Was ist ein dateiloser (speicherinterner) Angriff?

Kurze Antwort: Ein dateiloser Angriff ist ein Angriff, bei dem niemals ein Programm auf die Festplatte geschrieben wird. Der Angreifer injiziert bösartigen Code direkt in den Speicher eines legitimen, vertrauenswürdigen Prozesses und baut dort seine Payload auf. Da keine Datei erstellt wird, haben Sicherheitstools, die Dateien scannen — einschließlich der meisten EDR-Lösungen — nichts zu finden.

Warum dateibasierte Tools versagen

Herkömmlicher Endpunktschutz basiert auf einer einfachen Annahme: Malware ist eine Datei, also müssen Dateien überprüft werden. Dateilose Angriffstechniken entfernen die Datei vollständig aus der Gleichung.

In einem realen Einsatz betrieb ein Finanzdienstleistungsunternehmen drei branchenführende EDR-Produkte (Microsoft, CrowdStrike und Sophos) zusammen mit einem Top-50-Managed-SOC. Angreifer kompromittierten ein vertrauenswürdiges Remote-Monitoring-Tool, injizierten Code in die Verwaltungsprozesse von Microsoft SQL Server und kompilierten ihre Ransomware sowie ihre Datendiebstahl-Malware direkt im Serverspeicher. Da nichts auf die Festplatte gelangte, waren alle drei EDR-Lösungen, der MDR-Dienst und das SOC vollständig blind. Cyber Crucible fing eigenständig fast 10.000 bösartige Prozesse ab — 98 % davon auf der SQL-Server-Farm — ohne einen einzigen Alarm des Legacy-Stacks.

Wie Cyber Crucible dies erkennt

Cyber Crucible überwacht Verhalten und Absicht auf Kernel-Ebene, anstatt Dateien zu scannen. Ein Prozess, der sich bösartig verhält, wird in weniger als 200 Millisekunden gestoppt — unabhängig davon, ob jemals eine Datei geschrieben wurde.

Revision #1
Created 2026-07-24 04:26:12 UTC by Dennis Underwood
Updated 2026-07-24 04:26:12 UTC by Dennis Underwood