cisco SECURE

PROTECCIÓN CONTRA

ransomware

Seguridad de confianza cero para el personal moderno

PROTECCIÓN CONTRA

ransomware

Seguridad de confianza cero para el personal moderno

CONTENIDO

EL RANSOMWARE LLEGÓ PARA QUEDARSE	1
AMPLIACIÓN DEL PERÍMETRO	5
SUPLANTACIÓN DE IDENTIDAD, ATAQUES ESPECIALIZADOS Y VULNERABILIDADES	6
GUÍA PASO A PASO DE UN ATAQUE DE RANSOMWARE	7
CÓMO DETENER LOS PELIGROS DEL RANSOMWARE ANTES DE QUE SE PRODUZCAN	9
CONCLUSIÓN	10
REFERENCIAS	12

© 2021 Cisco Systems, Inc. y/o sus filiales. Todos los derechos reservados.

El ransomware llegó para quedarse

El ransomware evolucionó rápidamente como estrategia de ataque. Antes se trataba de la captura hostil de computadoras aisladas; ahora, los riesgos son mayores. Los actores malintencionados lanzan ataques cada vez más agresivos a los objetivos geopolíticos, los sistemas de empresas e infraestructuras esenciales (por ejemplo, objetivos grandes), lo que podría causar daños sin precedentes. En la actualidad, el ransomware es una de las principales amenazas de ciberseguridad, tras un aumento del 150 % en 2020 debido al cambio repentino al trabajo remoto.

El ransomware ahora se considera ciberterrorismo, y una orden ejecutiva reciente del presidente estadounidense Joe Biden confirma que se deben tomar medidas inmediatas para proteger los sistemas. El enfoque de confianza cero es la norma por excelencia para protegerse contra el ransomware. El Instituto Nacional de Normas y Tecnología (NIST) de los Estados Unidos manifestó: “Implementar una arquitectura de confianza cero se ha convertido en una obligación de ciberseguridad y una necesidad empresarial”.

En la hoja informativa de la Casa Blanca sobre el tema se afirma: “Los incidentes recientes relacionados con la ciberseguridad, como los casos de SolarWinds, Microsoft Exchange y Colonial Pipeline, son un recordatorio aleccionador de que las entidades estadounidenses de los sectores público y privado enfrentan cada vez más ciberactividad maliciosa de parte de atacantes de estados nacionales y ciberdelincuentes”.

> "Los incidentes recientes relacionados con la ciberseguridad, como los casos de SolarWinds, Microsoft Exchange y Colonial Pipeline, son un recordatorio aleccionador de que las entidades estadounidenses de los sectores público y privado enfrentan cada vez más ciberactividad maliciosa de parte de atacantes de estados nacionales y ciberdelincuentes".
>
> **Hoja informativa de la Casa Blanca de Estados Unidos de América**.

¿Qué es el ransomware?

En términos simples, el ransomware es el uso de varias tácticas para atacar a los usuarios, principalmente, mediante infecciones por malware, que en general comienzan con un ataque de suplantación de identidad por correo electrónico, una contraseña robada o un ataque de fuerza bruta. Un ataque de ransomware puede consistir en cifrar los archivos o las carpetas, evitar el acceso de sistema al disco duro y manipular el registro de arranque principal para interrumpir el proceso de arranque del sistema. Una vez que el malware se ha instalado y propagado, los hackers pueden acceder a datos sensibles y datos de respaldo para cifrarlos con el objetivo de pedir un rescate (de ahí el término en inglés, ransom) por la información. Los hackers pueden actuar rápidamente o pasar meses infiltrados sin ser detectados para entender la infraestructura de red antes de lanzar un ataque.

La usurpación de datos está destinada a intimidar con urgencia a las víctimas. La información queda inaccesible hasta que se reciba el pago (generalmente en Bitcoin). Aún después de pagar el rescate, es posible que no se devuelvan todos los datos. Hay muchas variantes de ransomware, pero los ataques de criptoransomware son los más frecuentes. Debido al polimorfismo (malware que cambia constantemente), hay muchas variantes para evitar la detección.

Los ataques de criptoransomware que bloquean los datos están mejorando rápidamente. En 2006, los ataques de ransomware usaban 56 bits con encriptación casera. La versión avanzada actual del ransomware usa algoritmos simétricos AES y encriptación con clave pública RSA o ECC para bloquear los datos.

El ransomware madura hasta convertirse en un negocio

A medida que el ransomware cobra más relevancia, se ha convertido en un negocio profesional para las organizaciones delictivas (principalmente de China, Rusia, Corea del Norte y Europa Oriental) que se dedican a seleccionar y atacar a objetivos de alto valor para extraer dinero a cambio de los datos. Para hacerlo con eficacia, estas organizaciones han llegado a crear centros de atención telefónica para orientar a las víctimas en el proceso de compra de Bitcoin y de pago del rescate. Algunos, incluso, reciben felicitaciones por la buena atención a las víctimas.

