

¿Qué es un token de sesión y por qué robarlo es peor que robar una contraseña?

Respuesta breve: Un token de sesión es la credencial que tu navegador o aplicación conserva *después* de iniciar sesión, y que demuestra que ya estás autenticado. Robar uno suele ser peor que robar una contraseña porque normalmente evita tanto la contraseña como la autenticación multifactor: el atacante simplemente retoma tu sesión existente.

Por qué existe

Volver a introducir la contraseña en cada solicitud sería inviable, por lo que, tras un inicio de sesión exitoso, el servicio emite un token. Cada solicitud posterior lleva ese token en lugar de tus credenciales. El servicio confía en él como prueba de que ya te autenticaste.

Por qué los atacantes lo prefieren

- **Evita la MFA.** La MFA se verifica en el inicio de sesión. Un token emitido *después* de esa verificación representa una autenticación ya superada, por lo que reutilizarlo normalmente no vuelve a activar el segundo factor.
- **Parece legítimo.** Para el servicio, un token válido equivale a un usuario válido. No hay señal de inicio de sesión fallido ni nada anómalo que genere una alerta.
- **Es portátil.** Muchos tokens funcionan desde una máquina, una red o un país distintos.

Por qué esto cambió el comportamiento de los atacantes

Los atacantes evitan cada vez más permanecer en una red. Quedarse residente aumenta las probabilidades de detección. En cambio, se llevan el material de identidad y se marchan, para luego regresar cuando quieran como un usuario autenticado. El token es una puerta trasera de apariencia legítima que el propio sistema de autenticación emitió.

Cómo lo aborda Cyber Crucible

El robo de tokens se detiene en el momento del acceso. Cuando un programa intenta acceder al almacenamiento del navegador o de la aplicación donde residen los tokens, su acceso se evalúa en menos de 200 milisegundos. A un programa legítimo pero que se extralimita se le entregan datos falsos o se le deniega el acceso; uno desconocido o comprometido es rechazado o suspendido. En cualquier caso, el token real nunca se entrega.

Revision #1

Created 2026-07-24 01:43:43 UTC by Dennis Underwood

Updated 2026-07-24 01:43:43 UTC by Dennis Underwood