Octubre de 2021

No pague el rescate

Una guía en tres pasos para la protección contra el ransomware

Barracuda®
Your journey, secured.

Índice

El ransomware y cómo está evolucionando

En pocas palabras, el Ransomware es software malintencionado que cifra sus datos o le impide acceder a sus propios sistemas. Después, los delincuentes exigen un rescate a cambio de la clave de descifrado, aunque, por supuesto, no existe garantía alguna de que la clave funciona y vuelva a tener acceso a sus datos. Muchas víctimas han pagado el rescate y no les han devuelto sus datos.

Barracuda

En comparación con los ataques sencillos de “compromiso y cifrado” del tipo de WannaCry de hace unos años, los atacantes emplean ahora un enfoque multivectorial más sofisticado. Los ataques suelen seguir iniciándose con un correo electrónico de suplantación de identidad personalizada, pero los ataques de ransomware de la actualidad no se inician en cuanto el destinatario hace clic en el enlace malintencionado.

En lugar de eso, los ciberdelincuentes utilizan este paso para robar las credenciales de la víctima. Las credenciales se utilizan en ese momento para acceder a la red de la organización y acechan desde ahí, evaluando los activos, los servidores, las bases de datos y la plataforma de correo electrónico. Esta vigilancia puede durar semanas, o incluso meses, antes de que lancen su ataque. Esto es exactamente lo que ocurrió con el ataque de ransomware que se lanzó contra el servicio irlandés de salud, el HSE. Los atacantes afirman que pasaron semanas dentro de la red del HSE antes de lanzar el ataque que cifró y robó 700 GB de datos de pacientes.

Una de las razones por las que se está oyendo hablar más del ransomware ahora es que las barreras para entrar han desaparecido. La tecnología del crimen se está volviendo más fácil de usar. Ahora puede comprar un kit de ransomware y elegir cuál va a ser su objetivo. Las bandas ofrecen asistencia técnica a cambio de un porcentaje del rescate. Si eso lo desanimara, el delincuente en potencia puede contratar a otros ciberdelincuentes para que lancen el ataque mediante un acuerdo de ciberdelincuencia como servicio. El aumento del valor de las criptomonedas y la popularidad de los ciberseguros también han conseguido que los ataques de ransomware sean más rentables para los ciberdelincuentes y atraigan a más bandas organizadas, y los ataques de ransomware patrocinados por los distintos gobiernos han llevado la guerra cibernética a otro nivel.

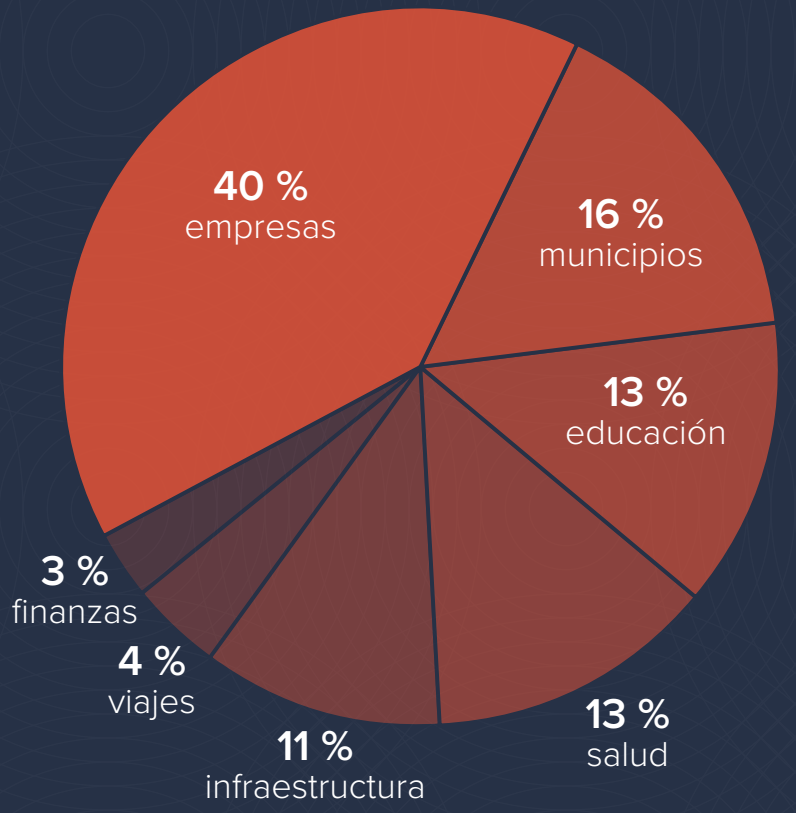
Los ciberdelincuentes están en auge

Los ataques de ransomware han subido tanto en la escala que los gobiernos ahora los tratan como ataques de terrorismo. Y no se trata de una reacción desmedida. Estos ataques han provocado la interrupción de la actividad de gobiernos locales, instituciones del orden público, y educativas, redes de salud, infraestructura crítica, etc. Ninguna entidad de ningún sector, organización o gobierno es inmune a estos ataques.

De acuerdo con las investigaciones recientes llevadas a cabo por Barracuda, los ataques contra corporaciones, tales como infraestructuras, viajes, servicios financieros y otros negocios, constituyeron hasta un 57 % de todos los ataques de ransomware producidos entre agosto de 2020 y julio de 2021, con un claro incremento si se compara con el 18 % de nuestro estudio de 2020. Las empresas relacionadas con las infraestructuras representan el 11 % de todos los ataques que estudiamos.

Las cantidades que se piden por los rescates también están aumentando considerablemente, y ahora lo que se pide de media por incidente supera los 10 millones de dólares. Solo para el 18 % de los incidentes analizados por Barracuda entre agosto de 2020 y julio de 2021 se pidieron menos de 10 millones de dólares por el rescate, y por el 30 % de los incidentes se pidieron más de 30 millones de dólares.