En algunos casos, para incentivar al pago, los atacantes proporcionan un "reporte de seguridad" paso a paso que detalla exactamente cómo realizaron el ataque tras el pago del rescate. Lo más lógico es que estos delincuentes desencripten los archivos a cambio del dinero para preservar su reputación para la próxima víctima, pero esto no siempre pasa. El reporte *Estado del ransomware en 2021* de Sophos indica que a solo un 8 % de las víctimas les devuelven los datos y que un 29 % recuperan más de la mitad de los datos. En ocasiones, los datos se recopilan y se venden a otros atacantes, o se guardan para pedir otro rescate en el futuro.

En años recientes, los atacantes malintencionados han creado el ransomware como servicio (RaaS), una solución totalmente integrada y lista para usar que permite que cualquier persona lance un ataque de ransomware por más que no sepa programar. Al igual que los productos de software como servicio (SaaS), RaaS da un acceso relativamente económico y simple a estos programas maliciosos por un cargo menor al costo de crear uno propio. Los proveedores de RaaS suelen quedarse con entre un 20 % y un 30 % de las ganancias del rescate. Ahora hay modelos de suscripción y de afiliados para realizar los ataques con éxito. El grupo de hackers REvil tenía un modelo de afiliados en el que compartían las ganancias con cualquier persona que contribuyera al éxito de un ataque de ransomware. Este modelo llevó a un aumento drástico del volumen de los ataques de ransomware.

Otra tendencia —atribuida por primera vez a la pandilla Maze— es la doble extorsión, mediante la cual los hackers amenazan con publicar la información robada en la dark web o en Internet si no se cumplen sus demandas. Cuentan con una infraestructura incorporada para manejar estas divulgaciones de datos, según el *Reporte de investigación sobre robo de datos de 2020* de Verizon. La táctica de "nombrar y humillar" ahora es popular entre la mayoría de las pandillas que realizan ataques de ransomware, al igual que el modelo de "multa", en el que el precio aumenta a medida que pasa el tiempo.

A medida que las empresas fortalecen su postura de seguridad para las computadoras y las redes ante los ataques de ransomware, los hackers ahora vuelcan su atención a explotar las vulnerabilidades de los dispositivos móviles. Los dispositivos móviles tienen una pantalla mucho más pequeña y no proporcionan toda la información a primera vista —del correo electrónico, por ejemplo—, lo que facilita que las víctimas hagan clic en enlaces maliciosos. Los ataques a través del Internet de las cosas (IoT) también están en aumento, ya que el ransomware y la falta de seguridad pueden convertir los dispositivos y los objetos en puntos de entrada para herramientas de ransomware. En 2020, los ataques de ransomware orientados a dispositivos de IoT aumentaron en un 109 % en todo EE. UU.

Estos factores, sumados a los países que actúan como refugio seguro para los atacantes, han llevado a un aumento de los ataques de ransomware. En 2020, hubo un ataque de ransomware exitoso cada 10 segundos y, según una encuesta de Anomali Harris Poll, uno de cada cinco estadounidenses son víctimas de ataques de ransomware. Sobre el tema, Infosecurity Magazine informa que el método de ataque más popular "fue, por mucho, el tráfico de botnets (28 %), seguido de la criptominería (21 %), el robo de información (16 %), y malware móvil (15 %) y malware bancario (14 %)." Como respuesta a esto, las empresas se apuraron a invertir más en seguridad (USD 150.000 millones en 2021, según Gartner).

Los ataques a individuos están disminuyendo a medida que los hackers se centran en objetivos específicos más lucrativos. Los prestadores de servicios administrados (MSP) han informado de un aumento del 85 % en los ataques contra PYMES. Los ataques se dirigen cada vez más a las grandes empresas de infraestructura, atención médica, fabricantes, así como agencias del gobierno, acompañados de pedidos de rescates millonarios a cambio de los datos. El monto de los rescates se ha duplicado en el último año, desde que los ataques se dirigen a empresas más grandes. Los ataques a proveedores, contratistas y software de terceros también aumentaron considerablemente. Las empresas han tenido que confiarles la seguridad a terceros externos que tienen acceso a sus sistemas.

