Pourquoi les attaques automatisées ciblent-elles les mêmes emplacements sur chaque ordinateur ?

Réponse courte : Les attaquants ne savent rien de votre environnement spécifique, c'est pourquoi leur automatisation est conçue pour cibler des emplacements qui existent sur pratiquement toutes les machines — les dossiers de profils utilisateurs, les lettres de lecteur et les répertoires de données d'application. Cette prévisibilité constitue une faiblesse que les défenseurs peuvent exploiter.

Les cibles prévisibles

- **Profils utilisateurs et bureaux :** sous Windows, `C:\Users\[Username]` contient de manière fiable des données précieuses. Un script parcourt tous les répertoires utilisateurs sans avoir besoin de comprendre le système.
- **Lettres de lecteur :** les outils automatisés énumèrent `C:\`, `D:\`, et au-delà pour trouver des partages réseau, des lecteurs externes et des partitions montées à chiffrer.
- **Dossiers de données d'application :** chaque système d'exploitation conserve les identifiants, cookies et configurations dans des chemins connus — des cibles de choix pour le vol d'identifiants.

Retourner la prévisibilité contre l'attaquant

Le schéma d'attaque n'est pas réfléchi ; il s'agit d'un balayage brutal des emplacements bien connus. Cyber Crucible surveille précisément ces points d'entrée connus pour le vol d'identité et de données. Tout programme qui accède à des données à ces emplacements — ainsi que ses processus parents et enfants et les bibliothèques associées — voit son intention évaluée en une fraction de seconde, et est intercepté si cette intention est malveillante.

Revision #1
Created 2026-07-24 06:49:58 UTC by Dennis Underwood
Updated 2026-07-24 06:49:58 UTC by Dennis Underwood