Was passiert, wenn CC Speicherangriffe erkennt

Zunächst ist es sehr wichtig zu beachten, dass Speicheränderungen aus verschiedenen Gründen auftreten können:

1. In-Memory-Angriffe
2. Interaktion zwischen Programmen
3. Softwarefehler
4. Exploits

Eine Prozessinjektion oder Speicheränderungstechnik, die verwendet wird, auch zwischen Programmen, ist also nicht zwangsläufig eine bösartige Aktion.

Wenn ein Programm, das ein wahrscheinlich bösartiges Speicherereignis erlitten hat (also #1 oder #4 oben), in eine automatisierte Reaktion von Cyber Crucible einbezogen wird, erfolgt eine automatisierte Erfassungsaktivität.

Der Teil des Speichers, der in einem Programm verändert wurde, sowie der Zustand „davor“ wird in einem strukturierten Cyber Crucible-Format namens .ccdiff gespeichert.

Dieser injizierte oder veränderte Speicherbereich wird gespeichert und steht im Cyber Crucible Webportal zum Download zur Verfügung.

Warum wird dies nicht automatisch zur Analyse an Virustotal (etc.) übermittelt?

Unter bestimmten Umständen enthält der bei einem Angriff verwendete bösartige Code Variablen, die für einen Angriff spezifisch sind, insbesondere für ein Opfer.

Die Übermittlung dieses bösartigen Codes an eine öffentliche Analyseplattform wie Virustotal würde eine unerwünschte, opferidentifizierende Informationsoffenlegung gegenüber der Sicherheitscommunity darstellen.

Warum wäre die Übermittlung dieser Binärdaten an Virustotal (etc.) hilfreich?

Signaturbasierte Antivirus- und EDR-Tools suchen nach Zeichenfolgen oder Code-Bytes, die bei früheren Angriffen beobachtet wurden. Selbst wenn diese Malware noch nie zuvor gesehen wurde, kann sie nach einiger Zeit der Sicherheitscommunity bekannt werden. Diese Scan-Tools benötigen den Code in der Regel nicht in einem korrekt formatierten Binärformat, um eine Zuordnung zu einer bekannten Malware zu erkennen.

Revision #1
Created 2026-07-24 04:34:26 UTC by Dennis Underwood
Updated 2026-07-24 04:34:26 UTC by Dennis Underwood