Protección contra el ransomware

Zero Trust Security para una fuerza de trabajo moderna

El ransomware ha llegado para quedarse

El ransomware ha evolucionado rápidamente como estrategia de ataque. Antes se trataba de la absorción hostil de computadoras en solitario; hoy, los ataques van en aumento. Los actores de amenaza apuntan cada vez más a objetivos geopolíticos, sistemas comerciales e infraestructuras críticas, lo que podría conducir a daños sin precedentes. Hoy en día, el ransomware es una de las mayores amenazas en ciberseguridad, con un aumento del 150% en 2020 debido al repentino paso al trabajo remoto.

El ransomware ahora se clasifica como terrorismo cibernético y la reciente orden ejecutiva del presidente de los Estados Unidos, Biden, confirma que se deben tomar medidas en este momento para mantener los sistemas seguros. Un enfoque de confianza cero es el estándar de oro para la protección contra el ransomware. Según indica el Instituto Nacional de Estándares y Tecnología (NIST, National Institute of Standards and Technology): "Implementar una arquitectura de confianza cero se ha convertido en un mandato de seguridad cibernética y una necesidad comercial".

Según establece la hoja informativa de la Casa Blanca:

"Los recientes incidentes de seguridad cibernética, como SolarWinds, Microsoft Exchange y el incidente de Colonial Pipeline, son un recordatorio aleccionador de que las entidades del sector público y privado de los EE. UU. enfrentan cada vez más actividades cibernéticas maliciosas sofisticadas tanto de actores de estados nacionales como de ciberdelincuentes".

Hoja informativa de la Casa Blanca de los Estados Unidos de América.

¿Qué es el ransomware?

En pocas palabras, el ransomware emplea una variedad de tácticas para atacar a los usuarios principalmente a través de infecciones de malware, que generalmente comienzan con la suplantación de identidad (phishing) por correo electrónico, una contraseña robada o un ataque a la fuerza. Un ataque de ransomware se puede llevar a cabo mediante el cifrado de archivos o carpetas, lo que impide el acceso del sistema al disco duro y, también, a través de la manipulación del registro de arranque maestro para interrumpir el proceso de arranque del sistema. Una vez que el malware se ha instalado y propagado, los piratas informáticos pueden obtener acceso a datos confidenciales y datos de respaldo, que proceden a cifrar para mantener la información como rehén. Los piratas informáticos pueden actuar rápidamente o pasar meses hurgando sin ser detectados para llegar a comprender la infraestructura de la red antes de lanzar un ataque.

El secuestro de datos tiene como propósito provocar el miedo y la urgencia de las víctimas. Su información es inaccesible hasta tanto se pueda realizar el pago (principalmente en bitcoins). Incluso en ese caso, es posible que las empresas no recuperen todos sus datos. Existen muchas variantes de ransomware, pero, en su mayor parte, el cryptoransomware domina el campo. Debido al polimorfismo (malware que cambia constantemente), existen muchas variantes que pueden evitar la detección.

El cryptoransomware que bloquea los datos se está perfeccionando rápidamente. En 2006, el ransomware usaba 56 bits con encriptación casera. La versión avanzada actual del ransomware utiliza algoritmos simétricos AES y encriptación de clave pública RSA o ECC para bloquear datos.

El ransomware se convierte en un negocio

A medida que el ransomware continúa cobrando impulso, ha madurado hasta convertirse en un negocio profesional liderado por organizaciones criminales (principalmente ubicadas en China, Rusia, Corea del Norte y Europa del Este), las cuales están dedicadas a marcar e interrumpir objetivos de alto valor y extraer dinero a cambio de datos. Para hacer esto con eficacia, estas organizaciones incluso han ido tan lejos como para establecer centros de llamadas para guiar a los objetivos a través del proceso de compra de bitcoins y el pago del rescate. Algunos, incluso, están bien calificados por su buen servicio al cliente por parte de sus objetivos.

A veces, para obligar al pago, los atacantes proporcionan un "informe de seguridad" detallado que explica exactamente cómo realizaron el ataque después del intercambio por el rescate. Si bien sería inteligente que las pandillas desencriptaran los archivos a cambio de dinero para mantener intacta su reputación para el próximo objetivo, no siempre resulta así. The State of Ransomware 2021 de Sophos afirma que solo el 8 % de las víctimas recupera sus datos y el 29 % recupera más de la mitad. A veces, los datos se recopilan y se intercambian con otros atacantes o se retienen para otra oportunidad de rescate futura.

En los últimos años, los malos actores han establecido el ransomware como servicio (RaaS), una solución lista para usar totalmente integrada que le permite a cualquier persona implementar un ataque de ransomware sin saber cómo codificar. Al igual que los productos de software como servicio (SaaS), el RaaS brinda un acceso relativamente económico y fácil a este tipo de programas maliciosos por una tarifa menor que el costo de crear uno propio. Los proveedores de RaaS, por lo general, toman un recorte del 20 % al 30 % de la ganancia generada por el rescate. Ahora existen modelos de suscripción y afiliados para ayudar a llevar a cabo ataques exitosos. El grupo de piratas informáticos REvil contaba con un modelo de afiliado que compartía las ganancias con cualquiera que contribuyera a un ataque de ransomware exitoso. Este modelo ha llevado a un aumento drástico en el volumen de ataques de ransomware.

Atribuida primero a la pandilla Maze, otra tendencia es la doble extorsión, en la que los piratas informáticos toman la información secuestrada y amenazan con publicarla en la web oscura o en Internet si no se satisfacen sus demandas. Tienen una infraestructura integrada para manejar estos volcados de datos, de acuerdo con el Informe de investigaciones de violación de datos de 2020 de Verizon. La táctica de "nombre y oprobio" ahora es popular para la mayoría de las pandillas de ransomware, al igual que el modelo de "penalización", donde el precio aumenta a medida que transcurre el tiempo.

