

Modification de la mémoire

Qu'est-ce que la modification de la mémoire ?

La modification de la mémoire, telle que Cyber Crucible utilise ce terme, correspond au cas où les sections exécutables de la mémoire d'un processus ont été modifiées de manière anormale. L'exécution normale d'un processus donné, sans intervention extérieure, ne déclenche pas ces modifications – elles sont distinctes des opérations normales de « mémoire volatile » au sein d'un processus.

Une technique courante de modification de la mémoire est le process hollowing, dans laquelle un attaquant démarre un processus victime sur la machine, souvent dans un état suspendu, puis modifie le code exécutable pour exécuter en réalité le code d'un autre programme.

Tactiques MITRE pertinentes :

- [MITRE T1055](#) - Injection de processus, généralement utilisée pour exécuter du code malveillant dans un processus cible tout en permettant au processus d'origine de continuer.
- [MITRE T1055-12](#) - Injection de processus par remplacement de code dans un processus, généralement avant qu'il ne commence son exécution.
- [MITRE T1559](#) - La communication inter-processus peut permettre à l'injecteur de contrôler le processus cible une fois l'injection terminée.
- [MITRE T1548](#) - L'abus de contrôle d'élévation peut permettre à un processus qui n'aurait normalement pas de privilèges élevés d'être escaladé pour accéder à des données protégées.

Quelles sont les conséquences ?

Les modifications de la mémoire peuvent avoir des conséquences très similaires à d'autres techniques d'injection de processus, mais sont encore plus évasives. Comme il n'y a pas de création de threads distants, ni d'appels à des fonctions externes, il peut souvent être très difficile de détecter les modifications de la mémoire, et encore plus difficile de les attribuer à un processus

particulier.

Un processus dont la mémoire a été modifiée peut être forcé à mener une activité malveillante qu'il n'aurait autrement pas exécutée. Aucun processus dont la mémoire exécutable a été altérée ne doit être considéré comme fiable, car ce n'est pas un événement normal pour les communications ou interactions inter-processus.

Que fait Cyber Crucible ?

Cyber Crucible surveille l'état de la mémoire d'un processus tout au long de son cycle de vie. Si la mémoire est jugée avoir été altérée, alors le processus est signalé et considéré comme non fiable. Au moment où un événement d'extorsion se produit, la mémoire fait l'objet d'un instantané afin d'être fournie lors d'éventuelles investigations IR.

La mémoire capturée dans l'instantané contient la mémoire exécutable d'origine, non altérée, ainsi que les « diffs » (différences), avec leurs décalages (offsets) dans la mémoire du processus. L'analyse de ces vidages mémoire peut être complexe, mais peut fournir des preuves solides quant aux comportements du code malveillant.

Comment le savoir ?

Cyber Crucible Indicates Responses with Modified Memory

Cyber Crucible indique les réponses avec mémoire modifiée

La mémoire modifiée est plus difficile et plus éphémère à localiser que d'autres méthodes d'injection de processus. Au lieu de cela, nous fournissons une valeur booléenne rapide permettant de voir que la modification a eu lieu, et à partir de là, l'analyse des diffs réels de la mémoire nécessite une investigation plus approfondie.

Some raw memory

Mémoire brute

Disassembled memory

Mémoire désassemblée

La collecte de la mémoire n'est que la première étape ; même après désassemblage, le code peut être très obfusqué et difficile à lire. La bonne nouvelle est que nous disposons de beaucoup d'éléments pour cette analyse lorsque nous avons la mémoire d'origine, les métadonnées associées, l'exécutable d'origine et les instructions de l'exécutable modifié elles-mêmes.

1. oui, 2.

Exemples de scénarios :

- [Scénario de formation - Modification de la mémoire](#)

Revision #1

Created 2026-07-24 06:18:10 UTC by Dennis Underwood

Updated 2026-07-24 06:18:10 UTC by Dennis Underwood