El avance de las pandillas de ransomware

	La primera instancia conocida de ransomware fue en 1989; se trataba de unos discos flexibles que tenían encuestas sobre SIDA y malware, distribuidos por todo el mundo por el Dr. Joseph Popp. Estos discos cifraban los archivos del sistema de la víctima y denegaban el acceso hasta que se enviara un pago de USD 189 a una casilla postal en Panamá. Los CD de señuelo se distribuyeron en la conferencia sobre el SIDA de la Organización Mundial de la Salud. Los pagos y el envío de CD eran problemáticos y costosos.
2006	Los ciberdelincuentes empezaron a usar una forma más eficaz de encriptación con clave pública RSA 660 para cifrar los archivos más rápido. Los protagonistas de esa época eran el troyano Archiveus y el código GPcode, que usaban la suplantación de identidad por correo electrónico como punto de entrada.
2008-2009	Aparece el nuevo software antivirus con malware de ransomware, y el software de seguridad malicioso usaba FileFix Pro para pedir un rescate por el descifrado.
2010	Bitcoin cambió todo. Se detectaron decenas de miles de variantes de ransomware; aparecieron los ataques de ransomware con bloqueo de pantalla.
2013	Había un cuarto de millón de muestras de ransomware, y Cryptolocker y Bitcoin se convirtieron rápidamente en el método de pago principal. El ransomware usaba encriptación RSA de 2048 bits para exigir rescates más cuantiosos, lo que fue muy lucrativo para las pandillas.
2015	Apareció el troyano de ransomware TeslaCrypt; ya había 4 millones de variantes de ransomware; surgió el ransomware como servicio (RaaS).
2016	Se popularizaron los ataques de ransomware con JavaScript y Locky, que infectaba a 90 000 víctimas por día. Los atacantes orientaban los ataques a organizaciones más grandes, como hospitales e instituciones académicas. El ransomware alcanzó ganancias de más de USD 1000 millones. El malware Petya provocó pérdidas financieras de USD 10 mil millones.
2017	Este año apareció el criptogusano WannaCry, del que se generaban diversas variantes a diario, y rápidamente se propagó a 300 000 computadoras de todo el mundo aprovechando una vulnerabilidad de Microsoft.
2018	Apareció Katsuya. SamSam causó la interrupción de varios servicios municipales, lo que afectó a la ciudad de Atlanta.
2019	Apareció REvil, una pandilla privada de RaaS de Rusia. Ryuk, una variante de ransomware sofisticada y costosa incorporada en archivos adjuntos maliciosos y mensajes de correo electrónico de suplantación de identidad, exigía mayores pagos que los ataques similares y causó el cierre efectivo de los principales periódicos de EE. UU.
2020	Darkside, Egregor y Sodinokibi surgieron como los principales protagonistas. Ryuk pasó de un caso por día a 19,9 millones en septiembre, lo que equivale a ocho casos por segundo.
2021	Los kits de REvil/Sodinokibi, Conti y Lockbit afectaron mucho al sector de atención médica. CryptoLocker obtuvo USD 40 millones del importante proveedor de seguros CNA Financial en uno de los mayores pagos de rescate por ransomware que se conocen a la fecha. DarkSide atacó con éxito a la empresa Colonial Pipeline Company en el hackeo más importante de infraestructura esencial de EE. UU. de divulgación pública.

Se expande el perímetro

¿Cómo se difundió tanto el ransomware? Antes, el perímetro era como un muro que protegía las aplicaciones y los datos centralizados mediante redes privadas virtuales (VPN), firewalls y soluciones de administración de dispositivos móviles (MDM), como un foso que rodea un castillo, que sería la red. En la actualidad, las actividades laborales se realizan desde cualquier lugar y con cualquier dispositivo —incluidos los dispositivos móviles personales—, y se debe acceder a los datos desde aplicaciones externas en la nube. Ya no hay un foso, sino que el castillo de la red pasa a tener varias entradas. El aumento del trabajo remoto durante la pandemia convirtió al perímetro tradicional en "perímetro definido por software". En el apuro por lograr que los empleados sigan trabajando, muchos empezaron a pensar tarde en la seguridad, lo que generó abundantes oportunidades de ransomware para los actores malintencionados.

Acceso remoto

Según el reporte *Principales tendencias de seguridad y riesgos para 2021*, el 64 % de los empleados ahora pueden trabajar desde su casa, y dos quintos de la fuerza laboral trabajan desde casa. Debido a las órdenes de permanencia obligatoria en el hogar, la mayoría de los empleados debieron pasar a trabajar de manera 100 % remota y tuvieron que emplear sus propios dispositivos y, al mismo tiempo, acceder a las aplicaciones de SaaS en la nube y en las instalaciones. Muchas empresas no contaban con la infraestructura necesaria para enfrentar este cambio. En la actualidad, el acceso remoto es la nueva realidad de la fuerza laboral. A medida que las organizaciones se adaptan a esta manera de operar, se predice que el personal adoptará un modelo híbrido de trabajo remoto y trabajo en la oficina.

Peter Firstbrook, vicepresidente de Análisis de Gartner, afirmó en una publicación para un blog: "A medida que toma forma la nueva normalidad, todas las organizaciones necesitarán adoptar una postura defensiva siempre conectada, y deberán tener en claro los riesgos empresariales de los usuarios remotos para preservar la seguridad".

Las empresas que no fortalecieron su posición de seguridad para este cambio o reforzaron la capacitación interna en seguridad facilitan los ataques. Gartner informó que un 57 % de las intrusiones implican negligencia de empleados o terceros. Según ZDNet, el protocolo de escritorio remoto (RDP) es la principal manera en que los actores de amenazas acceden a las computadoras con Windows e instalan ransomware y otro malware, tras aprovechar las vulnerabilidades de suplantación de identidad por correo electrónico y de errores de VPN.

Restricciones de VPN

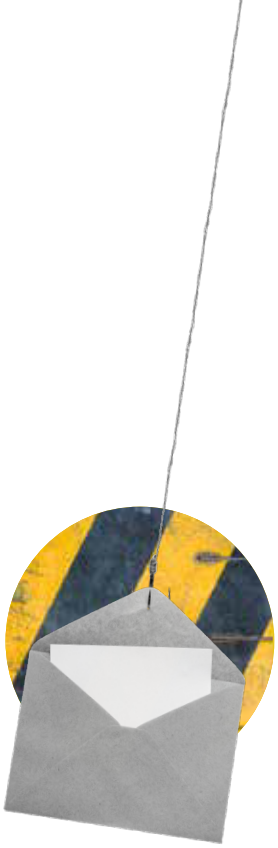
Las vulnerabilidades de hackeo de las VPN es el tercer método más popular de intrusión por parte de los hackers que realizan ataques de ransomware. El hackeo que causó una interrupción en Colonial Pipeline Company fue el resultado de una contraseña insegura de una VPN en desuso. Las VPN pueden limitar el acceso a las aplicaciones en las instalaciones, pero las incoherencias en el acceso a las aplicaciones en la nube pueden causar vulnerabilidades. Una vez que las VPN se ven afectadas, los hackers pueden obtener acceso a la red por la puerta trasera para instalar malware en los sistemas internos.

