Crecen en 2026 los ataques automatizados, el ransomware ultrarrápido y el phishing a empresas

Estrategias de Inversión
19/04/2026

Entre enero y marzo, más de la mitad de los incidentes detectados por Barracuda Managed XDR correspondieron a intentos de acceso por **fuerza bruta dirigidos a dispositivos de red, especialmente firewalls y sistemas perimetrales.**

Según datos de Barracuda Networks, el 56% de los incidentes confirmados entre febrero y marzo estuvieron relacionados con este tipo de ataques.

Lo que en realidad llevan a cabo es probar miles de combinaciones de credenciales de forma automatizada hasta encontrar accesos válidos. **Aunque muchos intentos fracasan, la repetición constante aumenta las probabilidades de éxito**, especialmente en entornos con contraseñas débiles o configuraciones deficientes.

Dispositivos perimetrales, el objetivo prioritario

Los atacantes están centrando sus esfuerzos en equipos clave como los sistemas SonicWall y FortiGate, que actúan como primera línea de defensa en muchas organizaciones.

Estos dispositivos, al estar expuestos a Internet, se convierten en puntos críticos si no están correctamente protegidos.

La estrategia es sencilla: **escanear redes en busca de accesos abiertos, cuentas antiguas o credenciales reutilizadas.**

Incluso cuando los intentos no logran entrar, generan ruido y presión constante sobre los sistemas, aumentando el riesgo de que un fallo puntual derive en una brecha de seguridad.

Entre los factores más comunes que facilitan estos ataques se encuentran el uso de contraseñas poco robustas, la ausencia de autenticación multifactor y la falta de monitorización de accesos. También **influyen las cuentas inactivas que siguen habilitadas, un vector de riesgo habitual en muchas organizaciones.**

El ransomware acelera su capacidad de impacto

A este escenario se suma la evolución del ransomware, que en 2026 ha dado un salto significativo en velocidad y eficacia.

ASOCIACIÓN ESPAÑOLA DE CONTRIBUYENTES

Una de las amenazas más destacadas es **Qilin, un grupo que ha perfeccionado sus técnicas hasta poder ejecutar ataques completos en cuestión de minutos tras la infección inicial.**

Este tipo de ransomware ya no necesita largos periodos de permanencia en el sistema. Una vez dentro, puede cifrar archivos críticos y **paralizar operaciones en muy poco tiempo**, reduciendo el margen de reacción de las víctimas.

El impacto potencial es elevado, especialmente en entornos con baja visibilidad de red o sin sistemas de detección temprana. **La falta de copias de seguridad actualizadas o de planes de contingencia** empresariales, puede agravar las consecuencias, obligando a las empresas a detener su actividad durante días.

Ojo con el auge del método ClickFix

Otra tendencia al alza es el uso de técnicas de ingeniería social más elaboradas. Entre ellas destaca el método conocido como ClickFix, que consiste en **engañar al usuario para que ejecute por sí mismo acciones que desencadenan el ataque.**

A diferencia del phishing tradicional, donde el objetivo es robar credenciales, en este caso se induce a la víctima a copiar comandos, descargar archivos o realizar acciones aparentemente legítimas que **activan código malicioso**.

Este enfoque **dificulta la detección por parte de soluciones de seguridad convencionales**, ya que el comportamiento del usuario parece normal. Además, aprovecha el contexto y la urgencia para aumentar la probabilidad de éxito.

Estos ataques son cada vez más personalizados, utilizando información real de la víctima para ganar credibilidad. Esto refuerza la necesidad de formación continua en ciberseguridad dentro de las organizaciones.

ASOCIACIÓN ESPAÑOLA DE CONTRIBUYENTES

Medidas básicas que siguen marcando la diferencia

A pesar del aumento de la sofisticación, muchas brechas de seguridad siguen produciéndose por errores básicos.

La implementación de contraseñas únicas y complejas, el uso de autenticación multifactor y la limitación de accesos son medidas que continúan siendo esenciales.

También resulta clave supervisar los intentos de acceso fallidos y restringir la exposición de sistemas críticos a redes públicas. Estas prácticas, aunque sencillas, pueden reducir de forma significativa el riesgo de intrusión.

El Instituto Nacional de Ciberseguridad, por su lado, **insiste en que la prevención sigue siendo el pilar fundamental frente a estas amenazas.**

Detectar comportamientos anómalos a tiempo y contar con protocolos de respuesta rápida puede evitar que un incidente puntual se convierta en un problema mayor.

ASOCIACIÓN ESPAÑOLA
DE CONTRIBUYENTES