Ataques de ransomware por sector



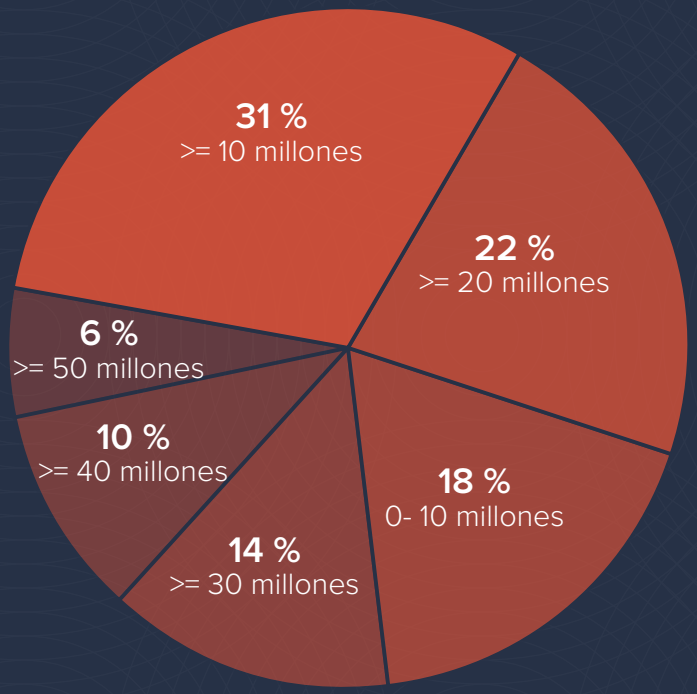
El rescate no es una amenaza nueva, pero se ha convertido en una criatura más destructiva. Los delincuentes han ampliado sus habilidades y refinado sus tácticas para crear un esquema de doble extorsión. Basan sus exigencias de rescate en la investigación que efectúan antes del ataque. Les roban datos confidenciales a sus víctimas y exigen un pago a cambio de su promesa de no publicar ni vender los datos a otros delincuentes. Como estos delincuentes no son de fiar, a menudo vuelven a ponerse en contacto con sus víctimas que pagan varios meses más tarde para solicitarles otro pago si quieren que se mantenga el secreto de los datos robados. Algunos delincuentes de ransomware aceptarán el pago, pero venden los datos en cualquier caso.

Nunca ha habido ninguna garantía de que pagar el rescate serviría para recuperar todos los datos cifrados. Las víctimas deberían comprender ahora que cualquier dato que se robe durante un ataque de ransomware quedará comprometido para siempre. Sencillamente, no hay ningún motivo para pagarle a los delincuentes por los delitos que cometen.

Debería dar por sentado que su empresa recibirá ataques de ransomware. Si el ataque tiene éxito, debería tener un plan para no pagar el rescate.

Proteger su empresa de los ataques de ransomware se basa en proteger sus datos. Puede desglosarlo en tres áreas de interés: proteger sus credenciales, asegurar sus aplicaciones web y creando copias de seguridad de sus datos. Echemos un vistazo más de cerca a cada uno de estos pasos.

Exigencias del ransomware



Paso 1: Proteja sus credenciales

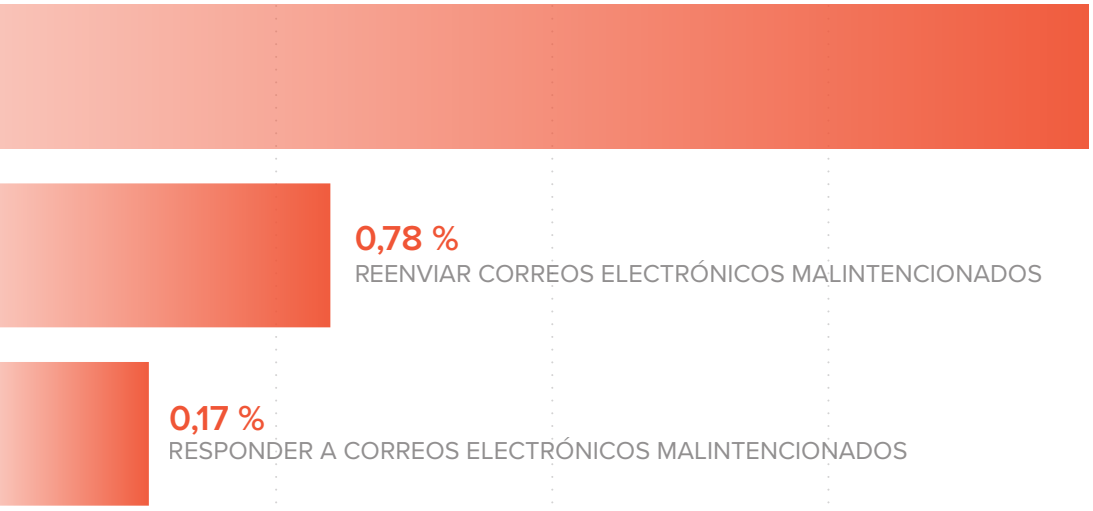
En primer lugar, el ransomware confía en filtrar el correo electrónico o asegurar las credenciales. Con los miles de nombres de usuario y contraseñas disponibles en línea, este primer paso puede resultar asombrosamente fácil. Los atacantes utilizan estas credenciales robadas para acceder a sus sistemas.

Barracuda

Como el phishing es el principal vector de ataque del ransomware, debe mantener una cultura de precaución alrededor de la seguridad de las credenciales. Desarrolle un proceso para formar a los usuarios en la seguridad del correo electrónico y desplegar tecnología antiphishing que pueda identificar y marcar cualquier actividad inusual. Si el atacante no puede acceder a las credenciales, será mucho más difícil escalar el ataque desde el phishing al ransomware.

Los ataques de phishing funcionan porque a la gente le gusta hacer clic en todo. Los hackers diseñan los ataques con mucho cuidado a medida de sus víctimas recopilando la información personal de dominio público sobre ellos y jugando con su sentido de la urgencia para recibir una respuesta. Los atacantes solo necesitan que una persona de dentro de la organización haga clic en el enlace o abra un archivo adjunto. Las investigaciones más recientes de Barracuda demuestran que, de media, el 3 % de la gente que recibe un correo electrónico de phishing hará clic en el enlace. Normalmente, el objetivo del ataque es capturar las credenciales de la cuenta, lo que permite al hacker moverse de forma lateral por toda la empresa y realizar un ataque de ransomwarer a toda la organización.

Proteger las credenciales y el acceso exige un enfoque de doble estrategia: en primer lugar, invertir en herramientas de detección y respuesta y, después, centrarse en formar a sus usuarios.



