Was ist Rogue Process Prevention (RPP)?

Kurze Antwort: Rogue Process Prevention ist Cyber Cruciblees patentierter Ansatz, aktiv gegen einen bösartigen Prozess einzuschreiten, statt ihn lediglich zu beobachten. Ob es sich um Ransomware handelt, die mit der Verschlüsselung beginnt, oder um einen Infostealer, der nach einem Sitzungstoken greift – der Prozess wird gestoppt, bevor Daten das Gerät verlassen.

Beobachten versus eingreifen

Der Großteil des Endpoint-Marktes ist darauf ausgelegt, zu beobachten. RPP ist darauf ausgelegt, einzugreifen. Der Unterschied entspricht dem zwischen einer Überwachungskamera, die einen Einbruch zur späteren Auswertung aufzeichnet, und einem Wachmann, der den Dieb am Tresor aufhält.

Wogegen es schützt

RPP adressiert die drei zentralen Bedrohungen gemeinsam, da moderne Angriffe in der Regel mehrgleisig erfolgen:

- **Identitätsdiebstahl** — Zugriff auf Schlüssel, Token und Passwörter, häufig völlig ohne Zutun des Mitarbeiters.
- **Informationsdiebstahl** — Massenexfiltration von Daten in Maschinengeschwindigkeit.
- **Ransomware** — Verhaltensanalyse in Kombination mit Hacker-Täuschungstechnologie, die die Verschlüsselung selbst einer einzigen Datei verhindert.

Eine Verteidigung, die sich eng auf Ransomware allein konzentriert, würde die ersten beiden Phasen übersehen – dort, wo der eigentliche Schaden meist beginnt.

Revision #1
Created 2026-07-24 04:34:55 UTC by Dennis Underwood
Updated 2026-07-24 04:34:55 UTC by Dennis Underwood