Febrero 2026

Informe de amenazas

El informe sobre amenazas globales de Managed XDR

Cómo los atacantes apuntan a las organizaciones y brechas de seguridad

Barracuda®
Your business, secured.

Contenido

Introducción

Las herramientas avanzadas y los expertos de Barracuda Managed XDR supervisan y protegen las redes de los clientes las 24 horas del día, 365 días al año. Cada minuto, la solución detecta y responde a una advertencia de seguridad. Cada 15 minutos, envía una alerta a un cliente, y cada 60 minutos, bloquea automáticamente una amenaza de alta gravedad, como un dispositivo comprometido o un incidente de ransomware en desarrollo.

Si no se resuelve, una sola señal de alerta puede convertirse rápidamente en un incidente generalizado que interrumpe las operaciones, reduce la productividad, compromete datos sensibles y daña la estabilidad financiera y la reputación de la marca. Ninguna organización es inmune; los atacantes apuntan a empresas de todos los tamaños, en todos los sectores y geografías.

Hay muchos factores que pueden hacer que los objetivos sean vulnerables: brechas de seguridad, dispositivos maliciosos, sistemas sin parches, descuidos, configuraciones erróneas... y la falta de tiempo y recursos para detectar la intrusión, eliminar a los atacantes y cerrar la puerta tras ellos.

El propósito de este informe es ayudar a los profesionales de TI y seguridad en organizaciones con recursos limitados a comprender mejor cómo los atacantes apuntan a posibles víctimas y los puntos débiles de seguridad que intentarán explotar.

Proporcionamos ejemplos de incidentes del mundo real y recomendaciones sobre cómo mantenerse seguro y ciberresiliente.

En un mundo en el que las amenazas cibernéticas son cada vez más complejas y evasivas, las organizaciones no se enfrentan solas al desafío. Su proveedor de seguridad cuenta con las herramientas y los conocimientos necesarios para ayudarle a abordar los problemas identificados en este informe, y le acompañamos en cada paso del camino.

Los datos subyacentes

Las conclusiones detalladas en este informe están basadas en el conjunto de datos único de Barracuda Managed XDR con más de dos billones de eventos de TI recopilados durante 2025, casi 600.000 alertas de seguridad y más de 300.000 terminales, cortafuegos, servidores, activos en la nube y otros elementos.

Principales conclusiones

100%

de los incidentes de seguridad involucraron al menos un endpoint no protegido o malicioso

96%

de los incidentes que involucraron movimiento lateral terminaron con el lanzamiento de ransomware

66%

de los incidentes involucraron la cadena de suministro o un tercero (frente al 45% en 2024)

3 horas

el ataque de ransomware más rápido, desde la brecha hasta el cifrado

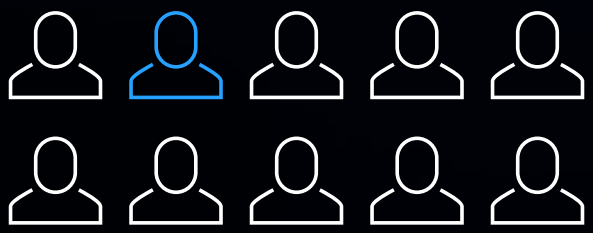
90%

de los incidentes de ransomware explotaron firewalls

13 años

la vulnerabilidad más detectada es un error de 2013 en un cifrado obsoleto

1 de cada 10



vulnerabilidades detectadas tienen un exploit conocido

Cómo los atacantes apuntan a las organizaciones

Las soluciones efectivas de detección y respuesta extendida (XDR) están diseñadas para interceptar amenazas entrantes en la etapa más temprana de la cadena de ataque: el punto de compromiso y acceso inicial. Barracuda Managed XDR no es una excepción. También proporciona visibilidad adicional en fases posteriores del ataque, incluyendo el movimiento lateral y el impacto. Esta amplia capacidad se refleja en el contenido de este informe.

A la cabeza de la lista de las amenazas más detectadas contra las organizaciones en los últimos 12 meses se encuentran los ataques dirigidos a las identidades y la seguridad de las mismas.

Esto incluye inicios de sesión inusuales o inesperados en una cuenta de usuario. Estas son conexiones que no corresponden al patrón de comportamiento típico del usuario en términos de dispositivo, ubicación o tiempo. Tales detecciones son un fuerte indicador de robo de credenciales y compromiso de la cuenta. Otras señales de alerta son los intentos de conexión desde una geolocalización bloqueada y la regla de 'viaje imposible', donde un usuario inicia sesión desde una segunda ubicación a la que nunca podría haber llegado en el tiempo transcurrido entre los inicios de sesión.

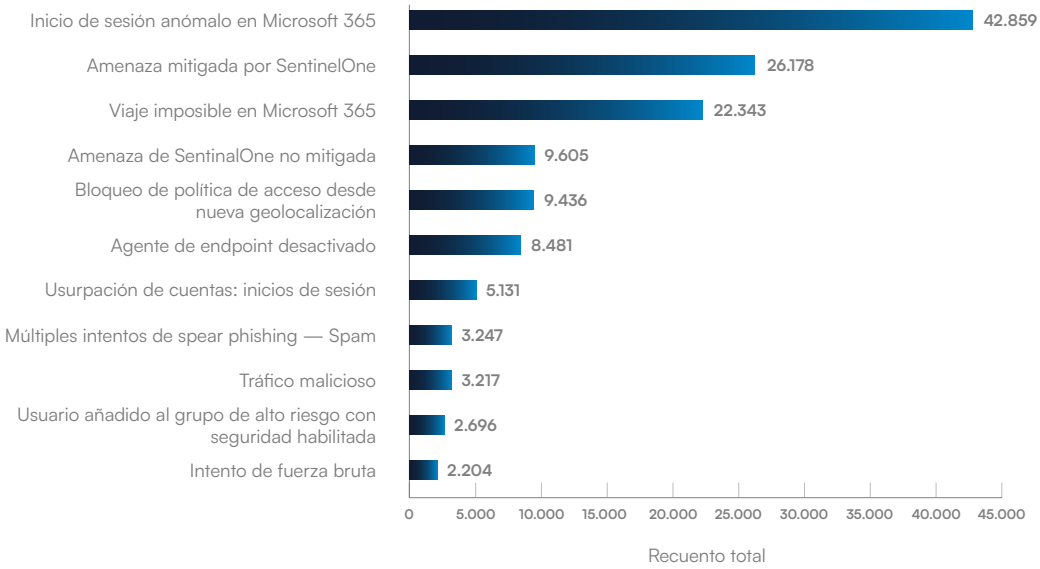


FIGURA 1

Principales detecciones de ataques contra organizaciones

La lista de principales detecciones también incluye actividades que podrían significar que una cuenta ha sido comprometida y los atacantes están en la red. Los equipos de seguridad deben investigar tales detecciones de inmediato. Incluyen señales que sugieren que alguien ha intentado eludir o desactivar la protección de endpoints y notificaciones de que un usuario ha sido añadido a un grupo sensible a la seguridad, lo que podría ser un atacante intentando escalar sus privilegios.