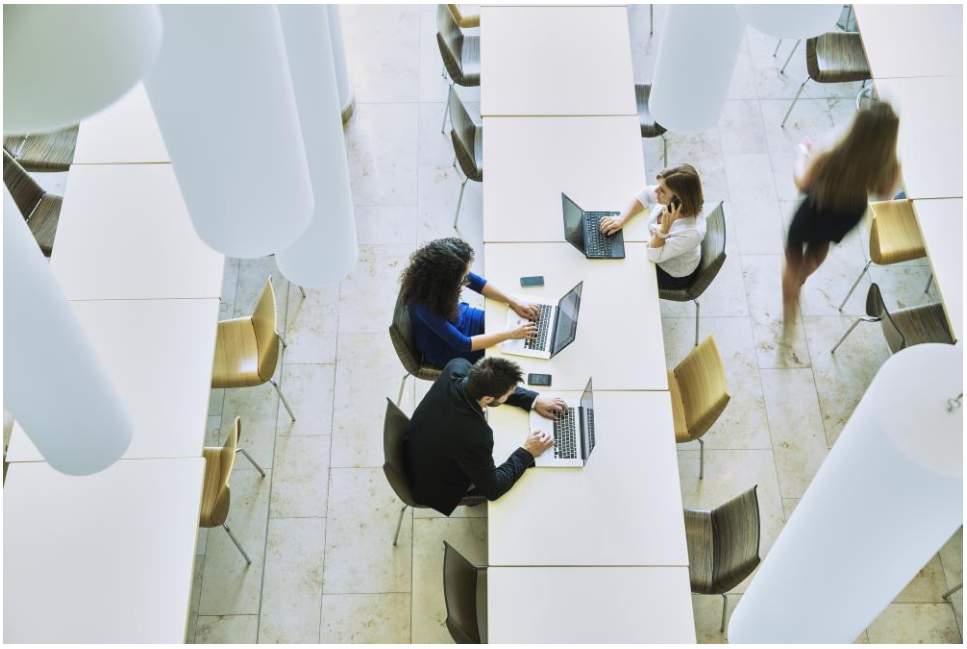
Tan pronto como las empresas fortalecen su postura de seguridad para las computadoras y las redes frente a los ataques de ransomware, los piratas informáticos ponen su atención en la explotación de dispositivos móviles. Los dispositivos móviles cuentan con una pantalla mucho más pequeña y no brindan información completa a primera vista (por ejemplo, el correo electrónico), lo que lleva a que las víctimas hagan clic en enlaces maliciosos. Los ataques de Internet de las cosas (IoT) también van en aumento, ya que el ransomware y la falta de seguridad pueden convertir dispositivos y objetos en puntos de entrada para las herramientas de ransomware. En 2020, los ataques de ransomware dirigidos a dispositivos de IoT aumentaron un 109 % en todo Estados Unidos.

Estos factores, junto con los países que actúan como refugio seguro para los atacantes, han llevado a un aumento de los delitos de ransomware. Hubo un ataque exitoso de ransomware cada 10 segundos en 2020 y, según una encuesta de Anomali Harris Poll, uno de cada cinco estadounidenses es víctima de ataques de ransomware. Por otra parte, según informa Infosecurity Magazine, el método de ataque más popular "fue por lejos el tráfico de botnets (28 %), seguido de los criptomineros (21 %), los ladrones de información (16 %), los dispositivos móviles (15 %) y el malware bancario (14 %)". En respuesta, las empresas se esfuerzan por gastar más dinero en seguridad (USD 150 mil millones en 2021, según Gartner).

Los ataques a personas están disminuyendo a medida que los piratas informáticos apuntan a objetivos específicos más lucrativos. Los proveedores de servicios administrados (MSP) informan un aumento del 85 % en los ataques contra las pymes. Las empresas, junto con las empresas de infraestructura, atención médica, gobierno y fabricación, están siendo atacadas más que nunca, y les exigen millones a cambio de sus datos. El tamaño de un rescate se ha duplicado en el último año a medida que los atacantes atacan a empresas más importantes. Los ataques al software de proveedores, contratistas y terceros también han aumentado considerablemente. Las empresas han tenido que confiar en la seguridad de estas partes externas con acceso a sus sistemas.

El auge de las pandillas de ransomware	El primer caso conocido de ransomware provino de disquetes que contenían encuestas sobre SIDA y malware, distribuidos por todo el mundo en 1989 por el Dr. Joseph Popp. Los discos cifraban archivos en el sistema de la víctima y le negaban el acceso hasta que enviaba un pago de USD 189 a un apartado postal en Panamá. Los CD trampa se distribuyeron luego en la conferencia sobre el SIDA de la Organización Mundial de la Salud. El pago y envío de CD era problemático y costoso.
2006	Los ciberdelincuentes comenzaron a usar una forma más eficaz de encriptación de la clave pública 660 RSA para cifrar archivos más rápidamente. Los grandes jugadores de esa época eran el troyano Archiveus y GPcode, que utilizaba la suplantación de identidad (phishing) por correo electrónico como punto de entrada.
2008–2009	Apareció un nuevo software antivirus cargado con malware de ransomware y un software de seguridad malicioso utilizó FileFix Pro para pedir dinero a cambio del descifrado.
2010	Los bitcoins cambiaron todo el panorama. Se detectaron diez mil variantes de ransomware, a la vez que apareció por primera vez el ransomware de bloqueo de pantalla.
2013	Existían un cuarto de millón de muestras de ransomware, y Cryptolocker y Bitcoin se convirtieron rápidamente en el principal método de pago. El ransomware usó la encriptación RSA de 2048 bits para aumentar las demandas, lo que fue lucrativo para las pandillas.
2015	Apareció el troyano de ransomware Teslacrypt, con lo cual ahora había 4 millones de variantes de ransomware, y se introdujo el ransomware como servicio (RaaS).
2016	El ransomware JavaScript y Locky era popular; Locky infectó a 90 000 víctimas por día. Los atacantes apuntaban a organizaciones más grandes, como hospitales e instituciones académicas. El ransomware alcanzó más de USD 1000 millones en ganancias. El malware Petya causó más de USD 10 mil millones en pérdidas financieras.
2017	El criptogusano WannaCry apareció este año y evolucionó en diversas variantes diariamente, tras lo cual se extendió rápidamente a 300 000 computadoras en todo el mundo a través de una explotación de Microsoft.
2018	Se introdujo Katsuya. SamSam dio de baja varios servicios municipales que afectaron a la ciudad de Atlanta.
2019	REvil, una pandilla privada de RaaS, se originó en Rusia. Ryuk, una variante de ransomware sofisticada y costosa que se incrustó en archivos adjuntos maliciosos y correos electrónicos de