2,94 %
HACER CLIC EN EL ENLACE DE UN CORREO ELECTRÓNICO MALINTENCIONADO

0,78 %
REENVIAR CORREOS ELECTRÓNICOS MALINTENCIONADOS

0,17 %
RESPONDER A CORREOS ELECTRÓNICOS MALINTENCIONADOS

Fuente: Foco de amenazas: Amenazas de correo electrónico tras la entrega

Barracuda

Herramientas de detección y respuesta

Su tecnología de protección del correo electrónico debería centrarse, no solo en la detección de contenido malintencionado a través de enlaces o archivos adjuntos, sino también en reconocer cuándo utilizan los ataques tácticas de ingeniería social diseñadas para burlar la tecnología de filtrado y engañar a los usuarios para que hagan algo. Debería buscar intenciones malintencionadas dentro de un correo electrónico, incluso en los casos en los que no incluya contenido malintencionado. La seguridad de correo electrónico que utiliza algoritmos de aprendizaje automático puede detectar ataques de ingeniería social con un mayor grado de precisión, puesto que busca la más mínima desviación de los patrones de comunicación habituales.

La protección de sus credenciales de usuario no puede llevarse a cabo sin la protección adecuada frente a la usurpación de cuentas. La autenticación multifactorial (MFA) sigue siendo una práctica recomendada y es algo que debería adoptar cualquier organización de hoy en día. Sin embargo, no es una bala de plata; no siempre funciona. Los atacantes intentan encontrar formas de sortear la MFA bien engañando a los usuarios para que instalen malware en sus dispositivos de verificación bien dándoles un acceso de aplicaciones falso a sus cuentas. Las organizaciones necesitan disponer de protección frente a la usurpación de cuentas que identificarán y alertarán rápidamente en caso de existir actividad malintencionada, tales como inicios de sesión sospechosos o ataques lanzados desde cuentas comprometidas.

Proteger las credenciales y el acceso exige un enfoque de doble estrategia: en primer lugar, invertir en herramientas de detección y respuesta y, después, centrarse en formar a sus usuarios.

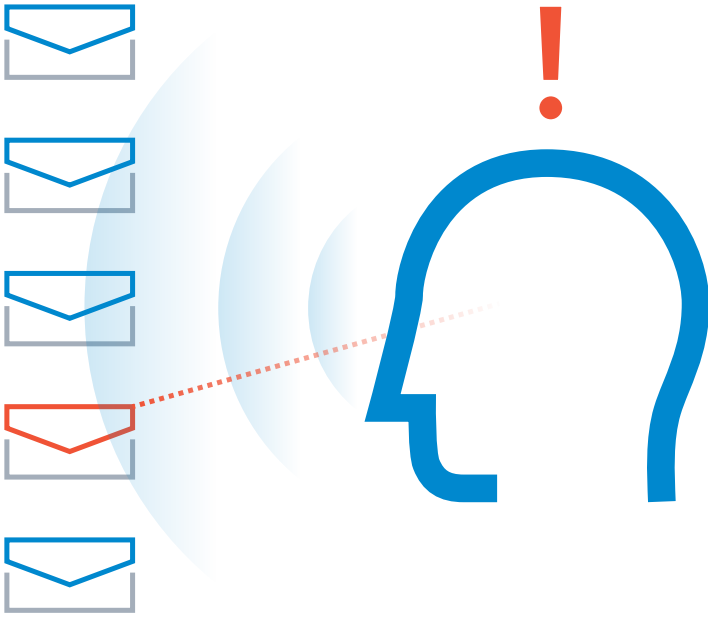
Barracuda

Formación de los usuarios

Como última línea de defensa, resulta crucial formar a sus empleados en cómo reconocer esos ataques e informar de ellos. Convierta la formación en concienciación sobre la seguridad y las simulaciones de phishing en parte de su estrategia de seguridad de correo electrónico. Históricamente, los ataques de phishing se asociaban únicamente con el correo electrónico, pero hoy en día, los ciberdelincuentes utilizan otros canales, como los SMS y la voz. Utilice la simulación de suplantación de identidad de correos electrónicos, buzón de voz, y SMS para formar a los usuarios para que sepan identificar los ciberataques. A continuación, pruebe la eficacia de la formación y evalúe a los usuarios más vulnerables a los ataques.

Asegúrese de que la formación en ciberseguridad no se haga solo como parte del primer día de las nuevas contrataciones. Debe tratarse de algo continuo para mantener a los empleados al día de cómo evolucionan las amenazas. Por ejemplo, las bandas de hoy en día utilizan ingeniería social sofisticada que resulta difícil de detectar. Los ataques de suplantación de identidad personalizada van dirigidos a un individuo o parte de un departamento, como el financiero, con mensajes muy personalizados.

Resulta crucial que sus necesidades de formación se ganen la confianza de su personal y que quieran dar la voz de alarma, incluso si se debe a un error que ellos mismos hayan cometido por accidente. Es posible que sea necesario impartir una formación complementaria, pero no penalice a las personas que comuniquen una alerta. Hay muchos ataques que no se comunican porque el personal teme que se le culpe por hacer clic en un enlace o abrir un archivo adjunto. Debe valorarse positivamente y premiarse a aquellas personas que avisan cuanto antes.



Paso 2: Asegure sus aplicaciones web y los accesos

El cambio al teletrabajo ha provocado que muchas aplicaciones salgan de los centros de datos y entren en Internet. En algunas ocasiones, las prisas por mantener los servicios de las empresas en funcionamiento han provocado que se deje de lado la seguridad, y los ciberdelincuentes están listos para aprovechar esas vulnerabilidades.