Cómo los atacantes manipulan los derechos de privilegio una vez dentro del sistema

La escalada de privilegios es crucial para los atacantes porque convierte el acceso limitado en control administrativo completo, lo que les permite desactivar defensas, moverse lateralmente a través de los sistemas y acceder a datos sensibles. El resultado puede ser un compromiso a gran escala y el lanzamiento de ransomware.

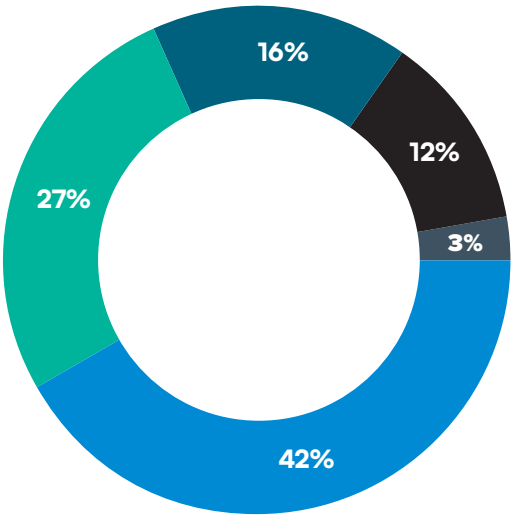


FIGURA 2

Cómo manipulan los derechos de privilegio los atacantes

- Windows: Se agregó un usuario a un grupo con derechos de seguridad de alto riesgo
- Windows: Se eliminó a un usuario de un grupo con derechos de seguridad de alto riesgo
- Microsoft 365: Se añadió un usuario como administrador global
- Microsoft 365: Se eliminó a un usuario como administrador global
- Firewall FortiGate: Se añadió un usuario como administrador

El firewall de Barracuda Managed XDR, las herramientas de seguridad de Windows y Microsoft 365 detectaron los siguientes comportamientos que indican un intento de escalada de privilegios:

Windows: Se añadió un usuario a un grupo con derechos de seguridad de alto riesgo (representando el 42% de las escaladas de privilegios sospechosas)

- **Lo que esto significa:** Se ha añadido un usuario a un grupo con permisos avanzados (por ejemplo, administradores de dominio).
- **Los atacantes pueden usarlo para:** Moverse lateralmente, desplegar malware o exfiltrar datos.
- **Cómo mantenerse seguro:** Supervise los cambios de grupo y gestione la asignación de todos los derechos de acceso privilegiado.

Windows: Se eliminó a un usuario de un grupo con derechos de seguridad de alto riesgo (27%)

- **Lo que esto significa:** Un usuario fue retirado de un grupo de alto privilegio.
- **Los atacantes pueden usarlo para:** Cubrir sus huellas después de la escalada de privilegios.
- **Cómo mantenerse seguro:** Investigue por qué se produjo la eliminación y verifique si hubo algún uso indebido antes de la eliminación.

Microsoft 365: Se agregó un usuario como administrador global (16%)

- **Lo que esto significa:** A alguien se le otorgó el nivel más alto de acceso en Microsoft 365.
- **Los atacantes pueden usarlo para:** Crear nuevas cuentas, robar datos o desactivar la seguridad.
- **Cómo mantenerse seguro:** Revisar los cambios en las funciones de los administradores, aplicar la autenticación multifactor (MFA) e introducir procesos adecuados de revisión y aprobación.

Microsoft 365: Se eliminó un usuario como administrador global (12%)

- **Lo que esto significa:** Alguien perdió sus derechos de administrador global.
- **Los atacantes pueden usarlo para:** Evitar la detección eliminando sus cuentas añadidas.
- **Cómo mantenerse seguro:** Verifique si el cambio fue autorizado y revise los registros de auditoría en busca de actividad sospechosa o uso indebido.

FortiGate Firewall: Se añadió un usuario como administrador del firewall (3%)

- **Lo que esto significa:** Se creó una nueva cuenta de administrador en el firewall.
- **Los atacantes pueden usarlo para:** Desactivar protecciones y abrir puertas traseras.
- **Cómo mantenerse seguro:** Confirme la legitimidad de la cuenta y aplique controles estrictos de administrador.

Informe de incidente: el archivo adjunto malicioso que condujo a un RAT

Se encontró un troyano de acceso remoto (RAT) en los sistemas de un cliente después de que un empleado descargara inadvertidamente un archivo ejecutable malicioso. El archivo intentó inmediatamente establecer persistencia: solicitó registrarse como un servicio de Windows, lo que le permitiría iniciarse automáticamente, ejecutarse en segundo plano y operar con acceso a nivel de sistema para poder controlar el sistema de forma remota sin soporte. También intentó instalar la herramienta de gestión remota de confianza ScreenConnect a través de PowerShell.

Ocultándose a simple vista

Agregar y eliminar usuarios de grupos de acceso privilegiado es una actividad legítima de TI. La capacidad de los atacantes para ocultar comportamientos maliciosos entre las tareas y herramientas cotidianas normales es uno de los mayores desafíos que enfrentan los equipos de seguridad hoy en día.

Este enfoque de vivir de la tierra (LOTL) está en aumento, con actores de amenazas aprovechando herramientas y técnicas de software legítimas para evadir la detección. Afortunadamente, la IA está ayudando a los sistemas de seguridad avanzados a detectar anomalías sutiles en actividades aparentemente benignas que pueden investigarse y mitigarse.

