Was ist ein Infostealer, und warum ist der Diebstahl von Sitzungstoken so gefährlich?

Kurze Antwort: Ein Infostealer ist Schadsoftware, die darauf ausgelegt ist, digitale Identitätsdaten – Passwörter, Sitzungstoken, API-Schlüssel und VPN-Anmeldedaten – abzugreifen und schnell zu exfiltrieren. Ein gestohlenes Sitzungstoken ist gefährlich, weil es Passwörter und Multi-Faktor-Authentifizierung oft vollständig umgeht und einem Angreifer erlaubt, sich als legitimer Benutzer anzumelden.

Warum Angreifer heute Identitäten stehlen, statt im Netzwerk zu verweilen

Moderne Angreifer vermeiden es zunehmend, sich dauerhaft in einem Netzwerk aufzuhalten. Ein Verbleib in der Umgebung erhöht die Wahrscheinlichkeit einer Entdeckung. Stattdessen entwenden sie die Identitätsdaten und verschwinden wieder, was ihnen zwei Vorteile verschafft:

1. **Geringeres Risiko** – Sie analysieren das Gestohlene in einer sicheren Umgebung, in ihrem eigenen Tempo.
2. **Einfache Rückkehr** – Mit einem gültigen Sitzungstoken, Passwort oder VPN-Schlüssel können sie jederzeit zurückkehren und erscheinen dem Authentifizierungssystem gegenüber vollkommen legitim.

Warum Geschwindigkeit das eigentliche Problem ist

Diese Tools bewegen sich innerhalb von Sekunden von der Infiltration zur Selbstlöschung – schneller, als eine Cloud-Warnung das Gebäude verlassen kann. Cyber Crucible erkennt die Absicht im Moment des Zugriffs auf Identitätsdaten und unterbricht den Prozess in unter 200 Millisekunden, bevor die Exfiltration beginnt.

Revision #1
Created 2026-07-24 04:26:43 UTC by Dennis Underwood
Updated 2026-07-24 04:26:43 UTC by Dennis Underwood