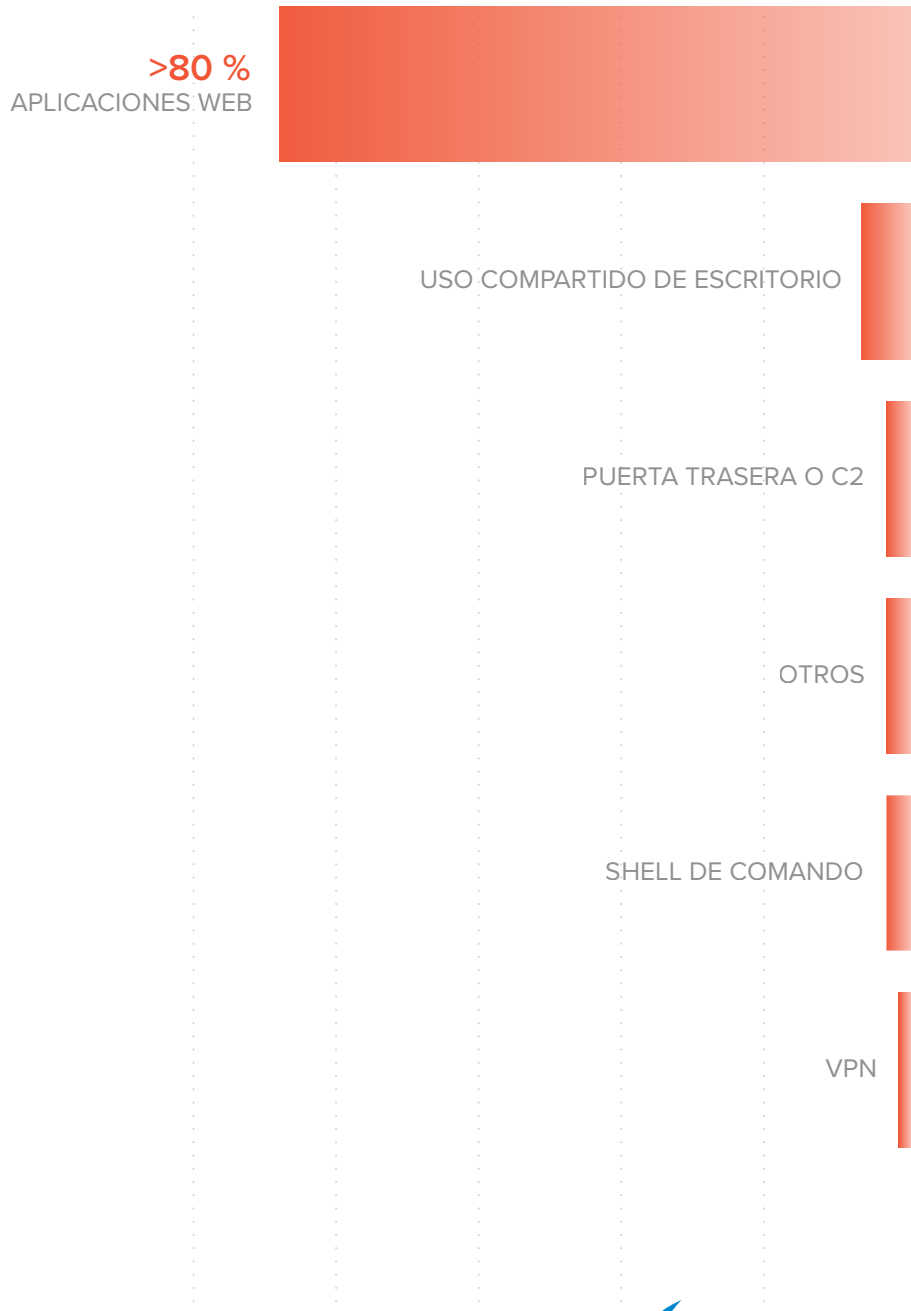
Barracuda

El informe Verizon 2021 Data Breach Investigations Report muestra que para los hackers, las aplicaciones web son el mayor vector de ataque en uso y suponen más del 80 % de todas las filtraciones de datos.

Las aplicaciones en línea, como los servicios de uso compartido de archivos, formularios web y sitios de comercio electrónico pueden verse comprometidas por los atacantes. Las aplicaciones web reciben ataques a través de la interfaz de usuario o una interfaz API. A menudo, estos ataques implican relleno de credenciales, ataques de fuerza bruta o vulnerabilidades de OWASP. Una vez que la aplicación se haya visto comprometida, el atacante puede introducir ransomware y otro tipo de malware en el sistema. Esto puede seguir moviéndose de forma lateral para infectar aún más su red, así como a los usuarios de su aplicación.

Es importante entender que proteger las aplicaciones y los accesos es igual de importante que la seguridad del correo electrónico a la hora de defenderse del ransomware y otro malware. El Open Web Application Security Project (OWASP) trabaja para aumentar la concienciación pública ante las vulnerabilidades de las aplicaciones más comunes que pueden aprovecharse en un ataque de ransomware.

Fuente: Verizon 2021 Data Breach Investigations Report



Un ejemplo reciente es el ataque de la cadena de suministro de ransomware de REvil que sucedió en julio de 2021. Se aprovecharon las vulnerabilidades en una aplicación MSP de Internet orientada al público para difundir ransomware a sus clientes. En este caso, como la aplicación tenía permisos profundos, el ransomware pudo difundirse muy fácilmente y tuvo un gran impacto antes de que pudiera detenerse. Este tipo de ataque podría ocurrir a través de cualquiera de sus aplicaciones de Internet orientadas al público; los atacantes entran en la aplicación y se mueven de forma lateral para causar estragos. Un escenario similar podría producirse en el caso de que dejara sus sistemas RDP abiertos a Internet, incluso si cambia el puerto determinado. Los atacantes utilizan credenciales recopiladas en dichos sistemas RDP para intentar infectar toda la red con ransomware a través de este vector de ataque desprotegido.

Hasta

1500

empresas se vieron afectadas por el ataque de la cadena de suministro de REvil

Barracuda.

4 vectores de ataque para aplicaciones web

Las aplicaciones son ahora el principal objetivo del ransomware, por lo que existen cuatro vectores de ataque que debe proteger: acceso a la aplicación, vulnerabilidades de la aplicación web, acceso a infraestructuras y movimiento lateral.

1. Acceso a la aplicación

Para identificar si el acceso a la aplicación es un problema que pueda comprometer a la actualización, hay varias preguntas clave que debe responder.

- **¿Los trabajadores que tiene contratados o que teletrabajan utilizan dispositivos no gestionados o siguen la política de Traiga su propio dispositivo (Bring Your Own Device, BYOD)?** Los dispositivos móviles son el ejemplo más claro. Un dispositivo BYOD o no gestionado puede verse comprometido y utilizarse para extraer credenciales o atacar la aplicación.
- **¿Tiene visibilidad de todos los usuarios y dispositivos de la red?** Por ejemplo, debe saber quién se conecta a su red de invitados y si está correctamente segmentado.
- **¿Tiene un registro de auditoría de quién accede y cuándo lo hace?** Debe poder mirar atrás y ver quién accede a sus aplicaciones, cómo accede a ellas y si cuenta con los permisos adecuados.