> Adoptar un enfoque de VPN y firewall en capas de confianza cero con MFA evita el 100 % de los ataques con bots automatizados, el 99 % de los ataques masivos de suplantación de identidad y el 90 % de los ataques personalizados, según una investigación de Google.

Terminales sin protección

A medida que se conectan más dispositivos a las redes corporativas, aumenta la cantidad de dispositivos personales y dispositivos desconocidos. Como es posible que estos dispositivos no estén monitoreados ni actualizados, pueden generar intrusiones en terminales clave sin detección. A medida que los hackers buscan meticulosamente una forma de infiltrarse, los terminales sin protección, junto con la falta de información sobre el estado de los dispositivos y sobre las personas y los dispositivos que se conectan a la red pueden permitir una intrusión.

Suplantación de identidad, ataques personalizados y vulnerabilidades



¿Qué técnicas se usan en los ataques de ransomware? Se emplea un proceso de varios pasos, que puede hacerse en relativamente poco tiempo o durante meses, para acceder y cifrar los datos más valiosos y que causen más daño si se los roba y se pide un rescate. CSOonline.com informa que el 94 % del malware se envía por correo electrónico, y que los ataques de suplantación de identidad representan un 80 % de los incidentes de seguridad. Otros puntos de entrada son las actualizaciones sin parches y las vulnerabilidades de día cero. Casi todos los ataques comienzan con el robo de credenciales.

Técnicas de ransomware

Ataques de tipo "disparar y rezar" o ataques masivos de suplantación de identidad

Los atacantes adquieren listas de direcciones de correo electrónico en el mercado negro, analizan las credenciales y distribuyen mensajes de suplantación de identidad por correo electrónico. Para que el ataque tenga éxito, solo se necesitan unas pocas credenciales, que suelen obtenerse mediante un correo electrónico con archivos adjuntos maliciosos, sitios web fraudulentos que parecen legítimos o una identidad falsa que tiene como objetivos a los empleados de alto valor.

Suplantación de identidad focalizada

Este ataque coordinado y dirigido se realiza al enviar mensajes personalizados con ingeniería social que provocan curiosidad, miedo o prometen recompensas de un origen que aparenta ser legítimo. Los mensajes de correo electrónico y el sitio web contienen malware que se usa para robar credenciales. El malware también puede propagarse por medios sociales y aplicaciones de mensajería instantánea.

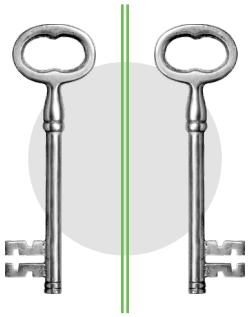
Fuerza bruta

Según una encuesta de LastPass, el 91 % de los encuestados reconoció que reutilizan las contraseñas. Los hackers saben esto y recopilan contraseñas de divulgaciones masivas de credenciales o la dark web. Luego, usan herramientas automatizadas para probar las contraseñas en varios sitios diferentes, en lo que se conoce como ataque de fuerza bruta o de robo masivo de credenciales. Una vez que obtienen acceso, el ataque puede comenzar.

Explotación de vulnerabilidades conocidas

Además de la información de los dispositivos que se conectan a la red, también es importante conocer el estado de los dispositivos y de los parches y actualizaciones, con el fin de mantener un alto perfil de seguridad. Security Boulevard informa: “Los componentes de código abierto desactualizados o abandonados son muy comunes. El 91 % de las bases de código tenían componentes con más de cuatro años sin actualizar o sin actividad de desarrollo en los últimos dos años”.

Guía paso a paso de un ataque de ransomware



Ransomware de encriptación

Los ataques de ransomware más comunes implican la encriptación de datos de los sistemas atacados, que quedan inaccesibles hasta que se pague un rescate para descifrarlos. La táctica más reciente implica la encriptación doble, mediante la cual los hackers cifran un sistema dos veces, o dos pandillas diferentes atacan a la misma víctima. Este enfoque permite que los atacantes obtengan dos rescates, ya que, tras recibir el pago por la primera capa de encriptación, sorprenden a las víctimas con otra capa tras cobrar el rescate por la primera capa. Los tipos más comunes de encriptación son asimétrico o simétrico.

Coordinación del ataque

En este punto, los hackers que hacen ataques de ransomware estudian a las empresas específicas que quieren atacar. Es posible que compren listas de direcciones de correo electrónico en la dark web, identifiquen a los líderes importantes, se informen sobre el estado financiero de la empresa, investiguen los perfiles en medios sociales y creen una lista de partes interesadas clave, como contratistas, proveedores y partners. ¿Qué tácticas emplean los hackers para obtener acceso? Los tres ataques más importantes de 2020 se debieron a terminales de RDP desprotegidos, a ataques de suplantación de identidad por correo electrónico y a la explotación de vulnerabilidades de VPN de día cero. El robo de credenciales es la principal manera en que los atacantes obtienen acceso.

