Warum zielen automatisierte Angriffe auf jedem Computer auf dieselben Speicherorte ab?

Kurze Antwort: Angreifer wissen nichts über Ihre spezifische Umgebung, daher ist ihre Automatisierung so geschrieben, dass sie auf Speicherorte abzielt, die praktisch auf jedem Rechner existieren – Benutzerprofilordner, Laufwerksbuchstaben und Anwendungsdatenverzeichnisse. Diese Vorhersehbarkeit ist eine Schwachstelle, die Verteidiger nutzen können.

Die vorhersehbaren Ziele

- **Benutzerprofile und Desktops:** Unter Windows enthält `C:\Users\[Username]` zuverlässig wertvolle Daten. Ein Skript durchläuft jedes Benutzerverzeichnis, ohne das System verstehen zu müssen.
- **Laufwerksbuchstaben:** Automatisierte Tools zählen `C:\`, `D:\` und weitere Laufwerke auf, um Netzwerkfreigaben, externe Laufwerke und eingebundene Partitionen zur Verschlüsselung zu finden.
- **Anwendungsdatenordner:** Jedes Betriebssystem speichert Zugangsdaten, Cookies und Konfigurationen an bekannten Pfaden – bevorzugte Ziele für Identitätsdiebstahl.

Die Vorhersehbarkeit gegen den Angreifer wenden

Das Angriffsmuster ist nicht durchdacht; es ist ein plumpes Durchkämmen bekannter Speicherorte. Cyber Crucible überwacht genau diese bekannten Einstiegspunkte für Identitäts- und Datendiebstahl. Bei jedem Programm, das an diesen Speicherorten auf Daten zugreift – zusammen mit seinen übergeordneten und untergeordneten Prozessen sowie den zugehörigen Bibliotheken – wird die Absicht in Bruchteilen einer Sekunde bewertet und im Falle einer böswilligen Absicht unterbunden.

Revision #1
Created 2026-07-24 04:26:33 UTC by Dennis Underwood
Updated 2026-07-24 04:26:33 UTC by Dennis Underwood