Wo speichert Windows Passwörter und Anmeldeinformationen?

Kurze Antwort: An mehreren vorhersehbaren Orten – im Windows-Anmeldeinformationsverwaltung (Credential Manager), in den Passwortspeichern der Browser, in der VPN-Client-Konfiguration und, auf Domänencontrollern, in der Active-Directory-Datenbank (NTDS). „Vorhersehbar" ist dabei das entscheidende Wort: Automatisierte Angriffe verlassen sich darauf, dass diese Orte auf jedem Rechner gleich sind.

Die wichtigsten Speicherorte

- **Windows-Anmeldeinformationsverwaltung (Credential Manager)** — gespeicherte Anmeldedaten für Netzwerkressourcen und Anwendungen.
- **Passwortspeicher der Browser** — Chrome, Edge und Firefox speichern gespeicherte Anmeldeinformationen jeweils an bekannten Profilpfaden.
- **VPN-Client-Anmeldeinformationen** — Benutzernamen, Passwörter und schlüsselbasiertes Authentifizierungsmaterial.
- **NTDS (Active Directory)** — auf einem Domänencontroller die Anmeldeinformationsdaten für die gesamte Domäne. Das wertvollste Ziel im Netzwerk.
- **Anwendungsspezifische Speicher** — Messaging- und Collaboration-Tools, Dateiübertragungs-Clients und Gaming-Plattformen unterhalten jeweils eigene Speicher.

Warum Vorhersehbarkeit der entscheidende Punkt ist

Angreifer wissen nichts über Ihre spezifische Umgebung. Ihre Automatisierung ist für Pfade geschrieben, die überall existieren — `C:\Users\[Username]`, Standardordner für Anwendungsdaten, Standard-Laufwerksbuchstaben. Ein Skript muss Ihr Netzwerk nicht verstehen; es durchläuft einfach bekannte Pfade.

Das ist eine Schwäche in ihrer Methode. Wenn genau diese Orte überwacht werden, wird die eigene Zuverlässigkeitsanforderung des Angreifers zu dem Auslöser, der ihn entlarvt.

Was Cyber Crucible damit macht

Diese Speicherorte sind die überwachten Einstiegspunkte für Identitätsdiebstahl. Bei einem Programm, das darauf zugreift, wird die Absicht in weniger als 200 Millisekunden bewertet — und es wird angehalten, falls diese Absicht bösartig ist, noch bevor eine Anmeldeinformation entwendet werden kann.

Revision #1
Created 2026-07-24 04:29:39 UTC by Dennis Underwood
Updated 2026-07-24 04:29:39 UTC by Dennis Underwood