Movimiento vertical

En la etapa de infiltración e infección, los atacantes usan el movimiento vertical para pasar de una posición externa a una posición interna. Una vez dentro del sistema, analizan los archivos y ejecutan código malicioso en terminales y dispositivos de red. El malware avanza por el sistema infectado, y desactiva los firewalls y el software antivirus. A esta altura, los atacantes ya controlan los datos, pero aún no los encriptaron. Los puntos de entrada comunes para el movimiento vertical son las cuentas de correo electrónico de suplantación de identidad, los servidores web de bajo nivel y los terminales desprotegidos.

Movimiento lateral

Las amenazas persistentes avanzadas (APT) han tenido más éxito debido al movimiento lateral. Para consolidar la infiltración en el sistema, los delincuentes deben cifrar las computadoras y propagar el ransomware a la mayor cantidad de equipos que sea posible. Una vez que obtienen acceso, los hackers comienzan la cacería. Durante semanas o meses, realizan movimientos laterales por la red sin ser detectados para identificar los objetivos clave, como el centro de comando y control (C2), las claves asimétricas y los archivos de respaldo. Al mismo tiempo, elevan su nivel de acceso y permisos al infectar sistemas y cuentas de usuario adicionales, y preparan una presencia maliciosa persistente para encriptar los datos y pedir un rescate. Algunos ejemplos de movimiento lateral son la explotación de servicios remotos, la suplantación de identidad focalizada interna y el uso de contraseñas robadas, también conocido como “pasar el hash”.

Exfiltración de datos

Una vez terminada la evaluación de inventario, comienza la encriptación. Se eliminan las copias de respaldo del sistema, se dañan los archivos y las carpetas locales, se conectan los dispositivos de red no asignados a sistemas infectados, y se entablan comunicaciones con el centro de comando y control para generar las claves criptográficas que se usan en el sistema local. Los datos de red se copian a nivel local, se cifran y luego se cargan en reemplazo de los datos originales. Los datos exfiltrados se pueden usar como estrategia de doble extorsión. En este caso, se exige un rescate para desencriptar los datos cifrados y, luego, se pide un segundo rescate para no divulgar los datos robados.

Pago y desbloqueo

En este punto, los atacantes activan el malware, bloquean los datos y anuncian sus demandas de rescate en ubicaciones comprometidas con instrucciones específicas para hacer el pago, generalmente en bitcoin. Un ataque de ransomware crea un problema de tiempo de inactividad muy costoso y extremadamente difícil de resolver. Se envían las amenazas y comienza la cuenta regresiva. Las empresas deben elegir entre acceder a las demandas y pagar el rescate, intentar restaurar los archivos por su cuenta, o usar el seguro de ciberseguridad, que solo cubre una parte del rescate. Para evitar esta situación de tener que elegir entre opciones malas o peores, es vital que las organizaciones implementen una arquitectura de confianza cero y prácticas recomendadas de seguridad reforzadas.

Sectores vulnerables

Los sectores más afectados por los ataques de ransomware son los de atención médica, gobiernos y municipalidades, comercio minorista, educación y finanzas. Estos sectores suelen tener soluciones heredadas complejas y no aprovechan la seguridad resistente en la nube. Los sectores de atención médica, educación y gobierno son lentos en actualizar sus medidas de seguridad con modernización y tecnología nueva, lo que los convierte en presas fáciles y lucrativas.

Cómo evitar los riesgos del ransomware antes de que se produzcan

Para hacer un ataque de ransomware, los atacantes primero necesitan obtener acceso. Pueden obtenerlo al conseguir credenciales comprometidas, como en el caso de la intrusión de Colonial Pipeline.

La autenticación de varios factores (MFA) puede ayudar a evitar que los ataques de ransomware obtengan acceso. Con la MFA, se exige a los usuarios que presenten una combinación de dos o más credenciales para verificar su identidad al iniciar sesión. Por ejemplo, además de un nombre de usuario y contraseña, Duo MFA exige otro factor de autenticación, como un dispositivo de confianza o token de software o hardware, para otorgar acceso a los recursos. Gracias a este requisito adicional, la MFA hace que sea mucho más difícil que los ataques de ransomware obtengan ese acceso inicial.

Los ataques de ransomware también suelen usar servicios remotos, como RDP y VPN, para obtener acceso a la red. Se sospecha que Darkside, el grupo que supuestamente estuvo detrás del ataque a Colonial Pipeline, usó acceso de VPN corporativo para ingresar al entorno de la víctima. Duo MFA, Duo Device Trust, Duo Network Gateway (DNG) y Duo Trust Monitor ofrecen mucho más que MFA y se combinan para crear una solución de acceso de confianza que puede ayudar a proteger el acceso remoto a la infraestructura de las instalaciones y evitar el acceso de ransomware.