Informe de incidente: el ransomware Akira utiliza la herramienta de gestión remota de la víctima en su contra

Los atacantes obtuvieron acceso al controlador de dominio (DC) e instalaron el Datto RMM. Su actividad reflejaba de cerca lo que un agente de copia de seguridad podría hacer legítimamente durante trabajos programados, lo que hizo que todo pareciera una actividad regular de TI.

Una mención sobre las herramientas de acceso remoto y gestión (RMM)

Las herramientas de acceso remoto son un objetivo creciente para los atacantes. Comprometer con éxito una herramienta RMM otorga a los atacantes una cantidad significativa de poder mientras reduce el riesgo de ser detectados, ya que los RMM son ampliamente utilizados por las organizaciones.

Durante los últimos 12 meses, Barracuda Managed XDR mitigó incidentes que involucraban el abuso de, entre otros, SonicWall SSL-VPN (una red privada virtual popular), ScreenConnect, RDP (el Protocolo de Escritorio Remoto), PsExec (una herramienta de línea de comandos para ejecutar programas y comandos en ordenadores remotos), AnyDesk y otras VPN de firewall.

Para reducir el riesgo, los equipos de seguridad necesitan implementar sistemas de detección que busquen específicamente el abuso de RMM. Por ejemplo, Barracuda Managed XDR ha desarrollado una regla de detección que utiliza la telemetría de los endpoints para identificar solicitudes enviadas desde ScreenConnect a dominios de nivel superior (TLDs) sospechosos.

Combinaciones de bandera roja

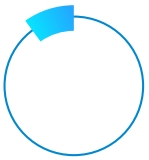
La actividad sospechosa también se puede identificar observando el panorama general. Un análisis de incidentes reales que involucraron Barracuda Managed XDR en los últimos 12 meses identificó las siguientes combinaciones comunes de herramientas/técnicas y comportamientos:

66%

de los casos que involucran malware sin archivos utilizaron PowerShell como el método principal de ejecución. PowerShell es una herramienta independiente de la plataforma utilizada para automatizar tareas y gestionar configuraciones.

44%

de los incidentes relacionados con el firewall involucraron el rociado de contraseñas, donde los atacantes prueban muchas contraseñas comunes contra nombres de usuario robados.



10%

de las violaciones de seguridad del servidor involucraron el borrado de registros de actividad para cubrir las huellas de los atacantes.

96%

de los casos que involucraron movimiento lateral resultaron en la implementación de ransomware.

90%

de los incidentes de ransomware explotaron firewalls a través de un CVE (una vulnerabilidad de software clasificada) o una cuenta vulnerable.

34%

de los incidentes involucraron ingeniería social que engañó a los usuarios para que descargaran archivos potencialmente maliciosos.

Para que los ataques tengan éxito, los atacantes deben encontrar y aprovechar las brechas en la seguridad de sus víctimas. Los datos de detección y la información sobre incidentes de Barracuda Managed XDR ponen de relieve algunos de los posibles puntos débiles que dejaron a los objetivos vulnerables a las ciberamenazas durante el último año.

Cómo las organizaciones quedan expuestas

Principales vulnerabilidades de seguridad de la red

Los métodos de cifrado inadecuados o desactualizados que no protegen el tráfico sensible, así como la falta de validación adecuada — o certificación — de la actividad de la red pueden ser utilizados por los atacantes para llevar a cabo sus ataques.

Barracuda Managed XDR ha identificado los siguientes riesgos de seguridad de la red durante el último año:

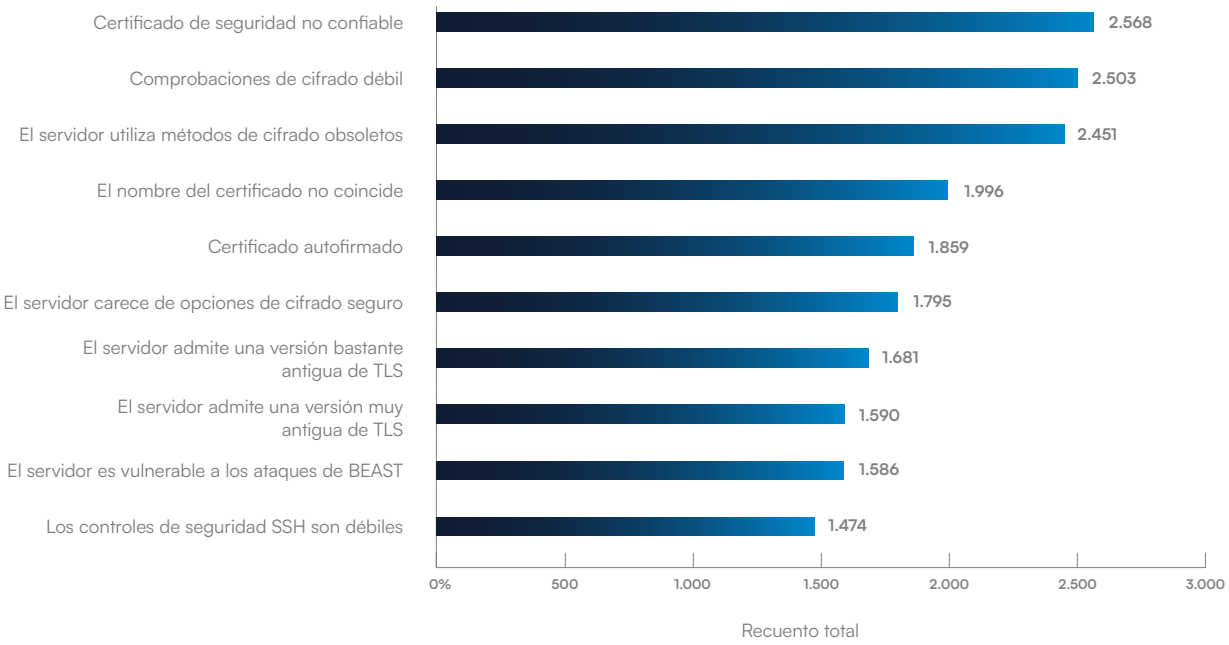


FIGURA 3

Principales vulnerabilidades de seguridad de la red

El certificado de seguridad no es fiable

Lo que esto significa:

El certificado presentado por el servidor no está emitido por una Autoridad de Certificación (CA) de confianza.

