En quoi l'analyse comportementale de la mémoire de CC diffère-t-elle de l'analyse de la mémoire ?

Qu'est-ce que l'analyse de la mémoire ?

L'analyse de la mémoire est la pratique consistant à prendre un bloc de mémoire, généralement en le copiant vers un autre emplacement du système à des fins d'analyse, puis à l'analyser.

Photographie versus action en direct

Il ne s'agit pas d'une analyse en direct du programme pendant son fonctionnement, mais d'un instantané du programme à un moment donné. Pensez-y comme à une photographie, par opposition à une diffusion en direct. L'état du programme peut varier considérablement d'un instant à l'autre, ce qui la rend surtout utile comme exercice d'analyse forensique dans un environnement contrôlé. Elle est moins utile dans un environnement non contrôlé, comme celui d'un client. Plus une machine est occupée, ou plus un programme effectue d'opérations, plus il est difficile d'obtenir une image précise de l'état actuel d'un programme.

Cyber Crucible a débuté avec un usage intensif de l'analyse de la mémoire, en essayant de prendre de nombreuses « photographies » des états mémoire des programmes. À mesure que nous gagnions en rapidité, nous avons rencontré plusieurs goulots d'étranglement liés à la vitesse à laquelle les instantanés mémoire pouvaient être pris, et ce, sur plusieurs programmes à la fois.

Préoccupations liées à la consommation de ressources CPU ou

GPU

Cette analyse de la mémoire peut être extrêmement gourmande en ressources et peut prendre un certain temps pour les programmes volumineux. Lorsque Cyber Crucible utilisait l'analyse de la mémoire, plutôt que la surveillance comportementale intelligente de la mémoire, un cœur de CPU entier était dédié à cette analyse.

Intel propose une technologie innovante appelée Intel TDT AMS, disponible sur des architectures spécifiques basées sur Intel dotées d'un GPU Intel intégré.

Elle analyse la mémoire d'un programme dès son démarrage, en utilisant le GPU pour éviter de surcharger le CPU. De plus, le GPU offre de meilleures performances pour le type d'analyse effectuée (nous y reviendrons plus loin).

Méthodologie d'analyse

L'analyse de la mémoire est effectuée pour rechercher des codes ou des « chaînes » spécifiques. Il s'agit souvent des mêmes éléments de données que les outils antivirus/EDR recherchent dans les fichiers potentiellement malveillants.

L'analyse de la mémoire, en particulier, est plus limitée que certaines des recherches complexes pouvant être effectuées sur un fichier.

Par conséquent, l'analyse recherche par défaut des éléments déjà connus, comme des logiciels malveillants plus anciens, mais sa capacité à le faire est limitée.

Cyber Crucible analysait auparavant les segments de mémoire à la recherche de matériel cryptographique, mais cette méthode s'est révélée trop limitée pour les environnements modernes, et nous avons inventé une méthode différente pour observer les comportements, en utilisant une logique basée sur le noyau.

Méthodologies basées sur le comportement versus l'analyse

Cyber Crucible est passé d'une méthodologie basée sur l'analyse à une méthodologie basée sur le comportement pour plusieurs raisons.

Inconvénients de l'analyse

La première raison est qu'une image en direct devait être utilisée pour l'ensemble des programmes. Les instantanés rendaient très difficile l'achèvement, même d'une analyse limitée, avant qu'un nouvel instantané ne soit nécessaire. Trop d'activité des programmes passait inaperçue, un peu comme une caméra vidéo fonctionnant à un taux d'images par seconde trop faible. Ce problème était aggravé par la nécessité de surveiller tous les programmes simultanément. Les serveurs ou les postes de travail très sollicités, sans doute les ordinateurs nécessitant le plus de surveillance et étant les plus importants, se retrouvaient avec le pourcentage de surveillance le plus faible. Quelle que soit l'entreprise ou le produit, les limites technologiques étaient évidentes et intenables.

La seconde raison est que, au-delà de la consommation de ressources, l'analyse nécessite, par défaut, la recherche de **quelque chose de connu**. Ainsi, l'analyse de la mémoire doit être basée sur des signatures. De plus, cette analyse par signature doit se limiter à un sous-ensemble des fonctionnalités plus complètes de l'analyse par signature que l'on trouve dans l'analyse antivirus basée sur les fichiers. Les attaquants échappent déjà depuis des années aux défenses basées sur les signatures de fichiers ; il y a donc très peu de chances qu'ils soient détectés par un système basé sur des signatures moins performant.

Avantages de l'analyse comportementale

La surveillance de la mémoire basée sur le comportement de Cyber Crucible ne nécessite pas de signatures et exploite l'accès à la mémoire du noyau pour suivre les comportements de tous les programmes simultanément. Décomposons cela.

Premièrement, la surveillance comportementale signifie que les nouveaux logiciels malveillants, ou ceux modifiés par des attaquants pour paraître nouveaux, peuvent être facilement détectés en temps réel. L'analyse basée sur les signatures, qu'il s'agisse de la mémoire ou des fichiers, repose sur le fait d'avoir déjà rencontré ce logiciel malveillant spécifique auparavant. Les attaquants échappent aux défenses basées sur les signatures depuis des années, malgré une suite complète de techniques d'analyse appliquées aux fichiers. Les techniques d'analyse disponibles pour la mémoire ne constituent qu'un sous-ensemble de celles-ci, et sont encore moins efficaces.

Deuxièmement, la nouvelle surveillance comportementale de la mémoire de Cyber Crucible est capable de rester en temps réel sur l'ensemble des programmes simultanément, pendant toute la durée de leur exécution. L'analyse de la mémoire souffre de graves goulots d'étranglement de ressources qui s'aggravent à mesure que davantage de programmes s'exécutent. Les attaquants exécutent généralement des dizaines d'échantillons de logiciels malveillants à la fois, ce qui engorge l'analyse de la mémoire en raison de la vitesse et du nombre de programmes à examiner simultanément, qu'il s'agisse d'une menace de type zero-day ou d'un logiciel malveillant plus

ancien.

Revision #1
Created 2026-07-24 06:57:09 UTC by Dennis Underwood
Updated 2026-07-24 06:57:09 UTC by Dennis Underwood