Speichermodifikation

Was ist Speichermodifikation?

Speichermodifikation ist, wie Cyber Crucible den Begriff verwendet, der Zustand, wenn die ausführbaren Speicherbereiche eines Prozesses auf ungewöhnliche Weise verändert wurden. Die normale Ausführung eines gegebenen Prozesses, ohne äußere Manipulation, löst diese Modifikationen nicht aus – sie unterscheiden sich von normalen „flüchtigen Speicher“-Vorgängen innerhalb eines Prozesses.

Eine gängige Technik der Speichermodifikation ist Process Hollowing, bei der ein Angreifer einen Opferprozess auf dem Rechner startet, häufig zunächst in einem angehaltenen Zustand, und den ausführbaren Code so verändert, dass tatsächlich der Code eines anderen Programms ausgeführt wird.

Relevante MITRE-Taktiken:

- MITRE T1055 - Process Injection, in der Regel verwendet, um schädlichen Code in einem Zielprozess auszuführen, während der ursprüngliche Prozess weiterläuft.
- MITRE T1055-12 - Process Injection durch Ersetzen von Code in einem Prozess, typischerweise bevor dieser mit der Ausführung beginnt.
- MITRE T1559 - Inter-Prozess-Kommunikation kann dem Injektor nach Abschluss der Injektion Kontrolle über den Zielprozess verschaffen.
- MITRE T1548 - Der Missbrauch von Rechteausweitungskontrollen kann es einem Prozess ermöglichen, der normalerweise keine höheren Rechte hätte, eskaliert zu werden, um Zugriff auf geschützte Daten zu erhalten.

Welche Folgen hat das?

Speichermodifikationen können sehr ähnliche Folgen wie andere Process-Injection-Techniken haben, sind jedoch noch schwerer zu erkennen. Da es keine Erstellung von Remote-Threads oder Aufrufe externer Funktionen gibt, kann es oft sehr schwierig sein, Speichermodifikationen überhaupt zu erkennen, und noch schwieriger, sie einem bestimmten Prozess zuzuordnen.

Ein Prozess mit modifiziertem Speicher kann dazu gezwungen werden, bösartige Aktivitäten auszuführen, die er sonst nicht ausführen würde. Kein Prozess mit manipuliertem ausführbarem Speicher sollte als vertrauenswürdig eingestuft werden, da dies kein normales Vorkommnis bei Inter-Prozess-Kommunikation oder -Interaktionen ist.

Was unternimmt Cyber Crucible?

Cyber Crucible überwacht den Zustand des Speichers eines Prozesses während seines gesamten Lebenszyklus. Wird der Speicher als manipuliert eingestuft, wird der Prozess markiert und als nicht vertrauenswürdig betrachtet. Zum Zeitpunkt eines Erpressungsereignisses wird der Speicher als Snapshot erfasst, um ihn für mögliche IR-Untersuchungen bereitzustellen.

Der erfasste Speicher-Snapshot enthält den ursprünglichen, unveränderten ausführbaren Speicher sowie etwaige „Diffs“ mit ihren Offsets innerhalb des Prozessspeichers. Die Analyse dieser Speicherabbilder kann anspruchsvoll sein, liefert jedoch häufig starke Hinweise auf das Verhalten des bösartigen Codes.

Woran erkenne ich das?

Cyber Crucible Indicates Responses with Modified Memory

Cyber Crucible zeigt Reaktionen bei modifiziertem Speicher an

Modifizierter Speicher ist im Vergleich zu anderen Methoden der Process Injection schwerer und flüchtiger aufzuspüren. Stattdessen bieten wir einen schnellen booleschen Wert, um zu erkennen, dass eine Modifikation stattgefunden hat; die eigentliche Analyse der Speicher-Diffs erfordert dann eine tiefergehende Untersuchung.

Some raw memory

Roher Speicherinhalt

Disassembled memory

Disassemblierter Speicherinhalt

Die Erfassung des Speichers ist nur der erste Schritt; selbst nach der Disassemblierung kann der Code stark verschleiert und schwer lesbar sein. Die gute Nachricht ist, dass uns für diese Analyse viele Informationen zur Verfügung stehen, wenn wir über den ursprünglichen Speicher, die zugehörigen Metadaten, die Original-Ausführungsdatei und die modifizierten ausführbaren Anweisungen selbst verfügen.

1. ja, 2.

Beispielszenarien:

- Trainingsszenario - Speichermodifikation

Revision #1
Created 2026-07-24 03:52:53 UTC by Dennis Underwood
Updated 2026-07-24 03:52:53 UTC by Dennis Underwood