Cómo ayuda Duo a protegerse de los ataques de ransomware

Según Gartner, el 90 % de los ataques de ransomware se pueden prevenir. Duo es la única herramienta que ayuda a las organizaciones en tres frentes:

1. Evitar que el ransomware obtenga acceso inicial al entorno.
2. Evitar o ralentizar la propagación del ransomware que logra infiltrarse en la organización.
3. Proteger los activos y las partes esenciales de la organización mientras el atacante aún tiene presencia en el entorno y hasta que se haya logrado corregir el problema por completo.

Duo MFA requiere más que un nombre de usuario y contraseña para la autenticación. DNG permite que los usuarios accedan a los sitios web en las instalaciones, las aplicaciones web, los servidores SSH y RDP sin tener que preocuparse por las credenciales de VPN. Duo Device Trust garantiza que el dispositivo que accede a los recursos de forma remota sea una computadora de confianza y no un dispositivo de un atacante. Por último, Duo Trust Monitor notifica de las solicitudes de autenticación sospechosas, como las que se originan de países con atacantes de ransomware activos y de países en los que la organización no tiene empleados.

El uso de malware también es una técnica muy usada de infección por ransomware. Cisco ofrece soluciones complementarias adicionales, como Secure Endpoint y Email Gateway, que permiten inspeccionar, detectar y bloquear ataques de ransomware basados en malware antes de que infecten los terminales.

Cómo evitar la propagación

Los ataques de ransomware que afectan a un número pequeño de sistemas tienen un impacto limitado, y es poco probable que interrumpan todas las actividades de la organización al punto de verse obligados a pagar el rescate. Por eso, la propagación del ransomware es fundamental para que afecte a una parte considerable de la organización y, de esta manera, se vea obligada a pagar el rescate para poder volver a operar rápidamente. En 2017, WannaCry y NotPetya usaron el ataque External Blue para aprovechar una vulnerabilidad de Microsoft y propagarse sin intervención del usuario.

La aplicación Device Health de Duo puede mantener los dispositivos actualizados y con los parches instalados, lo que dificulta la propagación automática del ransomware. Además, aporta visibilidad y comprueba el estado de los dispositivos, incluido el nivel de actualización, en cada intento de inicio de sesión. Con la capacidad de corrección automática de Duo, los usuarios pueden instalar fácilmente los parches más actualizados en los dispositivos sin ayuda del equipo de TI.

Corrección con seguridad

La recuperación tras un ataque de ransowmware y el restablecimiento de las funciones del sistema no necesariamente significan que el atacante haya abandonado el entorno. Es posible que haya intentado establecer una presencia persistente para volver a atacar luego. Una técnica común implica robar cuentas existentes o crear cuentas nuevas, a menudo mediante el acceso a Active Directory u otros directorios con cuentas de usuario. Duo MFA puede brindar la tranquilidad de que un atacante que aún está dentro de la red no pueda moverse lateralmente con facilidad mediante el uso de credenciales robadas. También permite ganar tiempo para evitar que el atacante cause más daño mientras el ataque se mitiga por completo, eliminando todo rastro de permanencia.

Implementación de un modelo de seguridad de confianza cero

Basado en el principio de “nunca confiar, siempre verificar”, el modelo de seguridad de confianza cero puede ayudar a las organizaciones a implementar proactivamente prácticas recomendadas conocidas para protegerse de los ciberataques, incluidos los ataques de ransomware.

El modelo de confianza cero es tan importante que la Casa Blanca emitió una orden ejecutiva en la que se exige el uso de modelos de confianza cero y MFA.

Duo proporciona MFA fácil de usar e implementar. También permite que las organizaciones solo concedan acceso si se puede verificar y confiar en el 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 necesarios para implementar un marco de confianza cero.

Conclusión

Los ataques de ransomware serán cada vez más comunes, por lo que las empresas deben estar más atentas. Los ataques de ingeniería social y suplantación de identidad focalizada tienen éxito porque se aprovechan del factor humano en el plano de la seguridad de la organización. Adoptar e implementar una filosofía de seguridad de confianza cero comienza con autenticación MFA sólida y una plataforma de acceso de confianza, y es vital para anticiparse a los ataques de ransomware.

Vaya un paso más allá y actualice sus defensas de MFA con Duo

Las organizaciones pueden defenderse de los efectos de los ataques de ransomware con suplantación de identidad focalizada e ingeniería social mediante la implementación de políticas de acceso condicional que aprovechan los factores contextuales, como la ubicación y la postura de los dispositivos, para otorgar confianza a usuarios y dispositivos.

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

1. Verificar las identidades de los usuarios con métodos de autenticación de varios factores.
2. Ofrecer a los usuarios una experiencia de inicio de sesión uniforme con el inicio de sesión único de Duo, que permite el acceso centralizado a las aplicaciones en las instalaciones y en la nube.
3. Obtener visibilidad de todos los dispositivos, y mantener un inventario detallado de todos los dispositivos que acceden a las aplicaciones corporativas.
4. Establecer la confianza en los dispositivos mediante controles de estado y postura de los dispositivos administrados y no administrados antes de conceder acceso a las aplicaciones.
5. Aplicar políticas de acceso granular para limitar el acceso a los usuarios y dispositivos que cumplen con los niveles de tolerancia al riesgo de la organización.
6. Monitorear y detectar el comportamiento riesgoso de inicio de sesión con Duo Trust Monitor o exportar los registros de eSIEM para resolver eventos sospechosos, como la inscripción de un dispositivo nuevo para autenticación o inicio de sesión desde una ubicación inesperada.