	suplantación de identidad (phishing), exigió pagos más suculentos en comparación con ataques similares y, efectivamente, cerró todos los periódicos más importantes de los EE. UU.
2020	DarkSide, Egregor y Sodinokibi surgieron como jugadores importantes. Ryuk pasó de 1 caso al día a 19,9 millones en septiembre, el equivalente a ocho casos por segundo.
2021	Los kits REvil/Sodinokibi, Conti y Lockbit afectaron notablemente a la atención médica. CryptoLocker obtuvo USD 40 millones del importante proveedor de seguros CNA Financial en uno de los mayores pagos de ransomware hasta el presente. DarkSide logró atacar a Colonial Pipeline Company y marcó el hackeo más grande divulgado públicamente de la infraestructura esencial de los EE. UU.



El perímetro se expande

¿Cómo se tornó tan frecuente el ransomware? Anteriormente, el perímetro era un muro cerrado que administraba aplicaciones y datos centralizados a través de firewalls de la red privada virtual (VPN) y soluciones de administración de dispositivos móviles (MDM), como una suerte de “foso” que rodeaba el castillo de la red. Hoy en día, el trabajo se realiza desde cualquier lugar y cualquier dispositivo (incluidos los dispositivos móviles personales) y es preciso acceder a los datos desde aplicaciones de terceros en la nube. No hay foso, sino muchas entradas al castillo. El surgimiento del trabajo remoto durante la pandemia convirtió el perímetro tradicional en el “perímetro definido por software”. Dada la prisa por mantener a los empleados trabajando, la seguridad fue una idea de último minuto para muchos, lo que ha generado oportunidades de ransomware para los malos actores.

Acceso remoto

Según se indica en las principales tendencias de riesgo y seguridad de Gartner para 2021, el 64 % de los empleados ahora puede trabajar desde casa y dos quintas partes de la fuerza laboral trabajan desde casa. Durante las órdenes obligatorias de quedarse en casa de la pandemia, la mayoría de los trabajadores tenían que trabajar de forma 100 % remota y necesitaban poder hacerlo en sus propios dispositivos mientras accedían a las aplicaciones de SaaS en la nube y en las instalaciones. Muchas empresas no tenían la infraestructura necesaria para soportar este cambio. Hoy, el acceso remoto es la nueva realidad para la fuerza laboral. A medida que las organizaciones se adapten a este estándar de operación, se prevé que la fuerza laboral sea un modelo híbrido de trabajadores remotos y aquellos que retornan a la oficina.

Peter Firstbrook, vicepresidente analista de Gartner, dijo en una publicación de blog: “A medida que la nueva normalidad tome forma, todas las organizaciones necesitarán una postura defensiva siempre conectada, además de claridad sobre los riesgos comerciales que los usuarios remotos elevan para mantenerse seguros”.

Las empresas que no han fortalecido su postura de seguridad para este cambio o mejorado su educación en seguridad interna propician una forma fácil de entrar para los atacantes. Según informa Gartner, el 57 % de las infracciones involucra la negligencia por parte de empleados/terceros. Según ZDNet, el protocolo de escritorio remoto (RDP) es la forma número uno en que los actores de amenazas obtienen acceso a las computadoras con Windows e instalan ransomware y otro malware, seguido por la suplantación de identidad (phishing) por correo electrónico y las vulnerabilidades de errores de VPN.

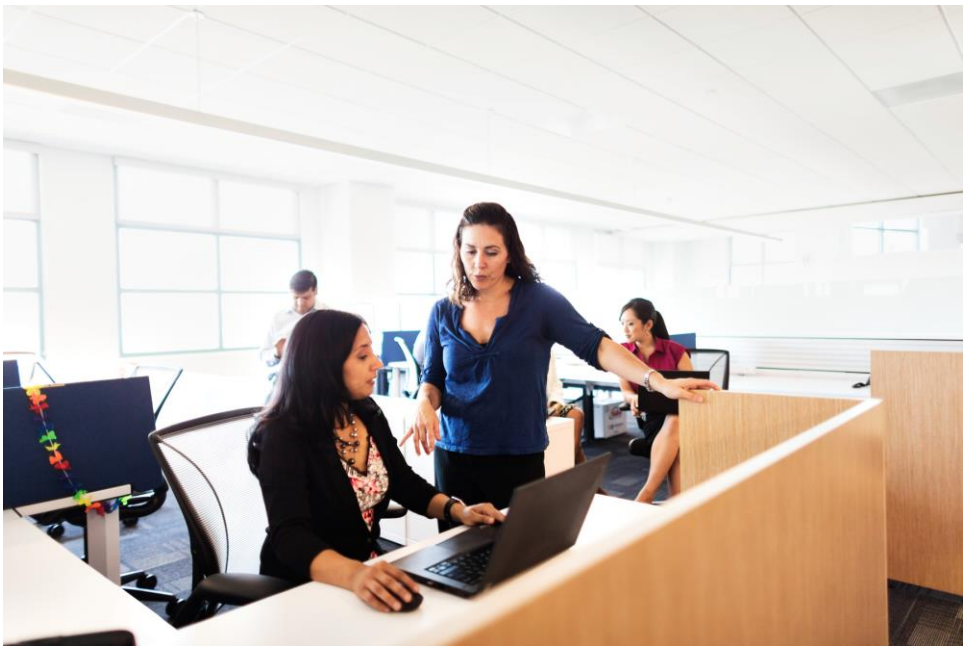
Restricciones de VPN

El hackeo de explotaciones en VPN es el tercer método de entrada más popular para los piratas informáticos de ransomware. El hackeo que cerró Colonial Pipeline Company fue el resultado de una contraseña comprometida de una VPN no utilizada. Si bien las VPN pueden condicionar el acceso a las aplicaciones locales, existe una inconsistencia en el acceso a las aplicaciones en la nube que puede generar vulnerabilidades. Una vez comprometidas, las VPN pueden conducir a un acceso a la puerta trasera de la red donde los piratas informáticos pueden instalar malware en el espacio interno sin interrupciones.