Los atacantes pueden usarlo para:

Suplantar un sitio legítimo utilizando un certificado falso, lo que permite a los atacantes introducirse en comunicaciones legítimas para robar datos, eludir la seguridad, inyectar contenido malicioso y mucho más.

Cómo mantenerse seguro:

Utilice certificados de CAs de confianza.

Para equipos más técnicos: Implemente una validación adecuada de certificados y habilite el 'certificate pinning' (donde la aplicación solo confía en un certificado específico al conectarse a un servidor). También es importante verificar si el certificado de una aplicación ha sido revocado (utilizando herramientas como CRL y OCSP) para evitar confiar en certificados comprometidos. Ver: OWASP Certificado Validación.

Los controles de cifrado son débiles

Lo que esto significa:

El servidor utiliza algoritmos débiles o longitudes de clave insuficientes para el cifrado.

Los atacantes pueden usarlo para:

Fuerza bruta o explotar debilidades para descifrar datos sensibles como contraseñas e información financiera. La fuerza bruta implica probar muchas combinaciones diferentes de nombre de usuario/contraseña para ver si alguna funciona.

Cómo mantenerse seguro:

Implemente estándares de cifrado fuertes como AES-256, RSA-2048+.

Para equipos más técnicos: Deshabilite cifrados débiles y audite regularmente las configuraciones. Considere implementar criptografía de curva elíptica (ECC), como ECDSA o ECDHE, para mejorar la seguridad y el rendimiento (Ver: Recomendaciones ECC de NIST). Utilice suites de cifrado Perfect Forward Secrecy (PFS) para proteger sesiones pasadas si las claves son comprometidas.

El servidor utiliza métodos de cifrado obsoletos

Lo que esto significa:

El servidor depende de algoritmos obsoletos como MD5, SHA-1 o RC4.

Los atacantes pueden usarlo para:

Explotar vulnerabilidades conocidas para romper el cifrado o falsificar firmas, lo que lleva a violaciones de datos.

Cómo mantenerse seguro:

Actualícese a algoritmos modernos como SHA-256 o AES y siga las mejores prácticas del sector (por ejemplo, las directrices del NIST mencionadas anteriormente).

Para equipos más técnicos: Elimine el soporte para algoritmos obsoletos (MD5, SHA-1, RC4) de todas las configuraciones. Pruebe con herramientas como SSL Labs para verificar que no se habiliten algoritmos desactualizados. Ver: SSL Labs Test.

El nombre del certificado no coincide

Lo que esto significa:

El nombre de dominio no coincide con el Nombre Común (CN) o el Nombre Alternativo del Sujeto (SAN) del certificado.

Los atacantes pueden usarlo para:

Lanzar ataques de interceptación redirigiendo el tráfico a un servidor malicioso.

Cómo mantenerse seguro:

Asegúrese de que los certificados coincidan con todos los dominios/subdominios en uso.

Para equipos más técnicos: Utilice campos SAN para certificados multidominio. Automatice la gestión de certificados para evitar desajustes durante las renovaciones.

Certificado autofirmado

Qué significa esto:

El certificado está firmado por la misma entidad que lo posee, no por una CA de confianza.

Los atacantes pueden usarlo para:

Facilita la suplantación de servidores, ya que cualquiera puede crear certificados autofirmados.

Cómo mantenerse seguro:

Utilice certificados emitidos por CA para servicios orientados al público y restrinja los certificados autofirmados a sistemas internos.

Para equipos más técnicos: Mantenga una CA privada para uso interno y distribuir su certificado raíz de manera segura. Monitorear certificados autofirmados no autorizados en su red.

El servidor carece de opciones de cifrado fuertes

Lo que esto significa:

El servidor no ofrece suites de cifrado modernas y seguras.

Los atacantes pueden usarlo para:

Forzar una degradación a un cifrado más débil.

Cómo mantenerse seguro:

Configure los servidores para admitir suites de cifrado fuertes, como Transport Layer Security (TLS) 1.2/1.3 con AES-GCM.

Para equipos más técnicos: Deshabilite el soporte para opciones de cifrado TLS débiles o inseguras, como NULL o EXPORT, para que solo se permitan conexiones fuertes, cifradas y autenticadas. Actualice regularmente el software del servidor para admitir los últimos protocolos y suites de cifrado.

El servidor admite versiones anteriores de TLS

Qué significa esto:

La versión de TLS utilizada está desactualizada y es vulnerable a ataques.

Los atacantes pueden usarlo para:

Explotar las debilidades del protocolo para ataques de interceptación o degradación que engañan al sistema para que utilice un protocolo de seguridad más antiguo y débil.

Cómo mantenerse seguro:

Actualice la versión de TLS utilizada.

Para equipos más técnicos: Desactivar TLS 1.0 y Solo admite TLS 1.2 y 1.3. Ver: Mozilla TLS Recommendations.

El servidor admite una versión muy antigua de TLS

Lo que esto significa:

La versión de TLS en uso es obsoleta e insegura.

Los atacantes pueden usarlo para:

Explotar vulnerabilidades conocidas.

Cómo mantenerse seguro:

Actualice la versión de TLS utilizada.

Para equipos más técnicos: Elimine por completo las versiones SSLv2, SSLv3 y las versiones tempranas de TLS. Utilice herramientas automatizadas para escanear el soporte de protocolos heredados.

Servidor vulnerable a ataque BEAST

Qué significa esto:

Los ataques BEAST (Browser Exploit Against SSL/TLS) tienen como objetivo versiones antiguas de TLS que presentan debilidades en su cifrado basado en bloques.

Los atacantes pueden usarlo para:

Descifrar HTTPS (Hypertext Transfer Protocol Secure) — una versión segura del protocolo básico de comunicación web) tráfico y exponer datos confidenciales.

Cómo mantenerse seguro:

Actualice a la última versión de TLS y utilice conjuntos de cifrado seguros.

Para equipos más técnicos: Considere TLS 1.2+ con conjuntos de cifrado AES-GCM o ChaCha20-Poly1305. Deshabilite los cifrados en modo CBC en versiones anteriores de TLS.

Los controles de seguridad SSH son débiles

Lo que esto significa:

La configuración de SSH utiliza algoritmos débiles o protocolos obsoletos. SSH (Secure Shell) es un protocolo de red seguro utilizado para acceder y controlar remotamente computadoras a través de una red no segura, como internet.

