Was zeigt die Seite "Prozesserstellungen" an?

Es kommt sehr selten vor, möglicherweise sogar nie, dass ein Angreifer einen gesamten Angriff innerhalb eines einzigen Prozesses durchführt.

Die Tatsache, dass ein Angriffswerkzeug oder eine Windows-Bibliothek mehrere Prozesse und Windows-Programme nutzt, ist für die Nutzer der Malware (also die Kriminellen) manchmal unsichtbar.

Prozessverhalten stellt eine wichtige Quelle von Variablen bei der Entscheidungsfindung von Cyber Crucible dar, die verhaltensbasierte Indikatoren aus einer Vielzahl von Quellen einbezieht.

Manchmal führen diese Prozessverhalten letztlich zu einer Prozessunterbrechung aufgrund von Datendiebstahl oder Ransomware-Verschlüsselung und können vom Einstiegspunkt des Angreifers durch das System bis hin zur endgültigen Ausführung der Erpressersoftware zurückverfolgt werden.

In anderen Fällen kann die Prozessverfolgung unbefugten Fernzugriff, Betrug, Insider-Bedrohungen oder unerwartete Software identifizieren, jedoch keine Datenerpressung. Es handelt sich also nicht um etwas, das die Software von Cyber Crucible zur Verhinderung von Datenerpressung automatisch unterbindet, aber dennoch um etwas, worüber Sie informiert sein sollten.

Unabhängig davon, ob die Prozessdaten Teil eines Datenerpressungsangriffs sind, auf etwas anderes Bemerkenswertes hinweisen oder lediglich normales Programmverhalten darstellen, werden die Quell- und Zielinformationen der Programme, einschließlich der Programmargumente, zur Verfügung gestellt. Dies liefert einen umfangreichen Datensatz zur Verfolgung von Angreifern, einschließlich solcher, die Taktiken des „living off the land“ nutzen.

Nachfolgend finden Sie einen Screenshot der Art von Daten, die aus Prozesserstellungen erfasst werden können.

CC_process_creation_demo.mp4

Revision #1
Created 2026-07-24 04:18:00 UTC by Dennis Underwood
Updated 2026-07-24 04:18:00 UTC by Dennis Underwood