Un enfoque de firewall y VPN en capas de confianza cero con MFA evita el 100 % de los bots automatizados, el 99 % de los ataques masivos de suplantación de identidad (phishing) y el 90 % de los ataques dirigidos, de acuerdo con una investigación de Google.

Terminales sin protección

A medida que más y más dispositivos se conectan a las redes corporativas, la cantidad de dispositivos personales y dispositivos en paralelo ha aumentado. Debido a que es posible que estos dispositivos no estén supervisados o no estén actualizados, pueden conducir potencialmente a infracciones en terminales clave sin ser detectados. A medida que los piratas informáticos buscan meticulosamente una forma de entrar, los terminales desprotegidos, la falta de información sobre quién y qué se conecta a su red y el estado del dispositivo pueden provocar una infracción.



Suplantación de identidad (phishing), ataques dirigidos y vulnerabilidades

¿Qué técnicas se utilizan en los ataques de ransomware? Es un proceso de varios pasos que puede ser relativamente breve o llevarse a cabo durante meses para acceder y cifrar los datos que resultan más valiosos y que causarán el mayor daño si se los retiene como rehenes. Según informa CSOonline.com, el 94 % del malware se envía por correo electrónico y los ataques de suplantación de identidad (phishing) representan más del 80 % de los incidentes de seguridad. Otros puntos de entrada incluyen actualizaciones sin parches y vulnerabilidades de día cero. Casi todos estos comienzan con el robo de credenciales.

Técnicas de ransomware

Ataques de tipo “disparar y rezar” o ataques masivos de suplantación de identidad (phishing)

Los agentes de amenazas adquieren listas de correos electrónicos del mercado negro y, luego, analizan las credenciales y distribuyen correos electrónicos de suplantación de identidad (phishing). Solo se necesitan unas pocas credenciales para tener éxito, las cuales a menudo se adquieren por correo electrónico con archivos adjuntos maliciosos, sitios web fraudulentos que parecen legítimos o una identidad falsa dirigida a empleados de alto valor.

Suplantación de identidad (phishing) focalizada

Este ataque coordinado y dirigido a un grupo específico de usuarios se lleva a cabo mediante el envío de mensajes personalizados y socialmente diseñados que suscitan la curiosidad, el miedo o la recompensa de una fuente legítima. Los correos electrónicos y el sitio web contienen malware que se utiliza para robar credenciales. El malware también se puede propagar a través de las redes sociales y las aplicaciones de mensajería instantánea.

Fuerza bruta

De acuerdo con una encuesta de LastPass, el 91 % de los encuestados admite reutilizar las contraseñas. Los piratas informáticos son muy conscientes de ello y recopilan contraseñas de volcados de credenciales o de la web oscura. Luego, usan herramientas automatizadas para probar contraseñas en diferentes sitios, lo que se denomina “relleno de credenciales” o “fuerza bruta”. Una vez dentro, el ataque puede comenzar.

Explotación de vulnerabilidades conocidas

Además de conocer qué dispositivos se están conectando a su red, conocer también el estado del dispositivo y qué tan actualizado está en cuanto a parches y actualizaciones es importante para mantener un alto perfil de seguridad. Según informes de Security Boulevard: “Los componentes de código abierto obsoletos y ‘abandonados’ son omnipresentes. El 91 % de las bases de código albergaba componentes que tenían más de cuatro años de desactualización o no habían tenido actividad de desarrollo en los últimos dos años”.

Guía paso a paso para un ataque de ransomware

Encriptación del ransomware

Por lo general, los ataques de ransomware cifran los datos en los sistemas de destino y los vuelven inaccesibles hasta que se paga un rescate por el descifrado. La última táctica es la doble encriptación, en la que los piratas cifran un sistema dos veces o dos pandillas diferentes apuntan a la misma víctima. Con este enfoque, los atacantes tienen la oportunidad de cobrar dos rescates al recibir el pago de la primera capa de cifrado y, luego, sorprender a las víctimas con otra capa después de haber cobrado el pago de la primera. La encriptación más común es asimétrica o simétrica.

Coordinación del ataque

En este punto, los piratas informáticos de ransomware hacen su tarea en las empresas específicas a las que apuntan. Pueden adquirir listas de correo electrónico de la web oscura, identificar líderes importantes, leer sobre las finanzas de la empresa, investigar perfiles de redes sociales y compilar una lista de partes interesadas clave, como contratistas, proveedores y socios. ¿Qué tácticas usan los piratas informáticos para entrar? Los tres principales ataques en 2020 se originaron en terminales de RDP mal protegidos, ataques de suplantación de identidad (phishing) por correo electrónico y la explotación de vulnerabilidades de VPN de día cero. La filtración de credenciales es la principal forma en que los malos actores obtienen acceso.

Movimiento vertical

En la fase de infiltración e infección, el movimiento vertical es cuando los actores de amenazas se mueven de una posición externa a una posición interna. Una vez dentro, escanean archivos y ejecutan códigos maliciosos en terminales y dispositivos de red. El malware se mueve a través del sistema infectado y deshabilita los firewalls y el software antivirus. Ahora, los atacantes se han apoderado de los datos, pero estos aún no están cifrados. Los puntos de entrada comunes para el movimiento vertical incluyen cuentas de correo electrónico suplantadas, servidores web de bajo nivel y terminales mal protegidos.

