Qu'est-ce qu'un infostealer, et pourquoi le vol de jetons de session est-il si dangereux ?

Réponse courte : Un infostealer est un logiciel malveillant conçu pour dérober des éléments d'identité numérique — mots de passe, jetons de session, clés API et identifiants VPN — et les exfiltrer rapidement. Un jeton de session volé est dangereux car il permet souvent de contourner entièrement les mots de passe et l'authentification multifacteur, laissant un attaquant se connecter en tant qu'utilisateur légitime.

Pourquoi les attaquants volent désormais l'identité au lieu de rester présents

Les attaquants modernes évitent de plus en plus de s'attarder au sein d'un réseau. Rester dans l'environnement augmente les probabilités de détection. Ils préfèrent plutôt s'emparer des éléments d'identité et repartir, ce qui leur procure deux avantages :

1. **Risque réduit** — ils analysent ce qu'ils ont volé depuis un environnement sûr, à leur propre rythme.
2. **Retour facile** — avec un jeton de session, un mot de passe ou une clé VPN valides, ils peuvent revenir quand ils le souhaitent, en apparaissant totalement légitimes aux yeux du système d'authentification.

Pourquoi la rapidité est tout le problème

Ces outils passent de l'infiltration à l'autodestruction en quelques secondes — plus vite qu'une alerte cloud ne peut quitter les locaux. Cyber Crucible détecte l'intention au moment même de l'accès aux données d'identité et suspend le processus en moins de 200 millisecondes, avant que l'exfiltration ne commence.

Revision #1
Created 2026-07-24 06:50:06 UTC by Dennis Underwood
Updated 2026-07-24 06:50:06 UTC by Dennis Underwood