

¿Qué son las cookies del navegador y cómo las explotan los atacantes?

Respuesta breve: Las cookies son pequeños fragmentos de datos que un sitio web almacena en su navegador, y algunas de ellas son cookies de autenticación que mantienen su sesión iniciada. Robar esas es funcionalmente equivalente a robar una sesión activa: el atacante puede cargarlas en su propio navegador y aparentar ser usted.

No todas las cookies importan por igual

- **Cookies de preferencias** — idioma, tema, diseño. Valor bajo.
- **Cookies de análisis** — medición de uso. Valor bajo.
- **Cookies de autenticación / sesión** — demuestran que ha iniciado sesión. **Valor alto.**

Los atacantes se interesan casi exclusivamente en la tercera categoría.

Por qué el robo de cookies es efectivo

Una cookie de autenticación robada normalmente no desencadena un evento de inicio de sesión, una solicitud de contraseña ni un desafío de MFA. La sesión ya existe; el atacante simplemente presenta una prueba de ella. Desde la perspectiva de la aplicación, esto parece actividad continua ordinaria.

Los navegadores almacenan las cookies en ubicaciones de archivo conocidas y predecibles en todos los sistemas operativos, por lo que las herramientas automatizadas pueden localizarlas sin saber nada específico sobre la máquina en cuestión.

Por qué el navegador es un punto focal

El navegador aloja cookies, contraseñas guardadas, tokens OAuth e historial en un solo lugar, lo que lo convierte en el objetivo de identidad más rico de la mayoría de los endpoints. Cyber Crucible ha observado esto directamente: desde el cuarto trimestre de 2023 en adelante, las respuestas automatizadas contra actividad de Chrome, Edge y Chromium aumentaron de cero a miles, con

CVE relacionados publicados posteriormente por Google y Microsoft.

Protección

El almacenamiento de credenciales del navegador es una de las ubicaciones de identidad protegidas. Un proceso que intenta leerlo se evalúa en contexto: un navegador explotado se trata de forma muy distinta a uno sano, y en ninguno de los dos casos una solicitud excesiva recibe la cookie real.

Revision #1

Created 2026-07-24 01:44:03 UTC by Dennis Underwood

Updated 2026-07-24 01:44:03 UTC by Dennis Underwood