Was ist ein System32-DLL-In-Memory-Angriff?

Kurze Antwort: Es handelt sich um einen Angriff, der die zentralen Windows-Codebibliotheken (System32-DLLs) infiziert, während diese im Arbeitsspeicher ausgeführt werden. Da nahezu jede Anwendung und jedes Sicherheitstool zur Funktion auf diese Bibliotheken angewiesen ist, verschafft deren Kompromittierung einem Angreifer nahezu vollständige Kontrolle über den Endpunkt – bei minimalen Spuren.

Warum dies den Höhepunkt der Endpoint-Angriffstechniken darstellt

System32-DLLs stellen die grundlegenden Operationen bereit, auf die sich Windows und seine Anwendungen verlassen – Speicherzuweisung, Kryptografie, Netzwerkkommunikation. Sie wurden für Geschwindigkeit und Zuverlässigkeit entwickelt, niemals dafür, im laufenden Produktivbetrieb gepatcht oder gehookt zu werden.

Ein Angreifer, der sie im Arbeitsspeicher verändern kann, erlangt die Fähigkeit, Daten und Programme auf dem System zu untersuchen, zu erstellen, zu verändern oder zu zerstören – mit nahezu nicht nachweisbarer Unauffälligkeit.

Warum die meisten Tools dies nicht erkennen können

Sicherheitsprodukte, die auf von Microsoft bereitgestellte Sensordaten angewiesen sind, verlassen sich per Definition auf genau die Bibliotheken, die angegriffen werden. Die für die Erkennung dieser Angriffsklasse erforderlichen Sensoren existieren in Standard-Toolsets schlicht nicht – sodass das Tool verstummt, während es meldet, dass alles in Ordnung sei.

Cyber Crucible wurde bewusst so entwickelt, dass es unabhängig von Windows-Bibliotheken funktioniert, damit ein kompromittiertes Betriebssystem es nicht blenden oder deaktivieren kann.

Revision #1
Created 2026-07-24 04:27:00 UTC by Dennis Underwood
Updated 2026-07-24 04:27:00 UTC by Dennis Underwood