

Où Windows stocke-t-il les mots de passe et les identifiants ?

Réponse courte : À plusieurs endroits prévisibles — le Gestionnaire d'identification Windows, les magasins de mots de passe des navigateurs, la configuration du client VPN et, sur les contrôleurs de domaine, la base de données Active Directory (NTDS). « Prévisible » est le mot clé : les attaques automatisées reposent sur le fait que ces emplacements sont identiques sur chaque machine.

Les principaux emplacements de stockage

- **Gestionnaire d'identification Windows** — identifiants enregistrés pour les ressources réseau et les applications.
- **Magasins de mots de passe des navigateurs** — Chrome, Edge et Firefox conservent chacun les identifiants enregistrés dans des chemins de profil connus.
- **Identifiants du client VPN** — noms d'utilisateur, mots de passe et éléments d'authentification par clé.
- **NTDS (Active Directory)** — sur un contrôleur de domaine, les données d'identification de l'ensemble du domaine. La cible la plus précieuse du réseau.
- **Magasins propres aux applications** — les outils de messagerie et de collaboration, les clients de transfert de fichiers et les plateformes de jeu gèrent chacun les leurs.

Pourquoi la prévisibilité est l'essentiel du problème

Les attaquants ne connaissent rien de votre environnement spécifique. Leur automatisation est conçue pour des chemins qui existent partout — `C:\Users\[Username]`, les dossiers de données d'application standard, les lettres de lecteur standard. Un script n'a pas besoin de comprendre votre réseau ; il se contente de parcourir des chemins connus.

C'est une faiblesse dans leur méthode. Si ces emplacements précis sont ceux qui sont surveillés, l'exigence de fiabilité propre à l'attaquant devient elle-même le déclencheur qui permet de le repérer.

Ce que Cyber Crucible en fait

Ces magasins constituent les points d'entrée surveillés du vol d'identité. L'intention d'un programme qui les lit est évaluée en moins de 200 millisecondes — et il est suspendu si cette intention est malveillante, avant que le moindre identifiant ne soit dérobé.

Revision #1

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

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