

Qu'est-ce qu'un jeton de session, et pourquoi le vol de celui-ci est-il pire que le vol d'un mot de passe ?

Réponse courte : Un jeton de session est l'identifiant que votre navigateur ou votre application conserve *après* votre connexion, prouvant que vous êtes déjà authentifié. Voler un tel jeton est souvent pire que voler un mot de passe, car cela contourne généralement à la fois le mot de passe et l'authentification multifacteur — l'attaquant reprend simplement votre session existante.

Pourquoi cela existe

Ressaisir un mot de passe à chaque requête serait inutilisable ; c'est pourquoi, après une connexion réussie, le service émet un jeton. Chaque requête ultérieure transporte ce jeton au lieu de vos identifiants. Le service lui fait confiance comme preuve que vous vous êtes déjà authentifié.

Pourquoi les attaquants le préfèrent

- **Cela contourne l'authentification multifacteur (MFA).** La MFA est vérifiée lors de la connexion. Un jeton émis *après* cette vérification représente une authentification déjà validée, de sorte que le rejouer ne déclenche généralement pas à nouveau le deuxième facteur.
- **Cela paraît légitime.** Pour le service, un jeton valide équivaut à un utilisateur valide. Il n'y a aucun signal d'échec de connexion et rien d'anormal à signaler.
- **C'est portable.** De nombreux jetons fonctionnent depuis une machine, un réseau ou un pays différent.

Pourquoi cela a changé le comportement des attaquants

Les attaquants évitent de plus en plus de s'attarder dans un réseau. Rester présent augmente les risques de détection. Ils préfèrent au contraire s'emparer des éléments d'identité et repartir — puis revenir à volonté en tant qu'utilisateur authentifié. Le jeton est une porte dérobée à l'apparence légitime, émise par le système d'authentification lui-même.

Comment Cyber Crucible y remédie

Le vol de jeton est stoppé au moment même de l'accès. Lorsqu'un programme tente d'accéder au stockage du navigateur ou de l'application où résident les jetons, son accès est évalué en moins de 200 millisecondes. Un programme légitime mais excessif se voit fournir de fausses données ou se voit refuser l'accès ; un programme inconnu ou compromis est rejeté ou suspendu. Dans tous les cas, le jeton réel n'est jamais transmis.

Revision #1

Created 2026-07-24 06:52:03 UTC by Dennis Underwood

Updated 2026-07-24 06:52:03 UTC by Dennis Underwood