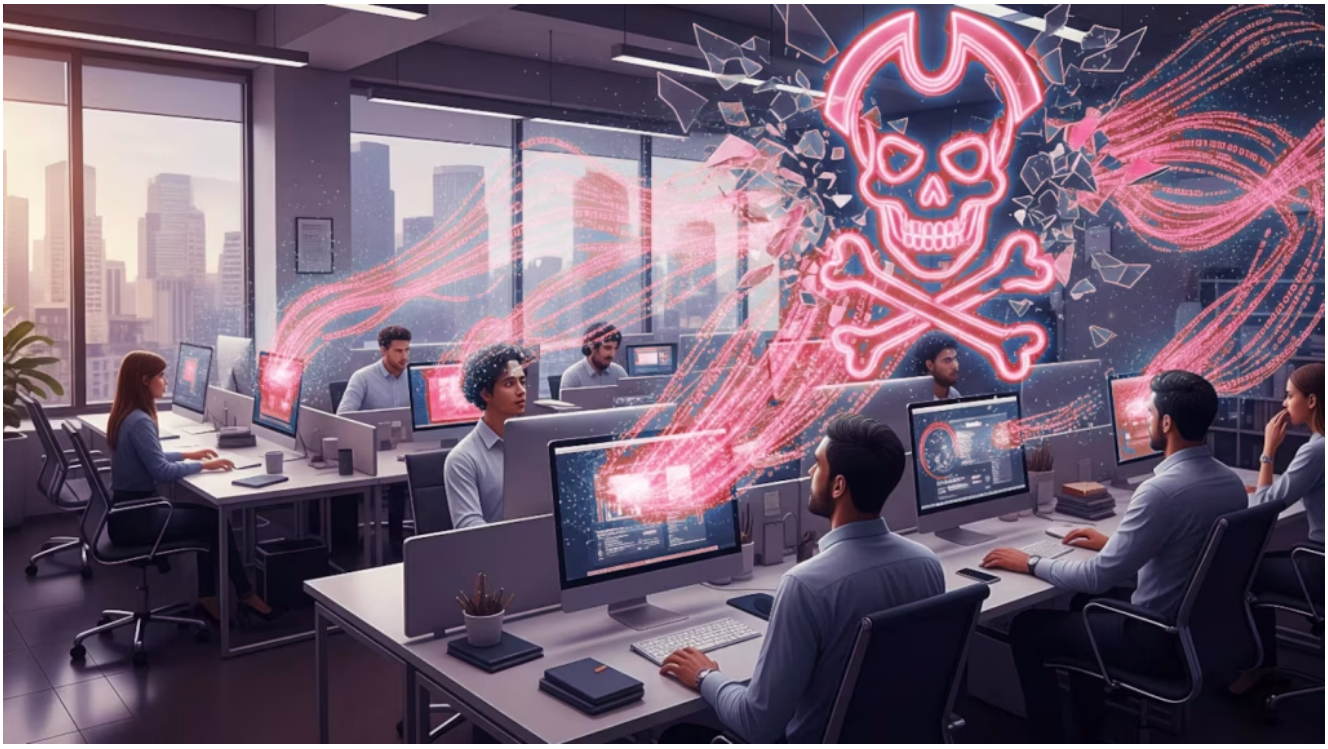
Ni hackeos ni malware: las claves robadas fueron el principal riesgo de ciberseguridad en 2025

10/11/2025



Durante la primera mitad de 2025, el principal enemigo de la ciberseguridad no fueron los hackers más creativos ni el malware más destructivo, sino el robo de contraseñas.

Según un nuevo estudio, la mayoría de los incidentes de seguridad informática no comenzaron con hackeos, sino con accesos e inicios de sesión con credenciales legítimas.

El *Informe Global de Amenazas 2025*, elaborado por el equipo FortiGuard Incident Response de Fortinet, reveló que los ciberdelincuentes dejaron de lado los ataques sofisticados con malware complejos y ahora prefieren **infiltrarse en sistemas a través del uso de claves reales**, nombres de usuario y contraseñas legítimas, robadas, reutilizadas o **compradas en**

la *dark web* o grupos y foros clandestinos.

Los ataques más efectivos del año no usaron inteligencia artificial ni software complejo: bastó con usuarios distraídos, contraseñas débiles y cuentas sin verificación multifactor. (Imagen generada con GeminiAI).

Así, en lugar de desplegar virus o herramientas de última generación, los atacantes logran **entrar como un empleado** más a sistemas corporativos **a través de servicios comunes**, como conexiones VPN o software de asistencia remota, y pueden moverse dentro de las redes **sin activar alarmas** y pasan inadvertidos entre la actividad habitual de la empresa.

Los analistas de Fortinet detectaron que los accesos son también obtenidos **mediante simples campañas de *phishing*** en la mayoría de los casos.

Una vez dentro, los delincuentes utilizan herramientas ya instaladas en la empresa o agregan versiones propias de software remoto para mantener **el control del sistema, copiar información** y, en algunos casos, **desplegar *ransomware*.**

El informe citó el caso de una organización que vio cómo sus servidores quedaban encriptados después de una conexión remota

hecha con una cuenta legítima de **VPN** que no tenía verificación multifactor. En otro, un grupo de atacantes instaló software de control remoto en decenas de equipos gracias a una cuenta de administrador robada, y permaneció dentro de la red durante días sin ser detectado.

Fortinet también reportó casos en los que los delincuentes aprovecharon **vulnerabilidades públicas ya conocidas**, instalando herramientas de acceso remoto y moviéndose manualmente entre servidores hasta identificar los archivos más valiosos para su extorsión.

Por qué estos ataques funcionan tan bien

El éxito de esta metodología se debe a varios factores:

- **Discreción total:** la actividad del atacante se confunde con la de un usuario real.
- **Rapidez:** con una clave válida, el acceso a la información sensible es inmediato.
- **Facilidad de ejecución:** no requiere conocimientos técnicos avanzados ni herramientas complejas.

"Estas operaciones son silenciosas, baratas y difíciles de detectar: los movimientos parecen legítimos y los sistemas basados en **malware** no registran anomalías. En foros clandestinos, las credenciales corporativas se venden desde 500 dólares", explicó Juan Brodersen, periodista especializado en ciberseguridad, en su newsletter *DarkNews*.

El informe además reveló que los accesos y contraseñas de corporaciones grandes pueden alcanzar **valores de hasta 20.000 dólares** en el mercado negro.

La empresa de ciberseguridad advierte en su reporte que las organizaciones deberían **dejar de enfocar todos sus recursos en**

amenazas mediáticas, como los ataques potenciados por **inteligencia artificial**, y **no descuidar los riesgos cotidianos** derivados del **mal uso de contraseñas y cuentas compartidas.**

Entre las principales recomendaciones, además de educar y concientizar a los empleados, se sugiere:

- Implementar **autenticación multifactor (MFA)** para todos los accesos, internos y externos.
- **Monitorear y restringir** el uso de software remoto no autorizado.
- Crear **alertas de comportamiento inusual**, como inicios de sesión desde ubicaciones imposibles o fuera del horario laboral.
- Aplicar el principio de **mínimo privilegio**, evitando que las cuentas con permisos elevados usen VPN.
- Analizar patrones de uso de los empleados para detectar movimientos anómalos entre sistemas.

Fuente: Canal 26