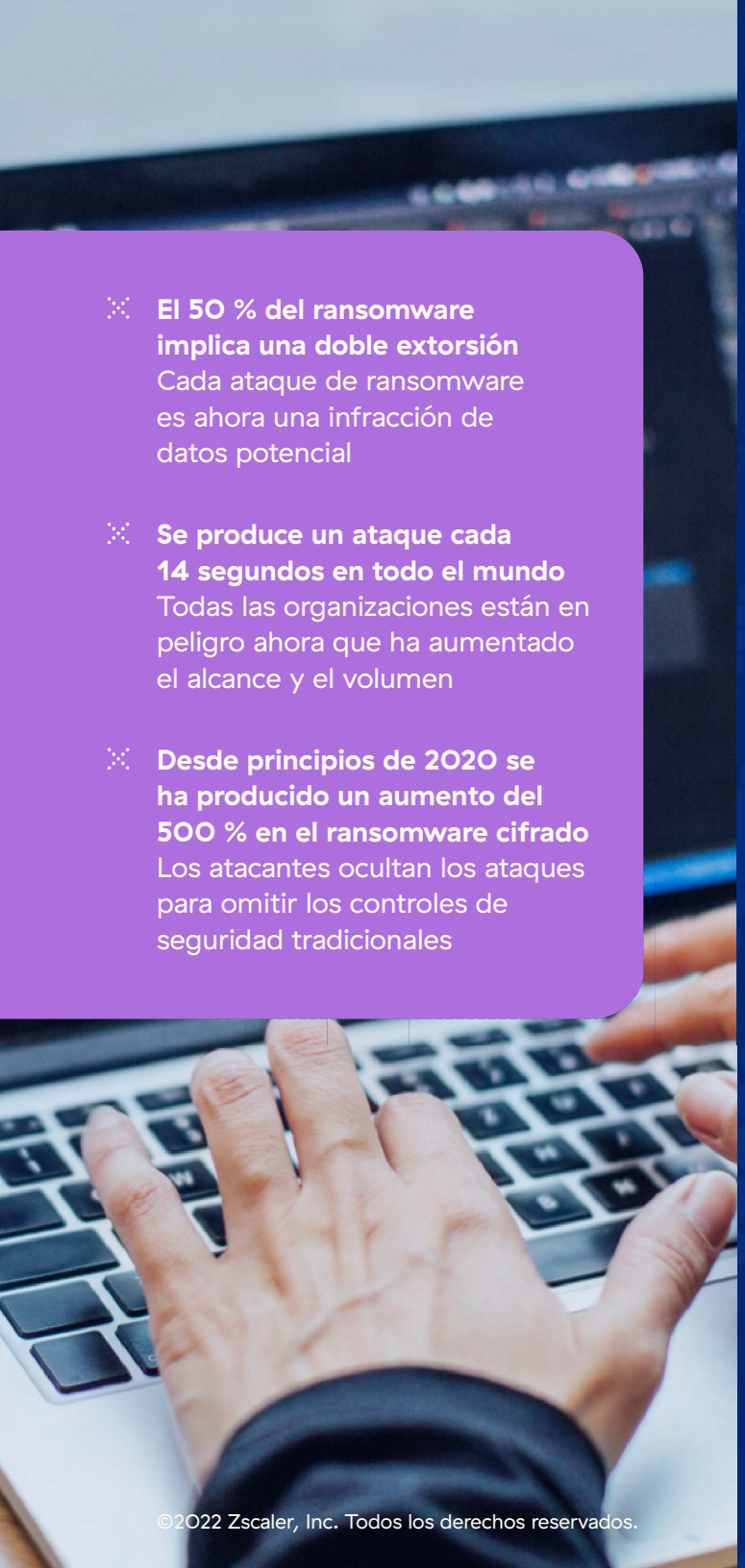
Libro electrónico

Diez maneras en las que una arquitectura de confianza cero protege contra el ransomware



- **El 50 % del ransomware implica una doble extorsión**
  Cada ataque de ransomware es ahora una infracción de datos potencial

- **Se produce un ataque cada 14 segundos en todo el mundo**
  Todas las organizaciones están en peligro ahora que ha aumentado el alcance y el volumen

- **Desde principios de 2020 se ha producido un aumento del 500 % en el ransomware cifrado**
  Los atacantes ocultan los ataques para omitir los controles de seguridad tradicionales