¿Por qué conviene elegir Duo?

Seguridad al instante
Duo ofrece los componentes de confianza cero en una solución rápida y fácil de implementar para los usuarios. Según el caso de uso específico, algunos clientes pueden ponerla en marcha en minutos.

Facilidad de uso
Los usuarios pueden inscribirse por su cuenta con solo descargar una aplicación de App Store e iniciar sesión. Los administradores pueden usar los controles de mantenimiento y políticas fácilmente para obtener una visibilidad clara.

Se integra con todas las aplicaciones
Nuestro producto está diseñado para funcionar sin restricciones con sistemas heredados. Duo permite proteger el acceso a todas las aplicaciones de trabajo, a todos los usuarios y desde cualquier lugar.

Menor costo total de propiedad (TCO)
Como Duo es fácil de implementar y no requiere que los sistemas se reemplacen, necesita menos recursos, tiempo y costo para ponerse en marcha rápidamente y, de esta manera, permitirle seguir en el camino hacia un modelo de seguridad de confianza cero.

Referencias

En la pandemia, los ataques de ransomware aumentaron un 150 % en todo el mundo, https://cisomag.eccouncil.org/growth-of-ransomware-2020/, CISO Magazine, 5 de marzo de 2021

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 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

HOJA INFORMATIVA: Iniciativas públicas constantes de EE. UU. para combatir los ataques de ransomware, https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware, boletín oficial de la Casa Blanca, 13 de octubre de 2021

Tipos de encriptación: ¿simétrica o asimétrica? ¿RSA o AES?, https://preyproject.com/blog/en/types-of-encryption-symmetric-or-asymmetric-rsa-or-aes/, Prey Project, 15 de junio de 2021

Qué se sabe de DarkSide, el grupo de hackers rusos que causó estragos en la costa este, https://www.heritage.org/cybersecurity/commentary/what-we-know-about-darkside-the-russian-hacker-group-just-wreaked-havoc, The Heritage Foundation, 20 de mayo de 2021

Qué se puede aprender de los ataques de ransomware "*Reportes de seguridad*," https://www.coveware.com/blog/2021/6/24/what-we-can-learn-from-ransomware-actor-security-reports, Coveware, 24 de junio de 2021

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

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

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

Disminuyeron los ataques de malware, pero aumentaron los ataques de ransomware e Internet de las cosas, https://www.techrepublic.com/article/malware-is-down-but-iot-and-ransomware-attacks-are-up/, Tech Republic, 23 de junio de 2020

En 2020 hubo una víctima de ransomware cada 10 segundos, https://www.infosecurity-magazine.com/news/one-ransomware-victim-every-10/, Infosecurity Magazine, 25 de febrero de 2021

Estadísticas impactantes: 1 de cada 5 estadounidenses son víctimas de ransomware, https://sensorstechforum.com/1-5-americans-victim-ransomware/, Sensors Tech Forum, 19 de agosto de 2019

Gartner predice que los gastos globales en seguridad y administración de riesgos superará los USD 150.000 millones en 2021, https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem, Gartner, 17 de mayo de 2021

1 de cada 5 pymes han sufrido ataques de ransomware, https://www.helpnetsecurity.com/2019/10/17/smbs-ransomware-attack/, Help Net Security, 17 de octubre de 2019

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

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

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

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

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 gastó USD 2,6 millones para recuperarse de una amenaza de ransomware de USD 52 000, https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare, Wired.com, 23 de abril de 2018

Ciberataques: Estados Unidos y Reino Unido culpan a Corea del Norte por el ataque WannaCry, https://www.bbc.com/news/world-us-canada-42407488, BBC.com, 19 de septiembre de 2017

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

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 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

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

Prevención de ataques extorsivos digitales, https://subscription.packtpub.com/book/networking_and_servers/9781787120365/4/ch04lvl1sec24/the-advancement-of-locker-ransomware-winlock, PackIt, mayo de 2017

Efectos irreversibles de los ataques de ransomware, https://www.crowdstrike.com/blog/irreversible-effects-ransomware-attack, CrowdStrike, 20 de julio de 2016

La nueva era del trabajo remoto exige adoptar un enfoque de seguridad moderno, Finds Thales Global Survey of IT Leaders, 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

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

Resumen de seguridad de Symantec, septiembre de 2021, https://symantec-enterprise-blogs.security.com/blogs/feature-stories/symantec-security-summary-september-2021, Symantec Security, 27 de septiembre de 2021

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

Principales tendencias de seguridad y riesgos para 2021, https://www.gartner.com/smarterwithgartner/gartner-top-security-and-risk-trends-for-2021, Gartner, 5 de abril de 2021

Encuesta de Gartner revela que un 82 % de los líderes empresariales piensan permitir el trabajo remoto a tiempo parcial, 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 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.