Si algún dispositivo que no tenga permiso para estar en la red está conectado a su red y alguien ha configurado herramientas para realizar un ataque informático en ella, eso puede suponer un grave problema. Y si no tiene ninguna visibilidad sobre todo esto, puede ser un auténtico reto identificar quién accede a qué y cuál es la vulnerabilidad, por lo que no podrá cerrar la superficie vulnerable ni bloquear el acceso al atacante.

2. Vulnerabilidades de la aplicación web

Las vulnerabilidades de la aplicación web constituyen el siguiente vector de ataque que necesita evaluar para determinar el grado de seguridad de sus aplicaciones.

Plantéese las siguientes preguntas:

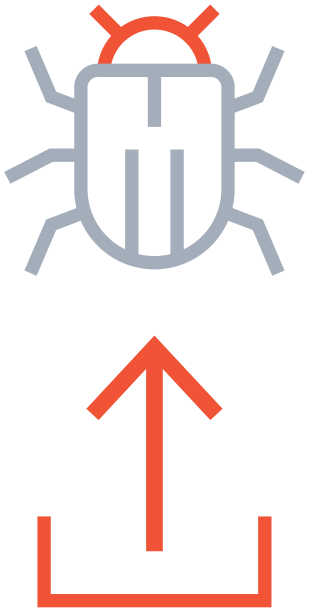
- ¿Qué grado de seguridad tiene su sitio web? ¿Cuándo lo actualizó por última vez?
- ¿Tiene formularios en su sitio web? ¿Qué hace para evitar los ataques a través de los formularios?
- ¿Acepta que se carguen elementos en su sitio web? ¿Cómo se protege del malware?

Activar HTTPS no es suficiente para mantener protegido su sitio. Simplemente significa que un atacante no puede espiar a alguien cuando inicia la sesión en su sitio para robar sus credenciales. Los ciberdelincuentes pueden seguir realizando un ataque de fuerza bruta dentro de ese marco de HTTP para intentar averiguar los inicios de sesión correctos de su sitio.

Disponer de CAPTCHA o reCAPTCHA delante de los formularios de inicio de sesión de su sitio también resulta insuficiente porque es fácil que la gente automatice y burle estos servicios.

Los inicios de sesión o IP que limitan la velocidad son otra medida de seguridad que los hackers pueden saltarse fácilmente mediante ataques bajos y lentos y varios sistemas de automatización.

Si acepta que se carguen archivos, ese es otro problema que debe resolver. Es bastante común que los atacantes intenten infiltrarse en un sitio web cargando un virus o malware de ransomware.



3. Acceso a infraestructuras

Desde el comienzo de la pandemia de la COVID-19, muchas organizaciones han utilizado las VPN para dar acceso a aplicaciones alojadas internamente. Esto sucede cuando no existe ningún reemplazo de SaaS para algunas aplicaciones autoalojadas. Ofrecer acceso a la VPN desde casa es el único modo de mantener la empresa en funcionamiento. Si no se adoptan unas prácticas de acceso e identificación adecuadas, este enfoque es una bomba de relojería que está a punto de explotar. Hay muchas credenciales robadas que pueden compartir nombres de usuarios y contraseñas que se utilizan para acceder a la infraestructura; esto supone, por tanto, un riesgo real que podría exponer su red, sus aplicaciones y sus datos.

4. Movimientos laterales

Después de comprometer su aplicación o infraestructura con credenciales robadas, los atacantes intentarán entrar más profundamente en la red y lanzar más ataques desde ahí, por lo que esto se convierte en el cuarto vector de ataque que debe resolver. Responda a las siguientes preguntas:

- ¿Está su red corporativa dividida en segmentos correctamente protegidos?
- ¿Tiene activada una autenticación multifactorial para acceder a la red?

Establecer una segmentación adecuada para la red conlleva mucho tiempo y esfuerzo, y es fácil encontrar motivos para abrir hasta dos segmentos y permitir el acceso de un segmento a otro. En última instancia, esto conduce a que el acceso esté abierto de formas que no quería que estuviera.

La autenticación multifactorial añade otra capa de protección importante para detener a los atacantes y que no puedan acceder a la red.

Cómo aprovecha un ataque de ransomware las vulnerabilidades de una aplicación

Aquí presentamos otro escenario posible: Una serie imaginaria, pero a la vez realista, de los pasos que podría dar un atacante para aprovecharse de la baja seguridad de la aplicación para crear un ataque de ransomware efectivo. El ataque va a intentar realizar una estafa de cupones aprovechando la ola emergente de plugins de cupones para navegadores.

Paso 1

El atacante crea un sitio web que imita un sitio web legítimo de cupones. El atacante se hace pasar por un popular sitio de cupones, que es relativamente sencillo utilizando la suplantación de dominios y el raspado de páginas web automatizado. Llamemos a este sitio falso Sitio Web X.

Paso 2

El atacante sondea una o más de las 10 principales vulnerabilidades de OWASP para robar credenciales de un sitio web legítimo pero mal protegido de la empresa, que llamaremos sitio web Y. Las vulnerabilidades como la autenticación rota y la exposición de datos sensibles permiten al hacker recoger las credenciales de los usuarios y otra información confidencial del sitio web Y.

Paso 3

El atacante utiliza las credenciales robadas para iniciar un ataque de relleno de credenciales credenciales contra un sitio web legítimo de comercio electrónico, que designaremos como sitio web Z. Se trata de un ataque automatizado que puede ejecutarse lentamente durante varias semanas. Este ataque intenta hacer coincidir las credenciales robadas con las cuentas reales de estos sitios.

Paso 4

Si el ataque encuentra una coincidencia y el hacker puede entrar en la cuenta de la víctima, el siguiente paso es utilizar esa cuenta para publicar reseñas reseñas de productos populares en el sitio web Z. Un ejemplo común en este paso es “¡Este producto es genial! Ahorra un 50 % de este precio con este cupón haciendo clic aquí”. El enlace al cupón lleva al visitante al sitio web X, el sitio web falso del primer paso.

Barracuda

Paso 5

Las víctimas potenciales entran en el sitio web Z y proceden a hacer clic en la reseña del producto, siguiendo el enlace al sitio web X, sin saber que han sido llevados a un sitio de estafa a menos que miren con mucho cuidado el nombre del dominio, la URL, el certificado del sitio y otros detalles. Las víctimas que confían en el sitio proporcionan entonces su información de contacto a cambio del cupón. El atacante tiene ahora la dirección de alguien que espera un correo electrónico de ese sitio web. El atacante se está ganando la confianza de la víctima y ésta ha bajado la guardia.