El ransomware es la mayor amenaza para la actividad empresarial digital

Aunque el ransomware existe desde hace décadas, su prevalencia se ha disparado en los últimos dos años. Estos ataques solían ser perpetrados por individuos; ahora son obra de grupos de socios que trabajan en red y comercializan entre sí sus paquetes de herramientas y habilidades especializadas. Antes, los ataques no tenían objetivos concretos y eran unidimensionales; ahora se dirigen a objetivos específicos, utilizan tácticas multicapa ante las que es mucho más difícil defenderse y exigen rescates mucho más elevados. **La previsión es que, para finales de 2024, el ransomware habrá causado daños por valor de 42 000 millones de dólares.**[1]

Probablemente la tendencia más impactante en el ransomware moderno es la llegada de ataques de doble extorsión, en los que los atacantes roban datos y amenazan con publicarlos además de cifrarlos. Aproximadamente el 50 % de los ataques de ransomware ahora incluyen intentos de extraer datos.

Hay una estrategia subyacente que maximiza las posibilidades de una organización de mitigar los daños que pueda causar un ataque de ransomware: la confianza cero.

La confianza cero es un enfoque de seguridad que se basa en la noción de que ya se ha producido una violación. Las arquitecturas, las políticas de control de acceso y las tácticas de supervisión y autenticación se ponen en marcha para mitigar la intensidad y la gravedad del daño que un atacante puede causar.

He aquí 10 formas en las que la confianza cero puede ayudar a su organización a defenderse del ransomware.

[1] *De acuerdo con Cybersecurity Ventures, "se prevé que, en el 2031, los costes globales de daños por ransomware habrán superado los 265 000 millones de dólares".*

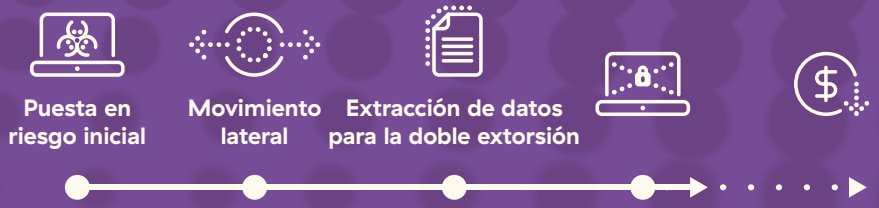
Comprender la secuencia de ataque del ransomware

En un ataque de ransomware, los adversarios deben completar una serie de objetivos para tener éxito. En primer lugar, deben conseguir entrar en su entorno infectando con éxito un sistema con una carga útil de ransomware malicioso. **Por lo tanto, el primer paso para detener un ataque es poner en marcha controles preventivos que reduzcan sus vulnerabilidades, minimicen su superficie de ataque y le permitan bloquear, controlar e inspeccionar el tráfico.**

En segundo lugar, los atacantes hacen un reconocimiento, localizando activos de alto valor para robarlos y cifrarlos. Para ello, deben ser capaces de moverse lateralmente por la red. **El segundo paso para detener un ataque y minimizar el daño que puede causar un atacante es limitar su capacidad de moverse lateralmente.**

En un ataque de doble extorsión, los atacantes roban datos y los mantienen como rehenes para aumentar sus posibilidades de éxito y el importe de sus exigencias de rescate. **El tercer paso para defenderse de un ataque de ransomware es la prevención de la pérdida de datos.**

Veamos cómo la confianza cero permite la defensa en toda la cadena de ataque.



N.º 1

Al hacer que las aplicaciones sean invisibles para los atacantes, una arquitectura de confianza cero minimiza la superficie de ataque.

Que las identidades de las aplicaciones, los usuarios y los dispositivos pueden descubrirse abiertamente en Internet es como si se expusieran públicamente sus activos de información más valiosos. Cuando estos activos son visibles, los atacantes son capaces de encontrar y explotar fácilmente las vulnerabilidades (como un software de servidor web sin parches o una contraseña débil que se pueda descifrar en un ataque de fuerza bruta), lo cual les pone en una posición sólida de forma inmediata.

Aprovechar una solución como Zscaler Private Access™ permite que las aplicaciones se conecten a los usuarios en lugar de que los usuarios se conecten a las aplicaciones. Con esta forma de conectividad interna, todas las aplicaciones siguen siendo privadas y, por lo tanto, invisibles para los atacantes. Hacer extensivo este enfoque a todos los dispositivos y aplicaciones de su entorno hace que sea casi imposible para los atacantes entrar a hacer un reconocimiento.

