¿Qué es un infostealer y por qué el robo de tokens de sesión es tan peligroso?

Respuesta breve: Un infostealer es un malware diseñado para capturar material de identidad digital —contraseñas, tokens de sesión, claves de API y credenciales VPN— y exfiltrarlo rápidamente. Un token de sesión robado es peligroso porque a menudo evita por completo las contraseñas y la autenticación multifactor, permitiendo que un atacante inicie sesión como un usuario legítimo.

Por qué los atacantes ahora roban la identidad en lugar de permanecer residentes

Los atacantes modernos evitan cada vez más quedarse dentro de una red. Permanecer en el entorno aumenta las probabilidades de detección. En su lugar, toman el material de identidad y se marchan, lo que les otorga dos ventajas:

1. **Menor riesgo** — analizan lo que robaron desde un entorno seguro a su propio ritmo.
2. **Regreso sencillo** — con un token de sesión, contraseña o clave VPN válidos, pueden volver cuando quieran, apareciendo como completamente legítimos ante el sistema de autenticación.

Por qué la velocidad es todo el problema

Estas herramientas pasan de la infiltración a la autoeliminación en segundos —más rápido de lo que tarda una alerta en la nube en salir del edificio. Cyber Crucible interpreta la intención en el momento del acceso a los datos de identidad y suspende el proceso en menos de 200 milisegundos, antes de que comience la exfiltración.

Revision #1
Created 2026-07-24 01:41:58 UTC by Dennis Underwood
Updated 2026-07-24 01:41:58 UTC by Dennis Underwood