Paso 6

La víctima recibe un correo electrónico personalizado sobre el producto y el cupón, con un archivo adjunto que se le indica que debe instalar para que el cupón funcione. Este archivo adjunto puede ser un ejecutable o una extensión del navegador que utiliza JavaScript para llevar a cabo el ataque. Como que este correo electrónico está completamente personalizado y el destinatario lo espera, es probable que se permita a través de las defensas de correo electrónico tradicionales. El sistema operativo de la víctima le pide que no instale ejecutables que no sean de confianza, pero en este punto la víctima probablemente confía plenamente en el atacante y hace clic.

Paso 7

La víctima instala el archivo adjunto y se lanza el ataque de ransomware. Una vez instalado un ejecutable, se pueden lanzar varios tipos de ataques, por ejemplo infectar el registro de arranque maestro, cifrar la tabla del sistema de archivos e incluso impedir el arranque del sistema operativo. Poco después, a la víctima le llegará el requerimiento de pago. El atacante normalmente intentará ampliar este ataque y cosechar más credenciales y cualquier otro dato que se pueda encontrar en la red. Una vez realizado esto, el ransomware cifrará los datos de la red.

En este ejemplo, el ransomware triunfa porque las vulnerabilidades de seguridad de la aplicación en varios sitios web permitieron construir el escenario convincente: el raspado de la web de un sitio legítimo en el primer paso, las credenciales robadas en el segundo, el relleno de credenciales en el tercer paso, el spam de comentarios y la URL malintencionada en los pasos cuatro y cinco, y la instalación del ejecutable en el séptimo paso. Una seguridad adecuada de la aplicación en cualquiera de estos pasos podría haber detenido este ataque.

Barracuda

Cómo asegurar sus aplicaciones y los accesos

Protección de su red

Evite que el ransomware se propague dentro de su red con la segmentación de la red y la prevención de intrusiones. Busque una solución de firewall de nueva generación que:

- Proporciona una seguridad multicapa que bloquea las amenazas avanzadas, incluidos los ataques de día cero
- Incluye la prevención de intrusiones y el sandboxing del malware
- Proporciona una potente segmentación de la red para evitar el movimiento lateral dentro de ella

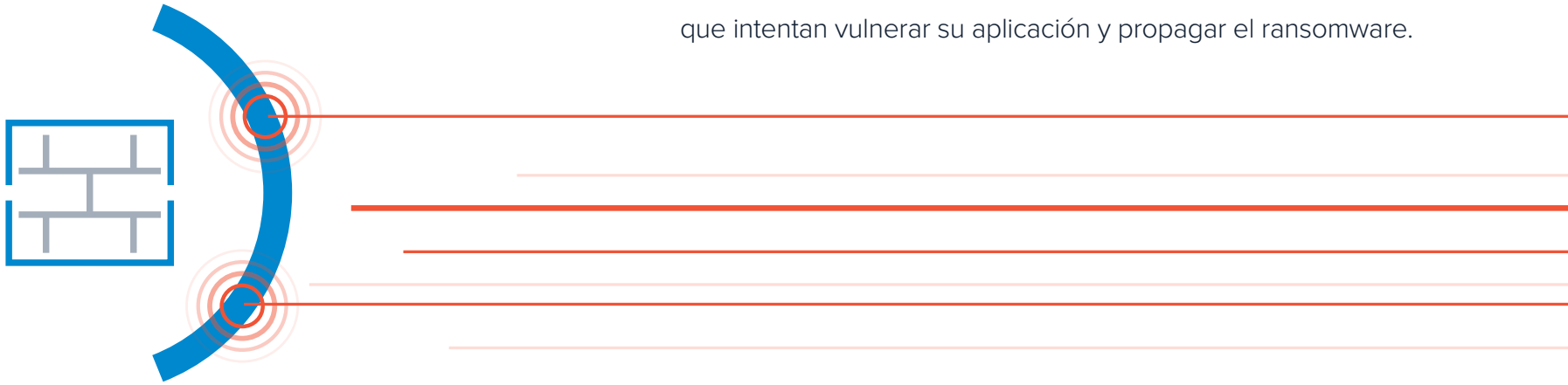
Asegure el acceso a la aplicación

Debe proteger el acceso de la aplicación con una solución Zero Trust Network Access (ZTNA) que proporcione un acceso seguro a las aplicaciones y las cargas de trabajo desde cualquier dispositivo y desde cualquier ubicación.

Busque una solución que:

- Verifica continuamente que solo la persona adecuada con el dispositivo adecuado puede acceder a los recursos de la empresa.
- Aplica un control de acceso basado en funciones y atributos para proporcionar un acceso con mínimos privilegios.

Al bloquear el acceso no autorizado, ZTNA detiene a los atacantes que intentan vulnerar su aplicación y propagar el ransomware.



Barracuda

Proteja sus aplicaciones web

Una de las mejores maneras de desplegar la seguridad de las aplicaciones es con un cortafuegos de aplicaciones web (WAF) para proteger su software, sus usuarios y sus datos dondequiera que estén. De esta forma, se detendrán ataques de bots, los ataques de denegación de servicio, y le dará una visión mucho más amplia de lo que está pasando. Busque una solución que tenga las siguientes características:

Fácil de desplegar y adaptar a su entorno

Un WAF no puede protegerle completamente si no es capaz de configurarlo para su entorno.

Escalable

El crecimiento del negocio, la transformación digital y otros factores pueden aumentar la demanda de sus aplicaciones y sitios web. Su WAF debe ser capaz de crecer con su negocio según sea necesario.

Protección integral contra las amenazas avanzadas

La protección OWASP Top Ten y la protección DDoS de la capa de aplicación son los pilares que uno debe esperar de un buen WAF. Para una protección completa, busque una solución que defienda contra ataques de día cero, relleno de credenciales, fuga de datos, bots maliciosos, etc.

Fácil de actualizar

Un WAF debe poder actualizar periódicamente el firmware para mejorar la seguridad y las capacidades del dispositivo. Una solución alojada que se actualiza automáticamente sin intervención del administrador es ideal.