N.º 2

En una arquitectura de confianza cero, todo el tráfico, incluido el cifrado, está sujeto a una inspección profunda y exhaustiva.

La gran mayoría del tráfico de Internet de hoy en día aprovecha el cifrado y el tráfico malicioso no es una excepción. Más del 90 % del tráfico de Internet está ahora cifrado y el cifrado del ransomware ha aumentado más del 500 % desde principios de 2020. Los equipos de seguridad ya no pueden asumir ciegamente que todo el tráfico cifrado por SSL es seguro.

No obstante, ahora que la inspección de todo el tráfico, cifrado o no, es una parte esencial de una estrategia defensiva sólida, las arquitecturas que dependen de los cortafuegos de próxima generación y otras defensas basadas en el perímetro ya no están a la altura. Es sencillamente imposible que incluso las herramientas de seguridad locales más avanzadas inspeccionen todo el tráfico cifrado con SSL sin producir cuellos de botella en el rendimiento que obstaculicen la productividad. Una arquitectura basada en proxy en la nube y creada específicamente para detectar malware cifrado por SSL a escala protegerá todo su tráfico y eliminará los puntos ciegos.

N.º 3

Las estrategias de confianza cero incluyen controles para detectar amenazas de ransomware nunca vistas antes de que puedan causar daños.

Cada vez es mayor el número de ataques de ransomware que aprovechan el malware elaborado a medida. Para defenderse de estos peligros, necesita ser capaz de detectar y bloquear las nuevas amenazas. Con el sandboxing nativo en la nube y la detección potenciada por IA, puede confiar en que el análisis de comportamiento descubrirá variantes de ransomware previamente desconocidas poniendo en cuarentena y analizando en su totalidad los archivos antes de que se entreguen a los usuarios o se permita su ejecución.

Con una solución como Zscaler Cloud Sandbox, puede definir políticas basadas en usuarios, grupos y tipos de contenido, lo que le dará un control granular sobre las acciones de cuarentena. Debido a que esta solución es parte de Zscaler Zero Trust Exchange™, obtendrá veredictos de archivos casi en tiempo real procedentes de una comunidad global, lo que minimiza el impacto en el usuario a la vez que maximiza la precisión de la detección de malware.

N.º 4

La confianza cero simplifica las políticas de control de acceso, aumenta la visibilidad y mejora la eficacia.

La microsegmentación es un concepto fundamental en la confianza cero. Implica restringir el acceso a las aplicaciones y los recursos para que los atacantes que ataquen a uno de estos no puedan dañar a los demás. En el enfoque heredado basado en la red para la microsegmentación, los cortafuegos aplicaban reglas examinando las direcciones de red. Dicho enfoque exigía redefinir y actualizar las políticas a medida que las aplicaciones se movían y las redes evolucionaban. Esto ya era en sí mismo un reto en el centro de datos local, pero lo efímero de la nube ha aumentado su complejidad hasta el punto de ser inmanejable.

Las arquitecturas de proxy reducen en gran medida la complejidad de la implementación de la microsegmentación, a la vez que proporcionan una protección más sólida para las cargas de trabajo. Dado que las políticas y los permisos se gestionan en función de las identidades de los recursos, son independientes de la infraestructura de red subyacente y pueden adaptarse de manera automática, independientemente de lo dinámica que sea la arquitectura de la red o de la rapidez con que cambien los requisitos de la empresa. Esto también simplifica la gestión: puede proteger un segmento con solo unas pocas políticas basadas en la identidad en lugar de tener cientos de reglas basadas en la dirección.

N.º 5

Una arquitectura de confianza cero protege a los usuarios y a los dispositivos estén donde estén.

Cuando la pandemia de la COVID-19 hizo que apoyar el trabajo remoto fuera imprescindible para las organizaciones de todos los sectores, muchas recurrieron a redes privadas virtuales (VPN) o al protocolo de escritorio remoto (RDP) para permitir que los empleados que trabajaban desde casa se conectaran a redes y recursos corporativos. Desafortunadamente, los operadores de ransomware no tardaron en seguir los pasos de estas organizaciones y lanzaron una nueva oleada de ataques basados en RDP y VPN. De hecho, se explotó una VPN en el ahora famoso ataque a Colonial Pipeline que detuvo el transporte de casi la mitad del suministro de combustible en el este de Estados Unidos.