Punto de apoyo lateral

Las amenazas persistentes avanzadas (APT) han aumentado su éxito debido al movimiento lateral. Para establecer un punto de apoyo, los delincuentes tienen que cifrar las computadoras y propagar el ransomware a tantos sistemas como sea posible. Una vez que se obtiene el acceso, comienza la búsqueda de los piratas informáticos. Comienzan a moverse lateralmente, sin ser detectados, durante semanas o meses a través de la red para identificar objetivos clave, como el centro de comando y control (C2), claves asimétricas y archivos de respaldo. Al mismo tiempo, elevan su acceso y permisos debido a que infectan sistemas y cuentas de usuario adicionales y preparan una presencia maliciosa persistente para secuestrar

Extracción de datos

Una vez que se completa la evaluación del inventario, comienza la encriptación. Las copias de seguridad del sistema se eliminan, los archivos y las carpetas locales se dañan, las unidades de red no asignadas se conectan a sistemas infectados y se establece una comunicación con el centro de comando y control para generar las claves criptográficas que se emplean en el sistema local. Los datos de la red se copian localmente, se cifran y, luego, se cargan y reemplazan los datos originales. Los datos extraídos se pueden utilizar para una doble extorsión. En este caso, se exige un rescate para descifrar los datos cifrados y, luego, un segundo rescate para no filtrar los datos robados.

Pago y desbloqueo

Luego, los atacantes activan el malware, bloquean los datos e indican sus demandas de rescate en las ubicaciones comprometidas con instrucciones específicas sobre cómo realizar el pago, que generalmente se realiza en bitcoins. Un golpe de ransomware origina un problema de tiempo de inactividad muy costoso que es extremadamente difícil de resolver. Se lanzan amenazas y comienza la cuenta regresiva. Las empresas tienen que decidir si quieren recibir el golpe y pagar, tratar de restaurar sus archivos por su cuenta o usar su seguro de ciberseguridad, que solo recuperará una parte del rescate. Es una elección entre malas opciones, por lo que es preciso que las organizaciones implementen una arquitectura de

		
Punto de apoyo lateral	**Extracción de datos**	**Pago y desbloqueo**
datos. Algunos ejemplos de movimiento lateral incluyen la explotación de servicios remotos, la suplantación de identidad (phishing) interna y el uso de contraseñas robadas, también conocido como “pasar el hash”.		confianza cero y tengan mejores prácticas de seguridad para evitar esta situación en lo sucesivo.

Industrias vulnerables

La atención médica, los municipios y el gobierno, así como el comercio minorista, la educación y las finanzas, son las industrias más afectadas por los ataques de ransomware. Estas industrias cuentan con soluciones heredadas complejas y es posible que no aprovechen una sólida seguridad en la nube. La atención médica, la educación y el gobierno tardan en adaptar su postura de seguridad con actualizaciones y nuevas tecnologías, lo que los vuelve objetivos lucrativos y fáciles.

Detención del grado de compromiso del ransomware antes de que comience

En un ataque de ransomware, los atacantes primero deben obtener acceso. Pueden hacerlo mediante la filtración de credenciales, como fue el caso en la violación que sufrió Colonial Pipeline.

La autenticación de varios factores (MFA) de Duo puede ayudar a evitar que el ransomware obtenga acceso en primer lugar. La MFA requiere que un usuario presente una combinación de dos o más credenciales para verificar su identidad para iniciar sesión. Por ejemplo, además de un nombre de usuario y contraseña, Duo MFA solicita algo propio, como un dispositivo confiable o un token de software o hardware, antes de otorgar acceso a los recursos. Gracias a este requisito adicional, la MFA hace que sea mucho más difícil para el ransomware obtener ese punto de apoyo inicial.

El ransomware también es proclive a usar servicios remotos, como el protocolo RDP y VPN, para obtener acceso a una red. Se sospecha que DarkSide, el presunto perpetrador del ataque de Colonial Pipeline, usó el acceso a la VPN corporativa para ingresar al entorno de la víctima. Además de la MFA, Duo MFA, Duo Device Trust, Duo Network Gateway (DNG) y Duo Trust Monitor se combinan en una solución de acceso confiable y pueden ayudar a proteger el acceso remoto a la infraestructura local y evitar que el ransomware obtenga acceso en primer lugar.

Duo MFA requiere más que un nombre de usuario y una contraseña para autenticarse. DNG permite a los usuarios acceder a sitios web locales, aplicaciones web, servidores SSH y RDP sin tener que preocuparse por las credenciales de VPN. Duo Device Trust garantiza que el dispositivo que accede de forma remota a los recursos sea una computadora confiable y no el dispositivo de un atacante. Por último, Duo Trust Monitor llama la atención sobre las solicitudes de autenticación que parecen sospechosas, como las que se originan en países donde se sabe que los actores de ransomware están activos y países donde una organización no tiene empleados.

El uso de malware también es una técnica popular de infección de ransomware. Cisco proporciona soluciones complementarias adicionales, como Secure Endpoint y Email Gateway, que pueden inspeccionar, detectar y bloquear ransomware basado en malware antes de que infecte los terminales.

Cómo ayuda Duo a protegerse contra el ransomware

Gartner informa que el 90 % del ransomware se puede prevenir. Duo está en una posición única para ayudar a las organizaciones en tres frentes:

1. Evitar que el ransomware obtenga un punto de apoyo inicial en un entorno.
2. Evitar o ralentizar la propagación de ransomware si logra infiltrarse en una organización.
3. Proteger activos críticos y partes de la organización mientras un atacante todavía tiene presencia en el entorno y hasta tanto se logre la remediación completa.

Cómo defenderse de la propagación

El ransomware que afecta a una pequeña cantidad de sistemas tiene un impacto limitado y es poco probable que haga que una organización se detenga y quiera pagar un rescate. Por eso la propagación de ransomware es crucial para derribar de manera eficaz una parte significativa de una organización y obligarla a pagar el rescate para que vuelva rápidamente al negocio. En 2017, WannaCry y NotPetya utilizaron la explotación de External Blue para aprovechar una vulnerabilidad de Microsoft y propagarla sin la intervención del usuario.

La aplicación Device Health Duo puede mantener los dispositivos con parches y actualizados, lo que dificulta que el ransomware se propague automáticamente. Además, ofrece visibilidad a la vez que verifica el estado de salud del dispositivo, incluido qué tan actualizado está el dispositivo, en cada intento de inicio de sesión. Y con la capacidad de autocorrección de Duo, los usuarios pueden mantener sus dispositivos con parches fácilmente sin la ayuda de TI.

