de daños. Por otro lado, definir el alcance del ataque permite comprender qué servicios, sistemas y datos se han visto comprometidos. De esta manera, uno puede mapear los sistemas afectados y trabajar en los procesos de recuperación dirigidos. Si el ámbito de ataque no está definido, se recomienda restaurar todos los sistemas y datos.

Este enfoque da como resultado una mayor pérdida de datos y tiempo de recuperación. Identificar el alcance del ataque en relación con los datos manejados por la empresa y establecer el nivel de criticidad, permite determinar si es necesario implementar procedimientos adicionales y notificar a los clientes.

El alcance debe considerar la evaluación de carpetas y controladores compartidos o no compartidos, espacios de almacenamiento en la red y en la nube, controladores externos y archivos importantes. Una forma de determinar el alcance del ataque es consultar los registros de los archivos generados por el *ransomware*, que especifican qué archivos han sido cifrados. Sin embargo, este enfoque requiere conocer el tipo de *ransomware* instalado durante el ataque. En cuanto a los datos, es posible determinar cuáles fueron copiados en base al mensaje de rescate del propio *ransomware*. Además, es posible explorar la propia red para buscar evidencia de copia masiva de datos.

Aislar los sistemas infectados y preservar la evidencia

La definición del ámbito de ataque le permite realizar un procedimiento de contención adecuado aislando los sistemas infectados. Esto evita que el *ransomware* se propague a equipos y dispositivos no infectados en un dominio o avance a otros segmentos de red.

Este paso requiere la desconexión del equipo ya sea por cable o por red inalámbrica a nivel físico. Para otras redes, es necesario realizar una desconexión temporal con Internet como una forma de garantizar la total indisponibilidad de acceso al atacante.

Es importante destacar que los sistemas y dispositivos aislados deben tener instantáneas válidas y no caducadas para permitir la recuperación de datos. Después de la neutralización y eliminación del *ransomware* acompañada del proceso de recuperación, se recomienda establecer un perímetro de red y someter los dispositivos objeto del ataque a supervisión mediante acuerdos de nivel de servicio basados en políticas de retención durante al menos un año.

Otra recomendación importante durante una respuesta a un ataque de *ransomware* es llevar a cabo la recopilación y conservación de pruebas tales como archivos de registro e imágenes del sistema. Es importante monitorear el estado de esta evidencia, que puede cambiar durante las etapas del ataque hasta su completa neutralización.

Para los ataques de *ransomware*, las claves de cifrado también son importantes como evidencia para una investigación adicional y deben ser capturados rápidamente antes de que sean eliminados por el *malware*. En caso de demanda de rescate, se recomienda registrar el correo electrónico, la dirección de pago y el texto de canje. Esta información es solicitada por la entidad que llevará a cabo las investigaciones forenses.

Definir el tipo de *ransomware* es un punto relevante, ya que cada *malware* tiene un patrón de cifrado, robo de datos y anuncio de rescate. Algunos *ransomware* pueden componer variantes de familias ya mapeadas de ataques anteriores, cuya información ayuda a la organización en la toma de decisiones. Además, las empresas de consultoría de ciberseguridad pueden mantener información sobre las claves de cifrado empleadas por el tipo de *ransomware*, ayudando en el proceso de descifrado. Otros aspectos técnicos pueden proporcionar información para que el proceso de neutralización sea efectivo.

Reportar el ataque

Después de cumplir con los pasos anteriores, todos los involucrados en el plan de prevención deben ser comunicados inmediatamente para que puedan realizar las rutinas establecidas. La comunicación debe hacerse a través del canal de comunicación definido en el plan de acción. La información debe presentarse de manera clara y objetiva a todo el equipo de TI, ejecutivos y gerentes, así como a los equipos legales y de relaciones públicas.

En el contexto legal, incluye la figura de la DPO – *Data Protection Office* – en liderar la empresa en relación con las acciones legales a emprender frente a la autarquía de cada país y los clientes, si el ataque involucra sus respectivos datos. La empresa debe gestionar los impactos internos y externos del ataque a través del intercambio correcto y en tiempo real de los resultados, permitiendo que la industria de las relaciones públicas se posicione adecuadamente para minimizar los impactos financieros en la marca.

Evaluar y neutralizar el ataque

Es importante mantener una evaluación del estado actual del ataque para que el proceso de recuperación tenga lugar después de que el ataque esté completamente neutralizado. Si el ataque no se neutraliza, hay altas posibilidades de reintroducir el *ransomware* y reinfectar los sistemas, lo que resulta en un aumento de los daños y el tiempo de inactividad para una mayor recuperación. Es importante establecer un perímetro de cuarentena para iniciar el proceso de recuperación. De esta manera, las restauraciones se pueden validar antes de volver al entorno de producción.

Restaurar sistemas y datos

El proceso de recuperación del sistema debe iniciarse solo después de que el *ransomware* haya sido neutralizado. La recuperación antes de la eliminación de *ransomware* resulta en una infección secundaria. Si el *malware* no puede aislarse y neutralizarse, la recuperación debe dirigirse a un entorno aislado para que la infección no se propague.

