Kann Cyber Crucible die laterale Bewegung von Angreifern stoppen?

Die Verhaltensanalyse-Engine des Produkts und die Zero-Trust-Methoden sammeln effektiv Nachweise für laterale Bewegung.

Dies können Nachweise für laterale Bewegung von Prozess zu Prozess auf dem Rechner selbst sein, oder es kann sich um die Entdeckung des Einstiegspunkts eines Angreifers in das System von einem entfernten System aus handeln, im Rahmen einer Root-Cause-Analyse.

Programme und ihre Argumente, die mit Methoden zur Prozessinjektion und mit „Living off the Land“-Prozessen verbunden sind, die andere Prozesse öffnen, werden erfasst und an Cyber Crucible übermittelt.

Aufgrund der kernelbasierten Verhaltensanalyse von Prozessen gibt es keine Prozesse, die für die Beobachtung und Berichterstattung durch Cyber Crucible zu privilegiert sind (einschließlich anderer Kernel-Treiber oder sogar anderer Endpoint-Security-Tools).

Automatisierte Gegenmaßnahmen gegen Erpressung erfolgen, sobald entweder Datenerpressung oder Ransomware-Verschlüsselungsaktionen begonnen werden.

Hier ist beispielsweise ein Video, das laterale Bewegung über einen Rechner hinweg zeigt, unter Verwendung von In-Memory-Techniken und dem Log4J-Exploit. Bitte beachten Sie, dass die automatisierte Suspendierung der betroffenen Prozesse erfolgte, nachdem Datendiebstahl- und Ransomware-Verhalten begonnen hatte.

rr-log4j-procinj-3mins.mp4

Ein weiteres Beispiel dieser Dynamik zeigt die Nutzung durch einen Angreifer, um eine Windows-Shell zu öffnen. Die Beobachtung erfasste alle Nachweise, aber die Aktivität wurde suspendiert, sobald die Windows-Shell versuchte, Datenerpressungsaktivitäten durchzuführen (in diesem Fall Datendiebstahl).

rr-com-dll.mp4

Schließlich wird auch die Migration von einem kompromittierten Browser aus beobachtet, und in diesem Fall gelang es dem Angreifer aufgrund der Überwachung des Speicherzustands des Browsers nie, sich erfolgreich vom kompromittierten Chrome-Browser aus zu bewegen:

rr-untrusted-chrome.mp4

Revision #1
Created 2026-07-24 04:24:01 UTC by Dennis Underwood
Updated 2026-07-24 04:24:01 UTC by Dennis Underwood