Reparación en la seguridad

Recuperarse de un ataque de ransomware y volver a poner los sistemas en línea no significa, necesariamente, que el atacante haya abandonado el entorno. El atacante podría haber intentado establecer la persistencia para volver más tarde. Una técnica común es comprometer las cuentas existentes o crear cuentas nuevas, a menudo mediante el acceso a Active Directory u otros directorios que contienen cuentas de usuarios. Duo MFA puede brindarle la tranquilidad de saber que un atacante que todavía está en la red no puede pivotar y moverse lateralmente con facilidad con credenciales filtradas. También puede hacerle ganar tiempo y evitar que un atacante cause más daño mientras el ataque se repara por completo, eliminando así todo rastro de persistencia.

Implementación de un modelo de seguridad de Zero Trust

Basado en el principio de “nunca confíe, siempre verifique”, Zero Trust es un modelo de seguridad que puede ayudar a las organizaciones a implementar de manera proactiva las mejores prácticas conocidas para protegerse contra los ataques cibernéticos, incluido el ransomware.

Zero trust es tan importante que la Casa Blanca emitió una orden ejecutiva que exige específicamente la confianza cero y la MFA.

Duo ofrece una MFA fácil de usar e implementar. También permite a las organizaciones otorgar acceso solo si se puede verificar y confiar en un usuario y su dispositivo. Esta capacidad de controlar y administrar el acceso es uno de los pilares fundamentales de la confianza cero y Duo MFA es uno de los primeros pasos para implementar un marco de confianza cero.

Conclusión

El ransomware será más frecuente y las empresas deben estar más atentas. La ingeniería social y la suplantación de identidad focalizada tienen éxito, ya que explotan el elemento humano de la seguridad de una organización. Adoptar e implementar una filosofía de seguridad de confianza cero que comience con una MFA sólida y una plataforma de acceso confiable es importante para anticiparse a los ataques de ransomware.

Actualice su defensa más allá del MFA con Duo

Las organizaciones pueden defenderse contra el impacto del ransomware a través de ataques de suplantación de identidad (phishing) sociales y dirigidos mediante la implementación de políticas de acceso condicional, las cuales se sirven de los factores contextuales, como la ubicación y la postura del dispositivo, para establecer la confianza en los usuarios y sus dispositivos.

La plataforma de seguridad basada en la nube de Duo protege el acceso a todas las aplicaciones para cualquier usuario y dispositivo, desde cualquier lugar. Hemos simplificado el acceso seguro para abordar los riesgos de identidad y dispositivos con seis capacidades críticas:

1. Verifique las identidades de los usuarios con métodos de autenticación de varios factores seguros y flexibles.
2. Proporcione una experiencia de inicio de sesión coherente con el inicio de sesión único de Duo, que confiere acceso centralizado a las aplicaciones en las instalaciones y en la nube.
3. Obtenga visibilidad en cada dispositivo y mantenga un inventario detallado de todos los dispositivos que acceden a las aplicaciones corporativas.
4. Establezca confianza en los dispositivos a través de verificaciones de estado y postura para dispositivos administrados o no administrados antes de proporcionar acceso a la aplicación.
5. Ponga en marcha políticas de acceso granular para limitar el acceso a aquellos usuarios y dispositivos que cumplan con los niveles de tolerancia al riesgo de la organización.
6. Supervise y detecte el comportamiento de inicio de sesión riesgoso mediante Duo Trust Monitor, o exporte registros a su SIEM, para remediar eventos sospechosos, como la inscripción de un nuevo dispositivo para la autenticación o el inicio de sesión desde una ubicación inesperada.

¿Por qué optar por Duo?

Velocidad para la seguridad

Duo ofrece los componentes básicos de la confianza cero en una solución que es rápida y fácil de implementar para los usuarios. Dependiendo de su caso práctico específico, algunos clientes pueden estar ejecutándose en cuestión de minutos.

Facilidad de uso

Los usuarios pueden autoinscribirse; simplemente deben descargar una aplicación de la tienda de aplicaciones e iniciar sesión. Los controles de mantenimiento y las políticas son fáciles de controlar para los administradores, que obtienen una visibilidad clara.

Integración con todas las aplicaciones

Nuestro producto está diseñado para ser agnóstico y funcionar con sistemas heredados. Independientemente de los proveedores de TI y seguridad que utilice, con Duo también puede asegurar el acceso a todas las aplicaciones de trabajo para todos los usuarios, desde cualquier lugar.

Menor costo total de propiedad (TCO)

Debido a que Duo es fácil de implementar y no requiere reemplazar sistemas, exige muchos menos recursos en tiempo y costo, lo que lo pone en funcionamiento rápidamente y comienza el viaje hacia un modelo de seguridad de confianza cero.

Referencias

The Pandemic-hit World Witnessed a 150% Growth of Ransomware (Aumento del 150 % del ransomware en el mundo pospandemia), https://cisomag.eccouncil.org/growth-of-ransomware-2020/, CISO Magazine, 5 de marzo de 2021

Exclusive: U.S. to give ransomware hacks similar priority as terrorism (Exclusiva: Los EE. UU. darían a los ataques de ransomware casi la misma prioridad que a los ataques terroristas), https://www.reuters.com/technology/exclusive-us-give-ransomware-hacks-similar-priority-terrorism-official-says-2021-06-03/, Reuters, 3 de junio de 2021

NIST Announces Tech Collaborators on NCCoE Zero Trust Project (NIST anuncia a los colaboradores tecnológicos del proyecto de confianza cero de NCCoE), https://www.hstoday.us/industry/emerging-innovation/nist-announces-tech-collaborators-on-nccoe-zero-trust-project/, Homeland Security Today, 24 de septiembre de 2021

FICHA TÉCNICA: Ongoing Public U.S. Efforts to Counter Ransomware (Iniciativas públicas en curso de los EE. UU. para contrarrestar el ransomware), https://www.whitehouse.gov/briefingroom/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware, la Casa Blanca, 13 de octubre de 2021

Types of Encryption: Symmetric or Asymmetric? RSA or AES? (Tipos de cifrado: ¿simétrico o asimétrico? ¿RSA o AES?), https://preyproject.com/blog/en/types-ofencryption-symmetric-or-asymmetric-rsa-or-aes/, Prey Project, 15 de junio de 2021

