Wie unterscheidet sich CCs verhaltensbasierte Speicheranalyse vom Memory Scanning?

Was ist Memory Scanning?

Memory Scanning ist die Praxis, einen Speicherblock zu nehmen, ihn normalerweise zur Analyse an einen anderen Ort im System zu kopieren und ihn dann zu scannen.

Fotografie vs. Live-Aktion

Dies ist kein Live-Scanning des Programms während es agiert, sondern eine Momentaufnahme des Programms zu einem bestimmten Zeitpunkt. Man kann es sich wie eine Fotografie im Vergleich zu einem Live-Stream vorstellen. Der Zustand des Programms kann sich von einem Moment zum nächsten drastisch ändern, weshalb dies am ehesten für forensische Zwecke in einer kontrollierten Umgebung nützlich ist. In einer nicht kontrollierten Umgebung, wie einer Kundenumgebung, ist es weniger nützlich. Je ausgelasteter die Maschine ist oder je mehr ein Programm tut, desto schwieriger ist es, ein genaues Bild vom aktuellen Zustand eines Programms zu erhalten.

Cyber Crucible setzte zu Beginn stark auf Memory Scanning und versuchte, möglichst viele „Aufnahmen“ der Speicherzustände von Programmen zu machen. Als wir schneller wurden, stießen wir auf mehrere Engpässe hinsichtlich der Geschwindigkeit, mit der Speicher-Momentaufnahmen erstellt werden konnten, sowohl bei einzelnen als auch bei mehreren Programmen gleichzeitig.

Bedenken hinsichtlich CPU- oder GPU-Ressourcenverbrauch

Dieses Memory Scanning kann äußerst ressourcenintensiv sein und bei großen Programmen einige Zeit in Anspruch nehmen. Als Cyber Crucible noch Memory Scanning einsetzte, anstatt intelligenter

verhaltensbasierter Speicherüberwachung, war ein gesamter CPU-Kern für das Scannen reserviert.

Intel verfügt über eine innovative Technologie namens Intel TDT AMS, die auf bestimmten Intel-basierten Architekturen mit integrierter Intel-GPU verfügbar ist.

Sie scannt den Speicher eines Programms beim ersten Start und nutzt dabei die GPU, um die CPU nicht zu belasten. Zudem ist die GPU für die Art des durchgeführten Scannens leistungsfähiger (dazu später mehr).

Scan-Methodik

Memory Scanning wird durchgeführt, um nach bestimmten Codes oder „Strings“ zu suchen. Dabei handelt es sich oft um dieselben Datenfragmente, nach denen Antivirus-/EDR-Tools in potenziell bösartigen Dateien suchen.

Memory Scanning ist speziell begrenzter als einige der komplexen Suchvorgänge, die gegen eine Datei durchgeführt werden können.

Daher sucht das Scanning standardmäßig nach bereits bekannten Elementen, wie älterer Malware, ist dabei jedoch in seinen Möglichkeiten eingeschränkt.

Cyber Crucible scannte früher Speichersegmente nach kryptografischem Material, dies erwies sich jedoch für moderne Umgebungen als zu limitiert, und wir entwickelten eine andere Methode, um Verhaltensweisen mittels kernelbasierter Logik zu beobachten.

Verhaltensbasierte vs. Scan-Methodiken

Cyber Crucible ist aus mehreren Gründen von einer scan-basierten zu einer verhaltensbasierten Methodik übergegangen.

Nachteile des Scannings

Der erste Grund ist, dass ein Live-Bild über alle Programme hinweg genutzt werden musste. Momentaufnahmen ermöglichten es kaum, auch nur eine begrenzte Analyse abzuschließen, bevor bereits die nächste benötigt wurde. Zu viel Programmaktivität wurde übersehen, fast so, als würde eine Videokamera mit zu niedriger Bildrate arbeiten. Dies wurde durch die Notwendigkeit, alle Programme gleichzeitig zu überwachen, noch verstärkt. Server oder stark ausgelastete

Arbeitsstationen – wohl die Computer, die am meisten Überwachung benötigten und am wichtigsten waren – erhielten letztlich den geringsten Anteil an Überwachung. Unabhängig vom Unternehmen oder Produkt waren die technologischen Grenzen offensichtlich und nicht praktikabel.

Der zweite Grund ist, dass Scanning, abgesehen vom Ressourcenverbrauch, standardmäßig die Suche nach **etwas Bekanntem** erfordert. Memory Scanning muss also signaturbasiert sein. Zudem muss das Signatur-Scanning eine begrenzte Teilmenge des umfangreicheren Signatur-Scannings sein, das bei dateibasiertem Antivirus-Scanning zu finden ist. Angreifer umgehen dateibasierte Signaturabwehrmaßnahmen bereits seit Jahren; die Wahrscheinlichkeit, dass Angreifer durch ein weniger leistungsfähiges signaturbasiertes System entdeckt werden, ist sehr gering.

Vorteile der verhaltensbasierten Analyse

Die verhaltensbasierte Speicherüberwachung von Cyber Crucible erfordert keine Signaturen und nutzt Kernel-Speicherzugriff, um die Verhaltensweisen aller Programme gleichzeitig zu verfolgen. Lassen Sie uns das im Detail betrachten.

Erstens bedeutet verhaltensbasierte Überwachung, dass neue Malware oder Malware, die von Angreifern verändert wurde, um neu zu erscheinen, leicht in Echtzeit erkannt werden kann. Signaturbasiertes Scanning, ob von Speicher oder Dateien, beruht darauf, dass dieses spezifische Stück Malware bereits zuvor gesehen wurde. Angreifer umgehen signaturbasierte Abwehrmaßnahmen seit Jahren, trotz einer vollständigen Palette an Scan-Techniken gegen Dateien. Die für den Speicher verfügbaren Scan-Techniken stellen davon nur eine Teilmenge dar und sind noch weniger effektiv.

Zweitens ist die neuartige verhaltensbasierte Speicherüberwachung von Cyber Crucible in der Lage, über die gesamte Laufzeit der Programme hinweg in Echtzeit über alle Programme gleichzeitig zu bleiben. Memory Scanning leidet unter schwerwiegenden Ressourcenengpässen, die sich verschlimmern, je mehr Programme ausgeführt werden. Angreifer führen normalerweise Dutzende von Malware-Samples gleichzeitig aus und überlasten dadurch die Memory-Scanning-Analyse durch die Geschwindigkeit und Anzahl der gleichzeitig zu untersuchenden Programme – unabhängig davon, ob es sich um Zero-Day- oder alte Malware handelt.

Revision #1
Created 2026-07-24 04:34:14 UTC by Dennis Underwood
Updated 2026-07-24 04:34:14 UTC by Dennis Underwood