Los atacantes pueden usarlo para:

Credenciales de fuerza bruta o explotar claves débiles para obtener acceso no autorizado.

Cómo mantenerse seguro:

Habilite algoritmos de intercambio de claves fuertes, deshabilite protocolos SSH débiles, utilice autenticación basada en claves y despliegue herramientas especializadas de prevención de intrusiones que protejan los servidores de ataques de fuerza bruta, como Fail2Ban o similares.

Para equipos más técnicos: Utilice solo la versión 2 del protocolo SSH. Haga cumplir las longitudes mínimas de clave (por ejemplo, RSA 4096, Ed25519). Desactive la autenticación por contraseña si es posible y utilice la autenticación basada en claves. Restrinja el acceso SSH por IP y use reglas de firewall. Actualice regularmente el software del servidor SSH. Ver: SSH Security Best Practices.

Las principales vulnerabilidades de software CVE detectadas

El software desactualizado y sin parches es un imán para las ciberamenazas. Según Barracuda Managed Vulnerability Security, estas son las principales vulnerabilidades de software identificadas en las redes de los clientes durante el último año:

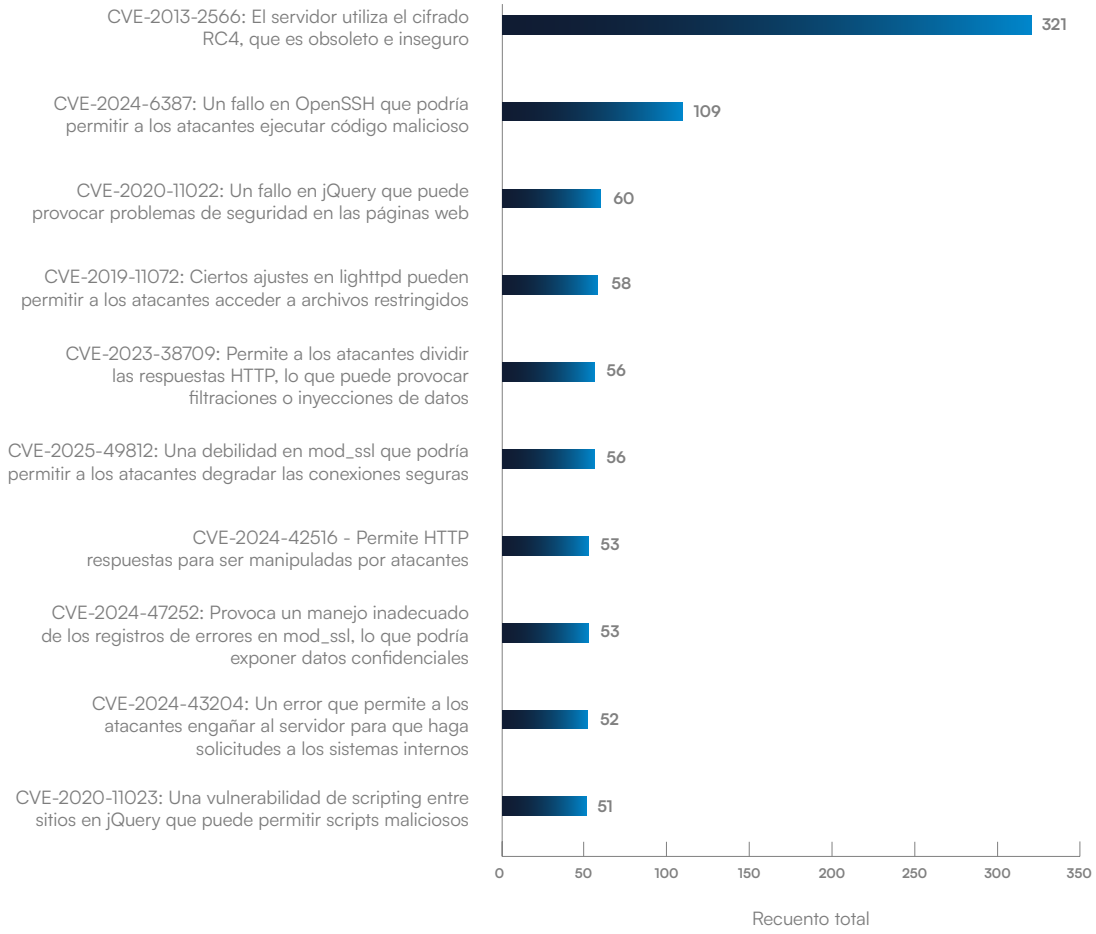


FIGURA 4

Principales vulnerabilidades con un CVE designado encontradas en organizaciones

La vulnerabilidad más detectada también es la más antigua. CVE-2013-2566 ha existido durante casi 13 años y aún se puede encontrar en sistemas heredados como servidores antiguos, dispositivos integrados o aplicaciones.

Estos sistemas pueden estar en uso activo, pero a menudo están inactivos y olvidados. La prevalencia de esta vulnerabilidad es una advertencia clara sobre el riesgo de exposición latente. Cuanto antes se corrija una vulnerabilidad, menos posibilidades hay de que pase desapercibida.

Solo un CVE en la lista tiene una calificación de gravedad crítica, pero cinco están designados como de alta gravedad. La puntuación media de gravedad de todas las vulnerabilidades detectadas en los últimos 12 meses fue de 5,9.

CVE-2013-2566 — El servidor depende de un cifrado RC4 vulnerable y obsoleto

Gravedad: **MEDIA**

Los atacantes pueden usarlo para:

Explotar el cifrado débil para descifrar datos sensibles en texto plano. RC4 es un tipo de cifrado.

Cómo mantenerse seguro:

Deshabilite RC4 en configuraciones de TLS (ver arriba) y utilizar cifrados modernos como AES, TLS 1.2+.

CVE-2024-6387: una vulnerabilidad en OpenSSH que podría permitir a los atacantes ejecutar código malicioso

Gravedad: **CRÍTICA**

Los atacantes pueden usarlo para:

Obtener control total de los sistemas afectados de forma remota. SSH es Secure Shell, un protocolo utilizado para conectarse de forma segura a sistemas remotos a través de una red no segura como internet, y OpenSSH es una versión gratuita y de código abierto.