What We Know About DarkSide, the Russian Hacker Group That Just Wreaked Havoc on the East Coast (Lo que sabemos sobre DarkSide, el grupo de hackers ruso que ha hecho estragos en la costa este), https://www.heritage.org/cybersecurity/commentary/what-we-know-about-darkside-the-russian-hackergroup-just-wreaked-havoc, The Heritage Foundation, 20 de mayo de 2021

What We Can Learn From Ransomware Actor "Security Reports" (Qué podemos aprender de los "informes de seguridad" de los atacantes de ransomware), https://www.coveware.com/blog/2021/6/24/what-we-can-learn-from-ransomware-actor-security-reports, Coveware, 24 de junio de 2021

The State of Ransomware 2021 (Estado del ransomware en 2021), https://secure2.sophos.com/en-us/content/state-of-ransomware.aspx, Sophos, 2021

Data Mining Process: The Difference Between Data Mining & Data Harveting (Proceso de minería de datos: La diferencia entre la minería de datos y la recolección de datos), https://www.import.io/post/the-difference-between-data-mining-data-harvesting, Import.io, 23 de abril de 2019

Ransomware: Enemy at The Gate (Ransomware: el enemigo más próximo), https://ussignal.com/blog/ransomware-enemy-at-the-gate, US Signal, 3 de septiembre de 2021

2020 Data Breach Investigations Report (Reporte de investigaciones sobre vulneración de datos de 2020), https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2020-data-breach-investigations-report.pdf, Verizon, 2020

Malware is down, but IoT and ransomware attacks are up (El malware está en baja, pero los ataques de ransomware y la IoT están en alza), https://www.techrepublic.com/article/malwareis-down-but-iot-and-ransomware-attacks-are-up/, Tech Republic, 23 de junio de 2020

One Ransomware Victim Every 10 Seconds in 2020 (Una víctima de ransomware cada 10 segundos en 2020), https://www.infosecurity-magazine.com/news/oneransomware-victim-every-10/, Infosecurity Magazine, 25 de febrero de 2021

Terrifying Statistics: 1 in 5 Americans Victim of Ransomware (Estadísticas aterradoras: 1 de cada 5 estadounidenses es víctima del ransomware), https://sensorstechforum.com/1-5-americansvictim-ransomware/, Sensors Tech Forum, 19 de agosto de 2019

Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed $150 Billion in 2021 (Gartner pronostica que el gasto en administración de riesgos y seguridad mundial superará los 150 000 millones de dólares en 2021), https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwidesecurity-and-risk-managem, Gartner, 17 de mayo de 2021

1 in 5 SMBs have fallen victim to a ransomware attack (Una de cada cinco pymes ha sido víctima de un ataque de ransomware), https://www.helpnetsecurity.com/2019/10/17/smbsransomware-attack/, Help Net Security, 17 de octubre de 2019

Ransomware – how to stop this growing, major cause of downtime (Ransomware: cómo detener esta importante causa de tiempo de inactividad en crecimiento), https://polyverse.com/blog/ransomware-how-to-stop-this-growing-major-cause-of-downtime, Polyverse.com

The strange history of ransomware (La extraña historia del ransomware), https://theworld.org/stories/2017-05-17/strange-history-ransomware, PRI The World, 17 de mayo de 2017

Ransomware Timeline (Línea de tiempo del ransomware), https://www.tcdi.com/ransomware-timeline, tcdi.com, 27 de diciembre de 2017

A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time (Historial de los ataques de ransomware: los mayores y peores ataques de ransomware de todos los tiempos), https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time, Digital Guardian, 2 de diciembre de 2020

One of the biggest US insurance companies reportedly paid hackers $40 million ransom after a ciberattack (Una de las empresas aseguradoras más grandes de EE. UU. habría pagado USD 40 millones de rescate a hackers tras un ciberataque), https://www.businessinsider.com/cna-financial-hackers-40-million-ransom-cyberattack-2021-5, Business Insider, 22 de mayo de 2021

Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Scare (Atlanta gasta 2,6 millones de dólares para recuperarse de un susto por ransomware de 52 000 dólares), https://www.wired.com/story/atlantaspent-26m-recover-from-ransomware-scare, Wired.com, 23 de abril de 2018

Cyber-attack: US and UK blame North Korea for WannaCry (Ciberataque: los EE. UU. y el Reino Unido culpan a Corea del Norte por WannaCry), https://www.bbc.com/news/world-uscanada-42407488, BBC.com, 19 de septiembre de 2017

Ransomware: Now a Billion Dollar a Year Crime and Growing (Ataques de ransomware: delitos por mil millones de dólares al año y en ascenso), https://www.nbcnews.com/tech/security/ransomware-now-billion-dollar-year-crime-growing-n704646, NBCNews.com, 9 de enero de 2017

The Untold Story of NotPetya, the Most Devastating Cyber Attack in History (La historia jamás contada de NotPetya, el ciberataque más devastador de la historia), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world, Wired.com, 22 de agosto de 2018

Ransomware in Healthcare Facilities: The Future is Now (Ransomware en instalaciones de atención médica: el futuro es hoy), https://mds.marshall.edu/cgi/viewcontent.cgi?article=1185&context=mgmt_faculty, Marshall University Digital Scholar, otoño de 2017

New ransomware holds Windows files hostage, demands $50 (Nuevo ataque de ransomware exige rescate de USD 50 por archivos de Windows), https://www.networkworld.com/article/2265963/new-ransomware-holds-windows-files-hostage--demands--50.html, NetworkWorld.com, 26 de marzo de 2009

Preventing Digital Extortion (Cómo prevenir la extorsión digital), https://subscription.packtpub.com/book/networking_and_servers/9781787120365/4/ch04lvl1sec24/the-advancement-of-locker-ransomware-winlock, PackIt, mayo de 2017

The Irreversible Effects of Ransomware Attack (Los efectos irreversibles de un ataque de ransomware), https://www.crowdstrike.com/blog/irreversible-effectsransomware-attack, CrowdStrike, 20 de julio de 2016

