

O que é um token de sessão e por que roubar um é pior do que roubar uma senha?

Resposta curta: Um token de sessão é a credencial que o seu navegador ou aplicação mantém *depois* de você iniciar sessão, comprovando que já está autenticado. Roubar um é frequentemente pior do que roubar uma senha porque isso normalmente contorna tanto a senha quanto a autenticação multifator — o atacante simplesmente retoma a sua sessão existente.

Por que existe

Reintroduzir a senha em cada pedido seria impraticável, por isso, após um início de sessão bem-sucedido, o serviço emite um token. Cada pedido posterior transporta esse token em vez das suas credenciais. O serviço confia nele como prova de que já se autenticou.

Por que os atacantes o preferem

- **Contorna a MFA.** A MFA é verificada no início de sessão. Um token emitido *depois* dessa verificação representa uma autenticação já concluída, pelo que reutilizá-lo normalmente não volta a acionar o segundo fator.
- **Parece legítimo.** Para o serviço, um token válido corresponde a um utilizador válido. Não há sinal de falha de início de sessão nem nada de anómalo para gerar um alerta.
- **É portátil.** Muitos tokens funcionam a partir de uma máquina, rede ou país diferente.

Por que isto mudou o comportamento dos atacantes

Os atacantes evitam cada vez mais permanecer numa rede. Permanecer residente aumenta a probabilidade de deteção. Em vez disso, recolhem material de identidade e saem — regressando depois à vontade como um utilizador autenticado. O token é uma porta dos fundos de aparência legítima que o próprio sistema de autenticação emitiu.

Como a Cyber Crucible resolve isto

O roubo de tokens é interrompido no momento do acesso. Quando um programa tenta aceder ao armazenamento do navegador ou da aplicação onde os tokens residem, o seu acesso é avaliado em menos de 200 milissegundos. Um programa legítimo mas com acesso excessivo recebe dados falsos ou é recusado; um programa desconhecido ou comprometido é rejeitado ou suspenso. Em qualquer dos casos, o token real nunca é entregue.

Revision #1

Created 2026-07-24 05:41:48 UTC by Dennis Underwood

Updated 2026-07-24 05:41:48 UTC by Dennis Underwood