Cómo mantenerse seguro:

Aplique inmediatamente los últimos parches de OpenSSH y restrinja el acceso SSH.

CVE-2020-11022 — Un error en jQuery que puede provocar problemas de seguridad en las páginas web

Gravedad: **MEDIA**

Los atacantes pueden usarlo para:

Inyectar scripts maliciosos en páginas web y robar sesiones y datos. jQuery es una biblioteca de JavaScript que facilita la codificación para los desarrolladores.

Cómo mantenerse seguro:

Actualice a la última versión de jQuery y limpie los datos antes de que su sistema los utilice.

CVE-2019-11072: Ciertas configuraciones en el servidor web lighttpd pueden permitir que los atacantes accedan a archivos restringidos

Gravedad: **ALTA**

Los atacantes pueden usarlo para:

Acceder a archivos restringidos en el servidor, incluidas configuraciones o datos sensibles. Un servidor lighttpd es un servidor web de código abierto diseñado para entornos donde la velocidad es crítica.

Cómo mantenerse seguro:

Actualice el servidor web lighttpd a la última versión y asegúrese de que cualquier ubicación de archivo proporcionada por los usuarios sea verificada y limpiada para prevenir un uso indebido.

CVE-2023-38709 — Permite a los atacantes dividir las respuestas HTTP en servidores web Apache vulnerables, lo que posiblemente provoque fugas de datos o inyecciones

Gravedad: **ALTA**

Los atacantes pueden usarlo para:

Agregar instrucciones falsas a las respuestas web, engañar a los sistemas para que almacenen datos dañinos o inyectar código malicioso en las páginas web, comprometiendo la integridad de los datos y la seguridad del usuario.

Cómo mantenerse seguro:

Actualice el servidor web Apache y asegúrese de que todas las instrucciones del navegador al servidor o los datos de encabezado se verifiquen y limpien adecuadamente.

CVE-2025-49812 — Una debilidad en mod_ssl que podría permitir a los atacantes degradar las conexiones seguras

Gravedad: **ALTA**

Los atacantes pueden usarlo para:

Reducir el nivel de cifrado o interceptar el tráfico y exponer datos sensibles. mod_ssl es un módulo del servidor HTTP de Apache que añade soporte para el cifrado.

Cómo mantenerse seguro:

Aplique los últimos parches de Apache y aplique configuraciones de cifrado TLS fuertes.

CVE-2024-42516: Una vulnerabilidad de seguridad que permite a los atacantes manipular las respuestas web HTTP enviadas a los usuarios

Gravedad: **ALTA**

Los atacantes pueden usarlo para:

Explotar debilidades en cómo un sistema recibe, verifica y procesa datos para inyectar contenido dañino o redirecciones que pueden llevar a phishing, entrega de malware o sesiones de usuario robadas.

Cómo mantenerse seguro:

Aplique los parches del proveedor de manera oportuna y haga cumplir encabezados de seguridad sólidos.

CVE-2024-47252: Da lugar a un manejo inadecuado de los registros de errores en mod_ssl que podría exponer datos sensibles

Gravedad: **MEDIA**

Los atacantes pueden usarlo para:

Inyectar contenido malicioso en los registros que puede contaminar los registros y potencialmente escalar privilegios.

Cómo mantenerse seguro:

Actualice Apache y restrinja el acceso a los registros.

CVE-2024-43204: Un error que permite a los atacantes engañar al servidor para realizar solicitudes a sistemas internos

Gravedad: **ALTA**

Los atacantes pueden usarlo para:

Forzar a un servidor a realizar solicitudes a sistemas internos, exponiendo la red interna.

Cómo mantenerse seguro:

Parchee Apache y valide configuraciones de encabezados.

CVE-2020-11023 — Una vulnerabilidad de cross-site scripting en jQuery que puede permitir scripts maliciosos

Gravedad: **MEDIA**

Los atacantes pueden usarlo para:

Inyectar scripts maliciosos.

Cómo mantenerse seguro:

Actualice jQuery, limpie las entradas de usuario y utilice herramientas para bloquear código dañino.

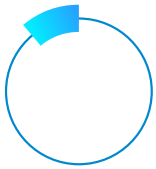
Hallazgos adicionales de Barracuda Managed Vulnerability Security

4.146

Número total de vulnerabilidades críticas detectadas.

2.525

Número total de vulnerabilidades únicas identificadas.



11%

Proporción de vulnerabilidades que tienen un exploit conocido.

Informe de incidente: firewall sin parche utilizado en intento de RansomHub

Los atacantes explotaron vulnerabilidades sin parchear en un firewall de Fortinet. Lanzaron una actividad de fuerza bruta contra la red de un cliente, pero fueron bloqueados. Un mes después, intentaron un inicio de sesión remoto (SSL VPN), pero fueron bloqueados nuevamente. Dos días después, hicieron un tercer intento. Barracuda Managed XDR detectó actividad de PsExec (comando remoto) y encontró software malicioso en el controlador de dominio principal y el servidor de copia de seguridad.

Configuración incorrecta: Incidentes que involucran herramientas de seguridad desactivadas accidental o intencionalmente

Las herramientas de seguridad que no se han configurado correctamente representan un gran riesgo de seguridad. El peligro puede aumentar por la falsa sensación de seguridad que se genera al tener la herramienta instalada en primer lugar. En los últimos 12 meses, Barracuda Managed XDR identificó funciones deshabilitadas que incluían agentes de protección de endpoints (que representan el 94% de las detecciones de seguridad deshabilitadas), MFA (3.62%), enlaces seguros (1.4%) y reglas de adjuntos seguros (0.6%).

Los estudios muestran que la mayoría de las organizaciones están intentando gestionar demasiadas herramientas de seguridad. Cuando los recursos están al límite, los errores de configuración pueden aparecer fácilmente. La mejor protección es una plataforma de seguridad integrada con visibilidad completa sobre configuraciones y ajustes que pueda identificar rápidamente y de forma automática las brechas que necesitan ser corregidas.