Inteligencia continua sobre amenazas

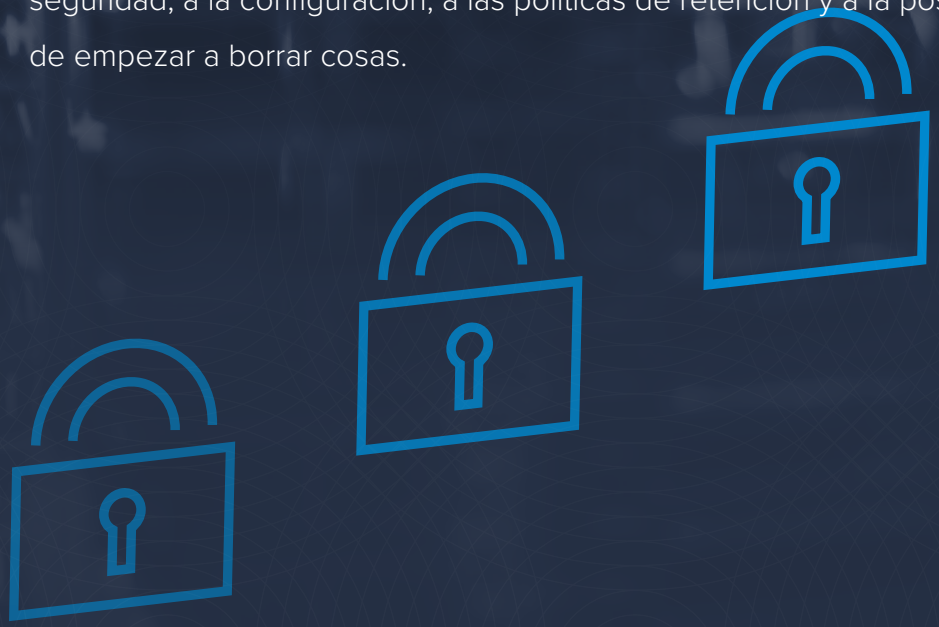
Cada día se desarrollan nuevos ataques, que pueden extenderse por todo el mundo en cuestión de horas. Su WAF debe recibir actualizaciones en tiempo real sobre estos ataques y emplear el aprendizaje automático para adaptarse a las variantes.

Al bloquear las vulnerabilidades comunes de las aplicaciones web y las amenazas de día cero, un buen cortafuegos de aplicaciones web impide que el ransomware se introduzca en sus sistemas.

Paso 3: Realice copias de seguridad de sus datos

Cualquier estrategia seria de protección contra el ransomware debe empezar por pensar en las copias de seguridad y la recuperación de desastres. El problema es que los delincuentes también lo saben.

Las soluciones de copia de seguridad son un foco de atención para los atacantes durante el periodo de “acecho”, cuando exploran la red. La consola de administración de copias de seguridad es especialmente importante para ellos porque les da acceso a los programas de copias de seguridad, a la configuración, a las políticas de retención y a la posibilidad de empezar a borrar cosas.



Barracuda

Los atacantes también tienen como objetivo el propio almacenamiento de copias de seguridad, con la esperanza de eliminar su servidor de copia de seguridad principal y cualquier copia de seguridad secundaria de recuperación de desastres que mantenga. Una vez que capturan las contraseñas de Active Directory para que nadie pueda entrar en sus cuentas, es cuando pueden apretar el gatillo. Tienen el control.

También sigue existiendo la idea errónea, demasiado común, de que porque los datos están en la nube no pueden verse afectados por el ransomware. Eso simplemente no es cierto.

Por ejemplo, es fácil engañar a un niño que navega por la web en su tablet del colegio o en su portátil en casa para que haga clic en un enlace malintencionado por accidente. Si ese dispositivo está conectado y sincronizado con OneDrive como parte de la cuenta de Office 365 de la escuela, un archivo de ransomware puede subirse automáticamente a OneDrive y cifrar los archivos y datos de la escuela guardados en la nube de Microsoft.

Considere la recuperación de desastres como una parte crucial y estratégica de su infraestructura. Pruébelo de forma periódica y realista: eso significa hacer una restauración real, no solo comprobar que funciona.

Barracuda

También hemos visto ejemplos en los que SharePoint, Exchange y otras fuentes de datos se han visto afectadas. Y si las unidades de red se asignan a las bibliotecas de documentos en Office 365 utilizando la función “abrir con el Explorador”, el ransomware también puede buscar e infectar los archivos de las unidades conectadas.

Incluso los datos de la nube y el SaaS pueden cifrarse con ransomware. Microsoft garantiza la disponibilidad del servicio, pero recomienda hacer una copia de seguridad de los datos mediante una solución de copia de seguridad de terceros. Sus datos pueden estar guardados en Microsoft Office 365, pero Office 365 no está diseñado para recuperar instancias enteras como puede ser necesario tras un ataque de ransomware.

Por lo tanto, es necesario defender y aislar correctamente los datos de las copias de seguridad. Piense en la frecuencia con la que hay que replicar los sistemas y en la rapidez con la que se pueden reconstruir los sistemas a partir de esas imágenes.

Hay que asegurarse de que sea posible la restauración de los sistemas a partir de las versiones de copia de seguridad en un plazo razonable y con información suficientemente actualizada. Eso significa que tienes que tomar el control y hacerlo. No basta con comprobar los registros para ver si los datos se replican con suficiente frecuencia y precisión.

Hay que hacer simulacros reales para demostrar que los sistemas funcionan. Puede elegir un departamento, o incluso una sola aplicación, en lugar de detener todo. Pero es fundamental que tenga plena confianza en que los sistemas volverán a funcionar en el momento oportuno.

Este es su mecanismo de protección. Incluso si todo lo demás falla, si tiene una copia de seguridad realmente actualizada y segura, los delincuentes no podrán detenerle.

Considere la recuperación de desastres como una parte crucial y estratégica de su infraestructura. Pruébelo con regularidad y de forma realista: eso significa hacer una restauración real, no solo comprobar que funciona.

Qué necesita de su solución de copias de seguridad

Para mitigar los riesgos asociados al ransomware, necesita una solución de copia de seguridad completa que ofrezca lo siguiente:

Almacenamiento inmutable

Incluso si el atacante obtiene acceso a sus copias de seguridad, no puede modificar o eliminar esos datos.

Nube de aire

Mantenga una copia de seguridad en una nube segura que resida en una red aislada.

Autenticación multifactorial (MFA)

Protege las cuentas y credenciales utilizadas para acceder a la copia de seguridad.

Redundancia

Replique sus copias de seguridad locales y en la nube en otra ubicación.

Control de acceso basado en funciones

Siga el principio del mínimo privilegio para todos los usuarios que tienen acceso al sistema de copia de seguridad.