En un enfoque basado en la confianza cero para proteger a los usuarios remotos, cada conexión recibe una protección idéntica, independientemente de la ubicación de los usuarios. La incorporación de un agente de punto final ligero, Zscaler Client Connector, al dispositivo de cada usuario remoto les da acceso a toda la seguridad, la aplicación de políticas y los controles de acceso disponibles a través de Zscaler Zero Trust Exchange. Y dado que Zscaler se distribuye en 150 centros de datos en todo el mundo, los usuarios siempre obtienen una conexión rápida a través de un centro de datos cercano, lo que elimina las molestias de la latencia de VPN.

N.º 6

Una auténtica arquitectura de confianza cero hace imposible que los atacantes se desplacen lateralmente por su red.

Demasiados equipos de seguridad siguen confiando en que la segmentación de red basada en un cortafuegos heredado mantendrá el tráfico malicioso fuera de las redes corporativas. Estas estrategias no solo son difíciles de implementar y gestionar, sino que siguen dejando expuestos los recursos internos. Si los atacantes consiguen vulnerar una aplicación o un cortafuegos, siguen pudiendo desplazarse lateralmente por el entorno, lo que les permite cifrar y robar muchos más datos de los que podrían conseguir de otro modo.

Un verdadero enfoque de confianza cero conecta a un usuario directamente con la aplicación que necesita en un segmento 1:1, sin exponer nunca la red. Los equipos de seguridad pueden utilizar una arquitectura proxy para autenticar continuamente a los usuarios y conectarlos directamente a las aplicaciones en lugar de confiar en el tráfico de una red o subred interna, lo que elimina el mayor riesgo digital al que se enfrentan las empresas actualmente. Lo mejor de todo es que un proxy funciona independientemente de dónde se encuentren sus usuarios, dispositivos o aplicaciones, proporcionando una conectividad segura tanto en las instalaciones como fuera de ellas.

N.º 7

Una arquitectura de confianza cero evita que los atacantes aprovechen las cargas de trabajo.

En una arquitectura de confianza cero, las políticas de seguridad se aplican en función de la identidad de las cargas de trabajo que intentan comunicarse entre sí. Estas identidades se verifican constantemente y se bloquea la comunicación de las cargas de trabajo no verificadas con otras. Esto significa que no pueden interactuar con servidores maliciosos remotos de comando y control, ni con hosts, usuarios, aplicaciones y datos internos.

Una plataforma como Zscaler Zero Trust Exchange garantiza automáticamente que todo el tráfico (independientemente de su origen) satisface todas las políticas corporativas al acceder a sus recursos. Además, aplica estas políticas de forma totalmente uniforme, independientemente de si los recursos en cuestión son SaaS internos, externos o de terceros. Este es un enfoque mucho más sencillo de la microsegmentación de la red que la aplicación de políticas de múltiples capas y, además, es más eficaz.

N.º 8

La confianza cero incluye estrategias proactivas para vencer a los contrincantes en su propio juego.

Los operadores actuales de ransomware son enemigos sofisticados que son capaces de omitir la prevención inicial. Por lo tanto, un aspecto clave de la confianza cero es emplear estrategias para encontrar y aislar ataques antes de que puedan causar daños. Como la única plataforma de confianza cero del mundo que integra capacidades de engaño, Zscaler Deception™ utiliza tácticas de engaño avanzadas para atraer, detectar e interceptar a los atacantes, independientemente de lo avanzadas o dirigidas que sean sus estrategias.

Este enfoque proactivo de la defensa implica llenar su entorno de TI con señuelos, como puntos finales, directorios, bases de datos, archivos y rutas de usuario falsas. Estos señuelos imitan los activos de producción de alto valor, pero permanecen ocultos a los usuarios reales. Su único propósito es alertar a su equipo de seguridad sobre la presencia de un adversario cuando alguien los toca. Puesto que no hay tráfico legítimo hacia los señuelos, las alertas son de una altísima fidelidad, lo que proporciona evidencia sólida de una amenaza o violación que las hace muy superiores al ruido de otros sistemas de detección. Esto le da a su equipo de seguridad una ventaja, lo que les permite interrumpir las tácticas programadas por los adversarios y mitigar los daños.

N.º 9

Las arquitecturas de confianza cero proporcionan una protección integral frente a la pérdida de datos.