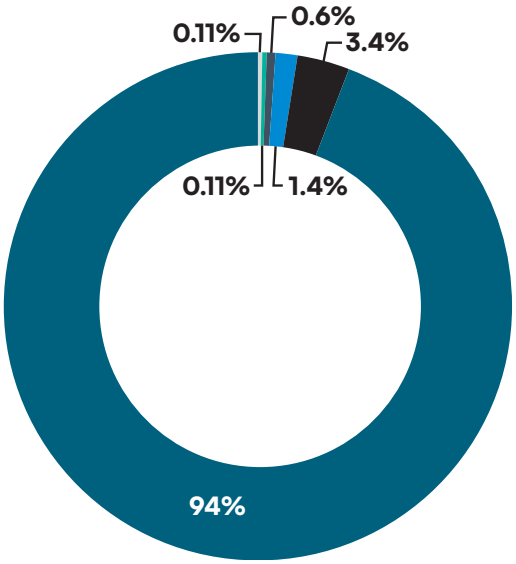


FIGURA 5

Funciones de seguridad deshabilitadas con mayor frecuencia

- Agente de Endpoint de SentinelOne deshabilitado
- Microsoft 365 MFA deshabilitado
- Regla de 'enlaces seguros' de Microsoft 365 ATP deshabilitad
- Regla de 'adjunto seguro' de Microsoft Office ATP deshabilitada
- Microsoft Azure MFA deshabilitado
- MFA de Google Workspace deshabilitada

100%

Proporción de incidentes a los que respondió Barracuda Managed XDR que involucraron al menos un endpoint no protegido o deshonesto

66%

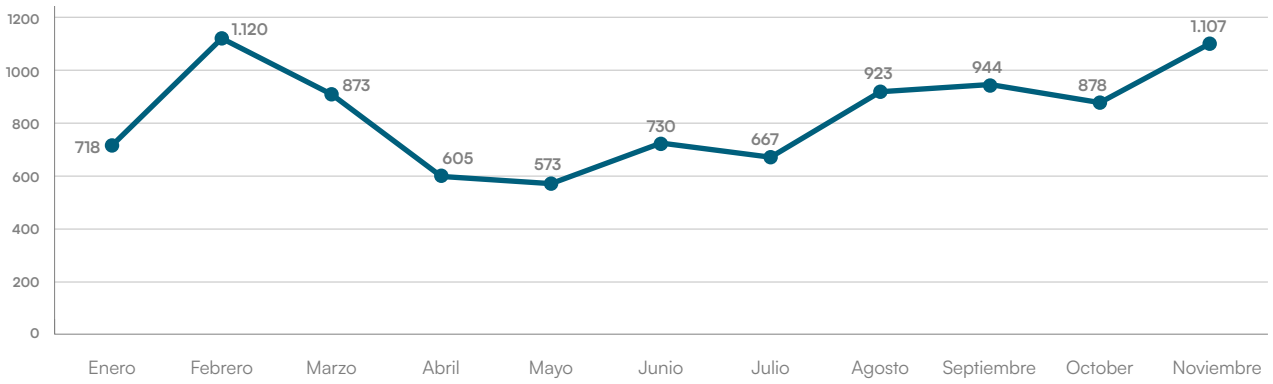
Proporción de incidentes a los que respondió Barracuda Managed XDR que involucraron la cadena de suministro o un tercero (frente al 45% en 2024)

La amenaza persistente del ransomware

Durante los últimos 12 meses, Barracuda Managed XDR identificó 13.514 indicadores de que un ataque de ransomware estaba en curso, incluidos herramientas, técnicas y comportamientos. A diferencia de años anteriores, ya no hay picos o valles pronunciados, sino un nivel alto constante de incidentes durante todo el año.

FIGURA 6

Incidentes relacionados con ransomware en 2025



1.5% a 5.6%

Proporción de todas las organizaciones afectadas por ransomware cada mes en 2024

5.1% a 10.9%

Proporción de todas las organizaciones afectadas por ransomware cada mes en 2025

Principales familias de ransomware encontradas en 2025

Akira

- Akira es un grupo de ransomware relativamente nuevo conocido por atacar a organizaciones con ataques sofisticados. A menudo emplea tácticas de doble extorsión, cifrando datos y amenazando con liberar información sensible a menos que se pague un rescate.
- **Tácticas**: Uso de malware avanzado, ataques dirigidos y robo de datos.

Qilin

- Qilin es un grupo de ransomware que ha ganado atención por sus ataques dirigidos a infraestructuras críticas y organizaciones empresariales.
- **Tácticas**: Doble extorsión, explotación de vulnerabilidades y aprovechamiento de malware para cifrar datos.

RansomHub

- RansomHub es una operación de ransomware que funciona como ransomware-as-a-service (RaaS), permitiendo a los afiliados desplegar ransomware bajo su propia marca.
- **Tácticas**: Modelo de Ransomware como Servicio (RaaS), robo de datos y extorsión.

Cactus

- Cactus es un grupo de ransomware que ha estado involucrado en ataques dirigidos, a menudo exigiendo elevados rescates.
- **Tácticas**: Cifrado de datos, doble extorsión y explotación de vulnerabilidades.

Informe de Incidente — Múltiples brechas de seguridad exponen el objetivo a Cactus

Las víctimas fueron engañadas para descargar archivos maliciosos a través de llamadas de Teams. Los atacantes configuraron canales para emitir comandos de forma remota, moverse lateralmente y mantener la persistencia. Tareas programadas maliciosas, ediciones del registro y carga lateral de DLL (cuando un programa es engañado para cargar un archivo de código compartido falso y dañino, de modo que el código del atacante se ejecuta en lugar del real) ayudaron a los atacantes a escalar privilegios y evadir la detección. El equipo de Barracuda Managed XDR encontró dispositivos fraudulentos y más de 1.600 dispositivos desprotegidos en la red, permisos laxos de Microsoft Teams, implementaciones vulnerables de protocolo de escritorio remoto (RDP) y shell seguro, archivos no firmados y falta de concienciación de los empleados.