New Era of Remote Working Calls for Modern Security Mindset, Finds Thales Global Survey of IT Leaders (Encuesta global de Thales a líderes de TI revela que la nueva era del trabajo remoto requiere una mentalidad moderna en materia de seguridad), https://www.businesswire.com/news/home/20210914005014/en/New-Era-of-Remote-Working-Calls-for-Modern-Security-Mindset-Finds-Thales-Global-Survey-of-IT-Leaders, Business Wire, 14 de septiembre de 2021

FBI sees spike in cyber crime reports during coronavirus pandemic (El FBI percibió un aumento pronunciado en los ciberdelitos reportados durante la pandemia de coronavirus), https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic, The Hill, 16 de abril de 2020

Symantec Security Summary (Resumen de seguridad de Symantec), https://symantec-enterprise-blogs.security.com/blogs/featurestories/symantec-security-summary-september-2021, Symantec Security, 27 de septiembre de 2021

INTERPOL report shows alarming rate of cyberattacks during COVID-19 (Reporte de INTERPOL muestra una tasa alarmante de ciberataques durante la pandemia de COVID-19), https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19, Interpol, 4 de agosto de 2020

Gartner Top Security and Risk Trends for 2021 (Tendencias principales en seguridad y riesgos de Gartner para el 2021), https://www.gartner.com/smarterwithgartner/gartner-topsecurity-and-risk-trends-for-2021, Gartner, 5 de abril de 2021

Gartner Survey Reveals 82% of Company Leaders Plan to Allow Employees to Work Remotely Some of the Time (Una encuesta de Gartner revela que el 82 % de los líderes empresariales planea permitir que los empleados trabajen de forma remota parte del tiempo), https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time, Gartner, 14 de julio de 2020

Gartner Highlights Identity-First Security as a Top Security Trend for 2021 (Gartner destaca la iniciativa que prioriza la identidad como principal tendencia de seguridad para 2021), https://www.attivonetworks.com/blogs/gartner-identity-first-security-in-2021, Attivo, 27 de abril de 2021.

2021 SonicWall Cyber threat Report (Informe sobre amenazas cibernéticas de SonicWall 2021), https://www.sonicwall.com/medialibrary/en/white-paper/2021-cyberthreat-report.pdf, SonicWall, 2021

Top exploits used by ransomware gangs are VPN bugs, but RDP still reigns supreme (Los errores de VPN son una de las principales vulnerabilidades que explotan las pandillas de ransomware, pero los ataques de RDP siguen siendo los más comunes), https://www.zdnet.com/article/top-exploits-used-by-ransomware-gangs-are-vpn-bugs-but-rdp-still-reigns-supreme, ZDNet.com, 23 de agosto de 2020

VPN exploitation rose in 2020, organizations slow to patch critical flaws (La explotación de vulnerabilidades de VPN aumentó en 2020; las organizaciones demoran mucho en aplicar parches para fallas críticas), https://www.cybersecuritydive.com/news/trustwave-network-security-remote-access/602044/, Cybersecurity Dive, 18 de junio de 2021

New research: How effective is basic account hygiene at preventing hijacking (Investigación nueva: eficacia de la higiene de cuenta básica para prevenir el hackeo), https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html, Google Blog, 17 de mayo de 2019

Top cybersecurity statistics, trends, and facts (Estadísticas, tendencias y datos principales en materia de seguridad cibernética), https://www.csoonline.com/article/3634869/top-cybersecuritystatistics-trends-and-facts.html, CSOonline.com, 7 de octubre de 2021

Protecting Companies From Cyberattacks (Cómo proteger a las empresas de los ataques cibernéticos), https://www.inc.com/knowbe4/protecting-companies-fromcyberattacks.html, Inc.com, 20 de septiembre de 2021

ThreatList: People Know Reusing Passwords Is Dumb, But Still Do It (ThreatList: La gente sabe que reutilizar contraseñas es mala idea, pero lo sigue haciendo), https://threatpost.com/threatlistpeople-know-reusing-passwords-is-dumb-but-still-do-it/155996/, Threatpost, 25 de mayo de 2020

Synopsys Study Shows 91% of Commercial Applications Contain Outdated or Abandoned Open Source Components (Estudio de Synopsys muestra que el 91 % de las aplicaciones comerciales contiene componentes de código abierto desactualizados o abandonados), https://www.securitymagazine.com/articles/92368-synopsys-study-shows-91-ofcommercial-applications-contain-outdated-or-abandoned-open-source-components, Security Magazine, 12 de mayo de 2020

Ransomware's Dangerous New Trick Is Double-Encrypting Your Data (Los nuevos ataques de ransomware hacen una doble encriptación de los datos), https://www.wired.com/story/ransomware-double-encryption/, Wired.com, 17 de mayo de 2021

Combating Lateral Movement and the Rise of Ransomware (La lucha contra el movimiento lateral y el auge del ransomware), https://www.msspalert.com/cybersecurityguests/combating-lateral-movement-and-the-rise-of-ransomware, MSSP Alert, 24 de junio de 2021

Lateral Movement (Movimiento lateral), https://attack.mitre.org/tactics/TA0008/, MITRE| ATT&CK, 17 de octubre de 2019

Industries Impacted by Ransomware (Industrias afectadas por el ransomware), https://airgap.io/blog/industries-impacted-by-ransomware, AirGap.com

Defend Against and Respond to Ransomware Attacks (Defensa y respuesta ante ataques de ransomware), https://www.gartner.com/en/documents/3978727/defend-against-and-respond-to-ransomware-attacks, Gartner Research, 26 de diciembre de 2019

Executive Order on Improving the Nation's Cybersecurity (Orden ejecutiva sobre la mejora de la seguridad cibernética del país), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/, la Casa Blanca, 12 de mayo de 2021

Sede central en América
Cisco Systems, Inc.
San José. CA

Sede Central en Asia Pacífico
Cisco Systems (EE. UU.) Pte. Ltd.
Singapur

Sede Central en Europa
Cisco Systems International BV Amsterdam.
Países Bajos

Cisco cuenta con más de 200 oficinas en todo el mundo. Las direcciones, los números de teléfono y de fax están disponibles en el sitio web de Cisco: **www.cisco.com/go/offices**.

Impreso en EE. UU. C11-3233828-00 10/22