Que sont les cookies de navigateur, et comment les attaquants en abusent-ils ?

Réponse courte : Les cookies sont de petites données qu'un site web stocke dans votre navigateur, et certains d'entre eux sont des cookies d'authentification qui vous maintiennent connecté. Les voler équivaut fonctionnellement à voler une session active — l'attaquant peut les charger dans son propre navigateur et paraître être vous.

Tous les cookies n'ont pas la même importance

- **Cookies de préférence** — langue, thème, mise en page. Faible valeur.
- **Cookies d'analyse** — mesure d'utilisation. Faible valeur.
- **Cookies d'authentification / de session** — prouvent que vous êtes connecté. **Valeur élevée.**

Les attaquants s'intéressent presque exclusivement à cette troisième catégorie.

Pourquoi le vol de cookies est efficace

Un cookie d'authentification volé ne déclenche généralement ni un événement de connexion, ni une invite de mot de passe, ni un défi MFA. La session existe déjà ; l'attaquant ne fait que présenter la preuve de celle-ci. Du point de vue de l'application, cela ressemble à une activité normale et continue.

Les navigateurs stockent les cookies dans des emplacements de fichiers connus et prévisibles sur chaque système d'exploitation, ce qui permet aux outils automatisés de les localiser sans avoir besoin de connaître quoi que ce soit de spécifique sur la machine.

Pourquoi le navigateur est un point central

Le navigateur regroupe en un seul endroit les cookies, les mots de passe enregistrés, les jetons OAuth et l'historique, ce qui en fait la cible d'identité la plus riche sur la plupart des postes de travail. Cyber Crucible l'a constaté directement : à partir du quatrième trimestre 2023, les réponses automatisées contre l'activité de Chrome, Edge et Chromium sont passées de zéro à plusieurs milliers, avec des CVE associés publiés ultérieurement par Google et Microsoft.

Protection

Le stockage des identifiants du navigateur est l'un des emplacements d'identité protégés. Un processus tentant d'y accéder en lecture est évalué en contexte — un navigateur exploité est traité très différemment d'un navigateur sain, et dans aucun des deux cas une requête excessive ne reçoit le véritable cookie.

Revision #1
Created 2026-07-24 06:52:24 UTC by Dennis Underwood
Updated 2026-07-24 06:52:24 UTC by Dennis Underwood