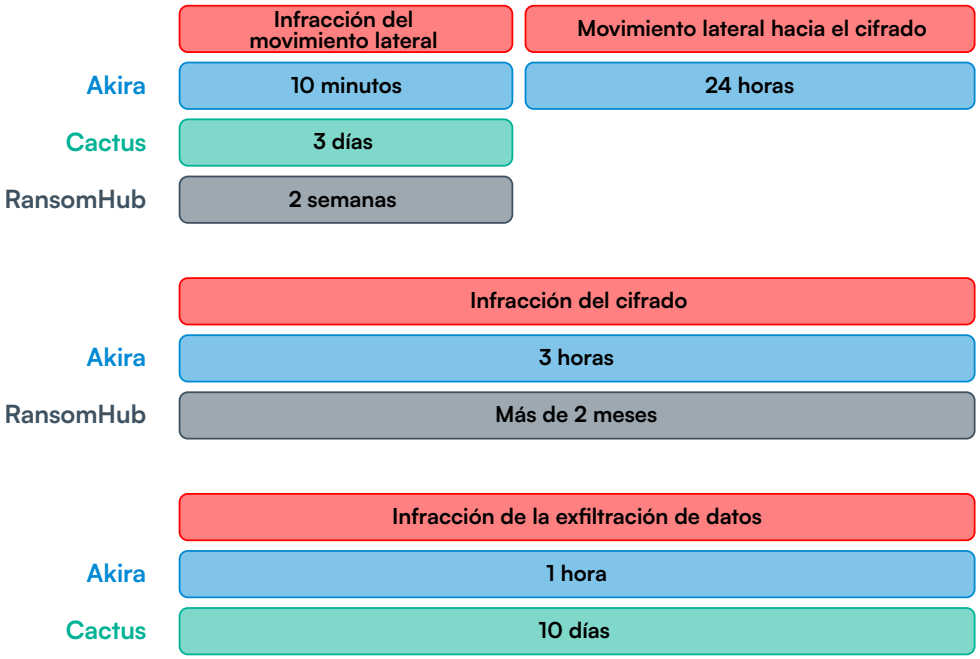
El ransomware se mueve a diferentes velocidades

Según los datos de detección e incidentes de Barracuda Managed XDR, los ataques de ransomware más rápidos en 2025 tardaron solo horas de principio a fin, mientras que los más largos tardaron meses.

Las intrusiones prolongadas permiten un daño máximo, ya que los atacantes tienen tiempo para el reconocimiento, la exfiltración de datos, el sabotaje y más. Los incidentes que se desarrollan a la velocidad del rayo pueden ser más difíciles de detectar y contener antes de que se ejecuten y el daño esté hecho.

Las organizaciones deben estar preparadas para ambos tipos de ataques y contar con herramientas de seguridad que estén siempre alerta.

La velocidad del ransomware — 3 actores



Tiempos estimados a partir de incidentes del mundo real

Informe de incidente: XDR detecta ransomware Akira explotando cuenta 'fantasma' y servidor desprotegido

Los atacantes violaron la red a través de una cuenta que fue creada para un proveedor externo y no se desactivó cuando se fueron. Los atacantes intentaron moverse lateralmente y desactivar la seguridad del endpoint, pero fueron bloqueados. Se trasladaron a un servidor desprotegido, escalaron sus privilegios y lanzaron el ransomware. Todos los dispositivos afectados fueron neutralizados. Otros riesgos encontrados en la red objetivo incluían dispositivos desprotegidos, un canal VPN abierto en su firewall y MFA inconsistente.

Conclusión: Cómo mantenerse seguro en un mundo de amenazas complejas

Los equipos de seguridad enfrentan desafíos cada vez mayores. Con recursos limitados, deben proteger un panorama en constante expansión de dispositivos, aplicaciones, vulnerabilidades críticas y herramientas de seguridad fragmentadas, a menudo sin la visibilidad unificada necesaria para adelantarse a las amenazas.

Todo está a punto de volverse aún más difícil a medida que los atacantes comienzan a aprovechar la IA agéntica.

Los sistemas de IA agéntica automatizarán las etapas iniciales y repetitivas de un ataque, escanearán entornos sin parar, identificarán configuraciones débiles y lanzarán exploits dirigidos en minutos. Los actores de amenazas que aprovechen los agentes de IA podrán tomar decisiones, ajustar estrategias y corregir o reescribir código malicioso cuando algo falle o encuentren un obstáculo. Este cambio aumentará drásticamente la velocidad, escala y consistencia de los ataques.

Las organizaciones necesitan una estrategia de seguridad unificada que integre tecnologías de detección avanzadas impulsadas por IA con un SOC completamente autónomo, complementado por la educación de los usuarios, la respuesta automatizada a amenazas y una cultura de seguridad resiliente.

Existen victorias rápidas, como las descritas a lo largo de este informe. Estas incluyen autenticación multifactorial y controles de acceso consistentes, un enfoque robusto para la gestión de parches y la protección de datos, y formación regular en concienciación sobre la ciberseguridad para los empleados.

Esto debe estar respaldado por una plataforma de seguridad gestionada integral y una solución XDR gestionada 24 horas al día, 7 días a la semana que integre la seguridad de la red, el endpoint, el servidor, la nube y el correo electrónico, proporcionando una visibilidad completa de extremo a extremo y control de gestión respaldado por un SOC completamente autónomo.

La seguridad a largo plazo reside en la ciberresiliencia. La detección y la prevención son los pilares de cualquier estrategia de seguridad, pero ante amenazas cada vez más complejas y evasivas, poder responder y recuperarse de los ataques de manera rápida y con un impacto mínimo es clave.

Las conclusiones detalladas en este informe están basadas en datos de detección de Barracuda Managed XDR, una plataforma de visibilidad, detección y respuesta ampliadas (XDR), respaldada por un centro de operaciones de seguridad (SOC) que proporciona a los clientes servicios ininterrumpidos de detección de amenazas, análisis, respuesta a incidentes y mitigación, tanto humanos como basados en inteligencia artificial.

Barracuda Managed XDR es parte de BarracudaONE, una plataforma basada en IA que protege el correo electrónico, los datos, las aplicaciones y las redes con soluciones innovadoras y un panel de control centralizado para maximizar la protección y reforzar la resiliencia cibernética.

Sobre Barracuda

Barracuda es una empresa líder mundial en ciberseguridad que ofrece protección completa frente a amenazas complejas para empresas de todos los tamaños. Nuestra plataforma BarracudaONE, impulsada por IA, protege el correo electrónico, los datos, las aplicaciones y las redes con soluciones innovadoras, XDR gestionado y un panel centralizado para maximizar la protección y reforzar la resiliencia cibernética. Con la confianza de cientos de miles de profesionales de TI y proveedores de servicios gestionados de todo el mundo, Barracuda ofrece defensas potentes que son fáciles de comprar, implementar y usar.