Barracuda.

Conclusión

Es posible que su empresa tenga un seguro cibernético u otros recursos para pagar un rescate, pero es extremadamente peligroso asumir que si paga el rescate, se restaurarán sus datos. No hay garantía de que los hackers vayan a descifrar los datos cuando se paga un rescate, e incluso si lo hacen, las últimas investigaciones demuestran que el 80 % de las organizaciones que han pagado un rescate han recibido ataques de nuevo.

Aunque hayas hecho todo lo que se ha indicado anteriormente, seguirás recibiendo ataques. Incluso con la mejor protección, es de sentido común prepararse para lo peor. Los delincuentes tienen millones para invertir en acceder a sus sistemas. La única forma sensata de prepararse es asumir que un día entrarán.

- ¿Quién forma parte de su equipo de respuesta al ransomware?
- ¿A quién hay que llamar si ocurre algo durante un fin de semana o un día festivo?
- ¿Quién está al mando?
- ¿Cuándo debe comunicarse a los clientes y proveedores?
- ¿Quién presta asesoramiento jurídico?
- ¿Hay que avisar a una entidad reguladora o a la policía?
- ¿Necesita a alguien de relaciones públicas que esté implicado desde el principio?

Tiene que pensar en lo que pasará cuando llegue ese día. Necesita un plan para no pagar el rescate.

Es como un simulacro de incendio: el momento de practicar no es cuando la oficina está en llamas. Pero los ataques actuales y más probables cambian con el tiempo, por lo que su estrategia y tácticas de defensa necesitarán una actualización periódica. Descargue nuestra lista de comprobación sobre el ransomware para ayudarle a poner en marcha su plan.

Barracuda

Esté preparado para responder a un ataque

Hay que pensar en lo que ocurre en el momento en que se identifica un ataque y en lo que ocurre si ese ataque se convierte en una filtración. ¿Se puede contener o restringir a una parte de su infraestructura deteniendo el tráfico de la red? ¿Necesita desconectar temporalmente los sistemas? Si es así, ¿quién se responsabiliza de ello?

La velocidad es absolutamente esencial en este caso. Velocidad enfocada. No querrá esperar a que su CTO le devuelva la llamada. Todo el mundo necesita saber qué hacer ahora mismo.

Si esto ocurre con la suficiente rapidez, es posible que incluso pueda impedir que se produzca el cifrado. También necesita un plan para comprobar rápidamente todos sus sistemas y obtener una visión definitiva de lo que está ocurriendo.

Los atacantes modernos tienden a utilizar más de un tipo de ataque simultáneamente. Es posible que esté ocupado lidiando con un ataque de denegación de servicio mientras un ataque de ransomware se dirige a otra parte. Una vez que entienda qué ha sucedido, y dónde, puede empezar a pensar en lo que tiene que hacer para erradicar el malware y volver a restablecer los sistemas en línea.

Una vez que se han restaurado los sistemas y los datos, ya sea a partir de una copia de seguridad o aislando el ataque en el tiempo, y se ha comprobado que no hay datos dañados ni falta ninguno, es el momento de empezar la investigación forense.

Evalúe cómo funcionó su respuesta contra un ataque real. Analiza lo que ha funcionado bien, lo que ha funcionado solo porque has tenido suerte y lo que te ha faltado. Piense en cómo mejorar y acelerar su respuesta la próxima vez.

Con los sistemas adecuados, tendrá una gran cantidad de datos forenses que considerar. Incluso puede tener suficiente información para que la policía empiece a investigar. Independientemente de los datos que tenga, debe dedicar el tiempo necesario para informar al equipo de respuesta y reflexionar sobre las lecciones aprendidas.

Una vez más, no se trata solo de tecnología, sino también de personas y procesos. ¿Es necesario volver a repasar la formación del personal? ¿Ha funcionado bien su equipo de respuesta, o necesita ser reforzado?

Manténgase informado

Las estrategias de defensa actuales deben ser activas, no solo reactivas. Necesita la mayor transparencia posible en sus sistemas de seguridad. Hay que observar qué ocurre, cuándo y con qué frecuencia. Debe prestar atención a sus compañeros: los atacantes de ransomware suelen dirigirse a un mercado vertical o a una geografía específica. También debe mantenerse al día sobre las últimas amenazas, tendencias y noticias del sector a través de recursos como el blog de Barracuda.

Los datos son cruciales para el éxito de una estrategia de seguridad: es probable que la postura o el perfil de su organización cambie con el tiempo. Tiene que estar preparado e informado para hacer ese cambio cuando sea necesario. La seguridad como servicio puede ayudar a eliminar parte del trabajo pesado de mantenerse al día con los desarrollos, especialmente cuando el panorama actual de la ciberseguridad está cambiando más rápido que nunca.

Para algunas empresas con una postura muy activa, o con un perfil de alto riesgo, esto podría significar tener personal a tiempo completo haciendo trabajos de inteligencia para obtener una alerta temprana de posibles ataques.

Pero para la mayoría de las organizaciones esto es más de lo que se requiere. Elija el socio adecuado y ponga en marcha los aspectos básicos. Los atacantes reales -a diferencia de lo que vemos en las películas y la televisión- no son genios del mal a los que les encanta destrozar los sistemas de seguridad más elaborados. En su mayor parte, buscan un pago fácil de alguien que ha sido negligente y no ha prestado atención o no ha invertido en la seguridad adecuada.

Tomar esas tres medidas -proteger sus credenciales, sus aplicaciones web y el acceso a ellas, y hacer una copia de seguridad de los datos- no garantizará que no reciba ningún ataque de ransomware. Pero le garantizará que nunca tendrá que pagar un rescate para recuperar sus datos.

Sobre Barracuda

En Barracuda, luchamos por hacer del mundo un lugar más seguro.

Estamos convencidos de que toda empresa merece disfrutar de soluciones de seguridad en la nube específicas para su labor que sean fáciles de adquirir, instalar y utilizar. Protegemos los correos electrónicos, las redes, los datos y las aplicaciones con soluciones innovadoras capaces de crecer y adaptarse a la experiencia de nuestros clientes.

Más de 200 000 organizaciones en todo el mundo confían en Barracuda para su protección —a unos niveles a los que puede que ni ellas sepan que están en riesgo—, de modo que puedan centrarse en llevar su negocio siempre un paso más allá. Para obtener más información, acceda a barracuda.com.

Barracuda
Your journey, secured.