La creciente prevalencia de las estrategias de ataque de ransomware de doble extorsión ha hecho que sea necesario considerar que cada ataque de ransomware sea una violación de datos. Las medidas que eviten la extracción y la publicación de sus datos confidenciales contribuirán en gran medida a mitigar las consecuencias más devastadoras de un ataque de ransomware.

El uso de una solución de agente de seguridad de acceso a la nube (CASB) le permite aplicar controles granulares sobre sus aplicaciones en la nube, proteger los datos en reposo dentro de las plataformas SaaS y evitar el uso compartido excesivo accidental, así como la inteligencia maliciosa. Un beneficio adicional es que disfrutará de una mejor visibilidad de sus aplicaciones en la nube, lo que facilita la identificación de vulnerabilidades, configuraciones incorrectas y la llamada "TI en la sombra", el uso de aplicaciones en la nube no autorizadas. Con las capacidades de prevención contra la pérdida de datos (DLP), podrá bloquear la extracción de datos automáticamente, lo que reducirá la amenaza de doble extorsión.

N.º 10

Una arquitectura de confianza cero le permite detener el robo de datos con una inspección en línea completa de todo el tráfico saliente.

Si los malhechores ocultan malware en el tráfico entrante cifrado por SSL, pueden utilizar la misma estrategia, aprovechando el cifrado, para ocultar el hecho de que están extrayendo datos corporativos confidenciales y valiosos. Poder inspeccionar el tráfico cifrado por SSL es fundamental para prevenir la pérdida de datos e identificar vulnerabilidades de extracción de datos de día cero.

Una solución basada en arquitecturas de confianza cero, como Zero Trust Exchange de Zscaler, garantiza que se verifiquen y protejan todas las conexiones en su entorno de manera individual, independientemente de si son entrantes o salientes. Con una arquitectura proxy nativa de la nube, es posible realizar una inspección SSL a escala sin afectar el rendimiento ni incurrir en costos excesivos. Esto elimina las brechas de seguridad que los operadores de ransomware han utilizado para lanzar sus devastadores ataques de doble extorsión.

Aplique la confianza cero para protegerse del ransomware

Zero Trust Exchange ofrece la defensa más completa frente a toda la secuencia de pasos que los atacantes deben dar para tener éxito. Vea cómo Zscaler utiliza la confianza cero para brindar una protección sin parangón para su organización.

Zero Trust Exchange

Evitar verse comprometido

Bloquee las amenazas antes de que lleguen a usted

Superficie de ataque eliminada
Las aplicaciones privadas son visibles para Internet, no se pueden descubrir ni atacar

Inspección de contenido en línea (SSL)
Arquitectura proxy patentada, motor sofisticado de inspección de contenido con efecto en la nube impulsado por AL

Protección de los datos de la nube pública
Corrija las configuraciones erróneas para evitar el acceso no autorizado a los recursos en la nube

Evitar el movimiento lateral

Detenga la propagación de la infección (LAN/WAN)

Segmentación de usuario a aplicación
Conecta un usuario y un dispositivo autenticado a una aplicación autorizada sin llevar al usuario a la red

Segmentación de carga de trabajo a carga de trabajo
Utiliza la identidad del software para permitir o bloquear las comunicaciones de la carga de trabajo en entornos híbridos y multinube

Engaño
Utiliza señuelos para detectar y detener el movimiento lateral de las amenazas activas dentro de la red que ya han omitido las defensas existentes

Prevenga la pérdida de datos

Prevenga la pérdida de datos en Internet

Inspección de contenido en línea (SSL)
Arquitectura proxy patentada con políticas DLP en línea para usuarios, servidores, cargas de trabajo, IoT y sistemas OT

Motor innovador de clasificación de datos
Con capacidades avanzadas de coincidencia de datos exacta y de huellas digitales de documentos

Datos SaaS seguros (CASB)
Evite que se comparta en exceso y el descubrimiento de los datos confidenciales en reposo

Detener los ataques modernos requiere seguridad moderna.

Proteja su empresa con la defensa contra ransomware más completa del sector.

Más información

zscaler™ | Experience your world, secured.™

Acerca de Zscaler

Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, resistentes y seguros. Zscaler Zero Trust Exchange protege a miles de clientes de los ciberataques y la pérdida de datos mediante la conexión segura de usuarios, dispositivos y aplicaciones en cualquier lugar. Distribuido en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basado en SASE es la mayor plataforma de seguridad en la nube en línea del mundo. Obtenga más información en **zscaler.es** o síganos en Twitter **@zscaler**.

+1 408.533.0288

Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134

zscaler.es