Reporte de ciberamenazas de SonicWall para 2021, https://www.sonicwall.com/medialibrary/en/white-paper/2021-cyber-threat-report.pdf, SonicWall, 2021

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

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

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

Principales estadísticas, tendencias y datos de ciberseguridad, https://www.csoonline.com/article/3634869/top-cybersecurity-statistics-trends-and-facts.html, CSOonline.com, 7 de octubre de 2021

Protección empresarial contra los ciberataques, https://www.inc.com/knowbe4/protecting-companies-from-cyberattacks.html, Inc.com, 20 de septiembre de 2021

ThreatList: la gente sabe que reutilizar contraseñas es mala idea, pero igual lo hace, https://threatpost.com/threatlist-people-know-reusing-passwords-is-dumb-but-still-do-it/155996/, Threatpost, 25 de mayo de 2020

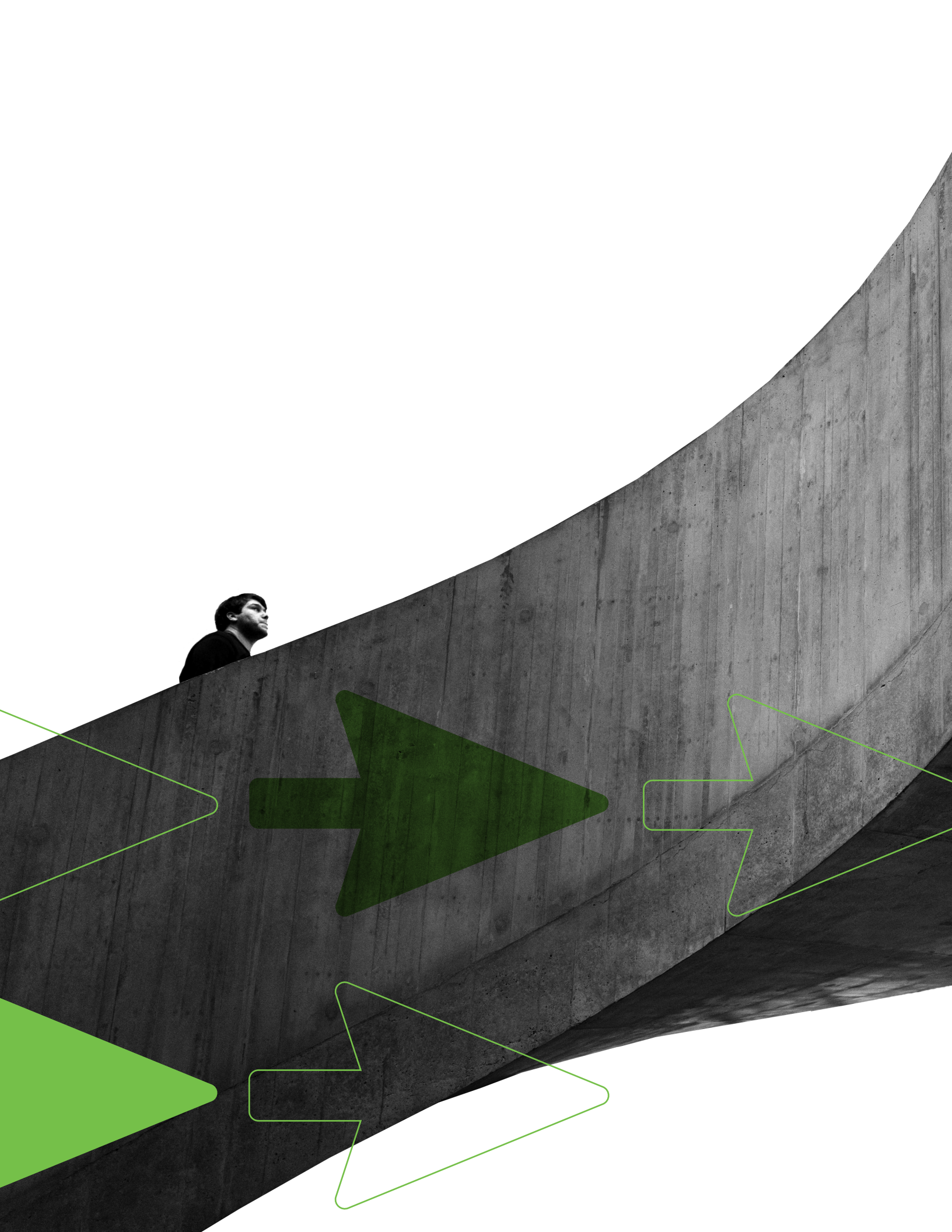
Estudio de Synopsys muestra que el 91 % de las aplicaciones comerciales tienen componentes de código abierto desactualizados o descatalogados, https://www.securitymagazine.com/articles/92368-synopsys-study-shows-91-of-commercial-applications-contain-outdated-or-abandoned-open-source-components, Security Magazine, 12 de mayo de 2020

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

Cómo combatir el movimiento lateral y el aumento del ransomware, https://www.msspalert.com/cybersecurity-guests/combating-lateral-movement-and-the-rise-of-ransomware, MSSP Alert, 24 de mayo de 2021

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

Industrias afectadas por el ransomware, https://airgap.io/blog/industries-impacted-by-ransomware, AirGap.com

Defensa y respuesta ante ataques de ransomware, https://www.gartner.com/en/documents/3978727/defend-against-and-respond-to-ransomware-attacks, investigación de Gartner, 26 de diciembre de 2019

Orden ejecutiva para mejorar la ciberseguridad, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/, boletín de la Casa Blanca. 12 de mayo de 2021