Warum erfordert der Schutz von Identitätsdaten Zugriff auf Kernel-Ebene?

Kurze Antwort: Weil der Diebstahl in dem Bereich zwischen der Anforderung von Anmeldedaten durch ein Programm und deren Bereitstellung durch das Betriebssystem stattfindet. Nur eine Verteidigung, die auf Kernel-Ebene arbeitet — unterhalb der Anwendungen und Bibliotheken, die ein Angreifer manipulieren kann — kann diese Anfrage erkennen, ihre Absicht beurteilen und sie rechtzeitig stoppen.

Die drei Anforderungen

1. Den Zugriff erkennen, während er geschieht. Identitätsdiebstahl äußert sich nicht dadurch, dass eine Datei auf der Festplatte erscheint; es handelt sich um einen Lesevorgang. Tools, die nach schädlichen Dateien suchen, sehen nichts, da bei einem modernen Infostealer nichts geschrieben wird. Der zu erfassende Vorgang ist der Zugriffsversuch selbst.

2. Schnell genug entscheiden. Automatisierte Tools können innerhalb von Sekunden eindringen, Daten sammeln und sich selbst löschen. Jede Architektur, die Telemetriedaten an einen Cloud-Dienst sendet und auf ein Urteil wartet, hat das Rennen bereits verloren. Die Entscheidung muss lokal erfolgen, innerhalb von Millisekunden.

3. Nicht von dem abhängen, was der Angreifer kontrolliert. Sicherheitstools, die auf Betriebssystembibliotheken angewiesen sind, können blind werden, wenn ein Angreifer diese Bibliotheken im Arbeitsspeicher kompromittiert — der Agent läuft weiter, meldet jedoch nichts. Cyber Crucible wurde bewusst von den Windows-Bibliotheken entkoppelt, sodass ein kompromittiertes Betriebssystem es nicht zum Schweigen bringen kann.

Die Konsequenz

Der Betrieb auf Kernel-Ebene ist es, der alle drei Anforderungen gleichzeitig ermöglicht: Sichtbarkeit des Zugriffsversuchs, eine lokale Entscheidung in unter 200 Millisekunden und Unabhängigkeit von einem möglicherweise kompromittierten Betriebssystem.

Deshalb funktioniert der Schutz auch ohne jegliche Konnektivität — abgeschottet (air-gapped), offline oder auf See —, da nichts das Gerät verlassen muss, damit eine Entscheidung getroffen werden kann.

Revision #1
Created 2026-07-24 04:30:16 UTC by Dennis Underwood
Updated 2026-07-24 04:30:16 UTC by Dennis Underwood