Warum haben Sicherheitstools mit „Cloud-Collector“ Schwierigkeiten bei modernen Angriffen?

Kurze Antwort: Ein Cloud-Collector ist ein schlanker Endpoint-Agent, der kaum lokale Analysen durchführt und stattdessen rohe Telemetriedaten zur Verarbeitung an eine Cloud-Plattform sendet. Dieser Umweg verursacht eine Verzögerung, die ein automatisierter Angriff nicht zulässt, und der Agent ist zudem von genau den Betriebssystemkomponenten abhängig, die Angreifer heute kompromittieren.

Warum die Branche es so aufgebaut hat

Kernel-Level-Engineering ist schwierig und teuer. Das Versenden von Telemetriedaten in die Cloud erlaubte es Anbietern, günstigere Endpoint-Software zu entwickeln, Cloud-Speicher zu monetarisieren und „Cloud-KI“-Funktionen zu vermarkten. Das Modell wurde auf einfache Entwicklung optimiert, nicht auf Verteidigung.

Die beiden Fehlermodi

1. **Zu langsam.** Automatisierte „Smash-and-Grab“-Angriffe sind innerhalb von Millisekunden abgeschlossen. Cloud-Analysen können in dieser Zeit keine Reaktion auslösen.
2. **Blind, wenn es am wichtigsten ist.** Da diese Agenten zum Funktionieren und zur Datenerfassung auf native Betriebssystembibliotheken angewiesen sind, kann ein Angreifer, der diese Bibliotheken kompromittiert, den Agenten zum Schweigen bringen. Er läuft weiter, meldet aber nichts – ein Dashboard, das signalisiert, alles sei in Ordnung, während Daten abfließen.

Cyber Crucible verarbeitet lokal im Kernel und trifft eigene Entscheidungen, sodass kein Umweg über die Cloud nötig ist und keine Abhängigkeit von einem möglicherweise kompromittierten Betriebssystem besteht.

Revision #1
Created 2026-07-24 04:32:42 UTC by Dennis Underwood
Updated 2026-07-24 04:32:42 UTC by Dennis Underwood