La recuperación de datos debe implicar un análisis exhaustivo para identificar el mejor enfoque. Si existe la posibilidad de descifrarlos para el ransomware identificado, uno debe continuar con el proceso para evitar la pérdida de datos entre la fecha de la última copia de seguridad y la ocurrencia del ataque. Actualmente, existe una iniciativa llamada **No More Ransom** que involucra a empresas de TI y seguridad legal para proporcionar soporte de recuperación de ataques de *ransomware*. Es de destacar que el proceso de descifrado debe llevarse a cabo en un entorno aislado y controlado.

Cuando sea necesario realizar la recuperación de sistemas y datos a través de *backup*, debe realizarse en entornos aislados en comparación con el infectado por el *ransomware*, evitando ataques secundarios. Como se ha analizado en las hipótesis de diseño del plan de recuperación, el proceso debe iniciarse en función del nivel de prioridad asociado al servicio o sistema afectado.

A restauración del sistema puede implicar dos enfoques: reparaciones o reconstrucción. La restauración rápida de las piezas afectadas por el ataque, no recomendada, es una opción barata y ágil. Sin embargo, no hay garantía de que el *malware* fue eliminado por completo, exponiendo la infraestructura de la red a un posible ataque secundario. Por otro lado, la reconstrucción de cada servicio o aplicación en la red es una práctica recomendada, ya que garantiza la eliminación completa del *ransomware*. Por lo tanto, implica un mayor tiempo de trabajo de los equipos de TI y puede afectar a los procesos de producción de la organización.

Evaluación y aprendizaje posterior a la recuperación

Después de la respuesta al incidente y la recuperación de sistemas y datos, es importante llevar a cabo una investigación forense digital a nivel de datos e información para identificar si solo se produjo cifrado local en el proceso de ataque. Si se detectan pruebas de exfiltración, debe facilitarse información de las autoridades competentes y, en caso de estar implicada, debe notificarse a los clientes.

El análisis forense digital también permite evaluar las vulnerabilidades que permitieron que el ataque se produjera en primera instancia. Posteriormente, este conocimiento debe ser aplicado en el proceso de corrección de vulnerabilidad con la implementación de buenas prácticas en seguridad cibernética. En este punto, las medidas preventivas presentadas en este documento son válidas según el caso identificado.

Gestionar riesgos

El plan de respuesta y recuperación para incidentes que involucren ataques de *ransomware* debe incluir la gestión de riesgos y la política de pago de rescate. De esta manera, las partes involucradas deben establecer directrices sólidas para definir si el pago del rescate se ejecutará o no. Cabe destacar que la recomendación es nunca pagar el rescate por las razones adecuadas:

- El pago no garantiza que el atacante entregará los medios de descifrado
- El pago refuerza la práctica delictiva
- La experiencia muestra que no siempre se reconstruyen todos los archivos cifrados
- No hay garantía de que el atacante detendrá el proceso de extorsión después del primer pago. Si se produce la exfiltración de datos, existe la posibilidad de una segunda demanda de rescate
- El pago no garantiza que el atacante conservará la información y no la publicará.

Sin embargo, la organización debe tener sus capacidades técnicas mapeadas y, durante un incidente que involucra *ransomware*, definir la posibilidad de recuperación de sistemas, datos e información. Se debe establecer el nivel de sensibilidad de los datos e información en poder del atacante y los impactos en el negocio de la organización. Estos factores influyen en la decisión sobre si pagar el rescate.

Si la organización decide realizar el pago de reembolso, deben definirse los posibles enfoques. Entre ellos, se cita la figura del comerciante, cuánto está dispuesta a pagar la empresa y los medios de acceso a la criptomoneda para el pago.

Acerca de CxSC Telecom

El Centro de Segurança Cibernética (CxSC Telecom Inatel) es el centro de investigación de seguridad cibernética del Instituto Nacional de Telecomunicações - Inatel, ubicado en Santa Rita do Sapucaí - MG. El CxSC abarca diferentes áreas de especialización como educación, certificación, formación, investigación aplicada y servicios relacionados con la ciberseguridad y áreas relacionadas. Creada en 2020, CxSC tiene como objetivo desarrollar la ciberseguridad en el contexto de la sociedad brasileña. El centro cuenta con trabajos de investigación de profesores y expertos de Inatel. Además, colaboraciones con empresas como Huawei, Sikur y otros institutos de investigación como IMREDD (*Institut Méditerranéen du Risque, de l'Environnement et du Développement Durable*).

Reconocimiento

Este trabajo se desarrolló a partir de información y opiniones de diversas personas y empresas del sector de las telecomunicaciones. Inatel agradece toda la información recibida y especialmente el apoyo y las contribuciones realizadas por Huawei, que siempre apoya las iniciativas del Centro de Segurança Cibernética do Inatel.

HUAWEI

24 ANOS
NO BRASIL PARA O BRASIL

CxSC Telecom
Centro de Segurança Cibernética

Inatel