Que se passe-t-il lorsque CC détecte des attaques en mémoire

Tout d'abord, il est très important de noter que les altérations de mémoire se produisent pour plusieurs raisons différentes :

1. Attaques en mémoire
2. Interaction entre programmes
3. Bugs logiciels
4. Exploits

Ainsi, une injection de processus ou une technique d'altération de mémoire utilisée, même entre programmes, n'est pas nécessairement une action malveillante.

Si un programme ayant subi un événement mémoire probablement malveillant (donc, #1 ou #4 ci-dessus) est impliqué dans une réponse automatisée de Cyber Crucible, une activité de collecte automatisée se produit.

La portion de mémoire qui a été altérée dans un programme, ainsi que l'état « avant », est enregistrée dans un format structuré Cyber Crucible appelé .ccdiff

Cette portion de mémoire injectée ou altérée est enregistrée et disponible en téléchargement dans le portail web Cyber Crucible.

Pourquoi cela n'est-il pas automatiquement soumis à Virustotal (etc.) pour analyse ?

Dans certaines circonstances, le code malveillant utilisé dans une attaque contient des variables qui sont propres à une attaque, spécifiquement à une victime.

Soumettre ce code malveillant à un moteur d'analyse public tel que Virustotal représenterait une divulgation d'informations identifiant la victime, non souhaitée, à la communauté de la sécurité.

Pourquoi la soumission de ces données binaires à Virustotal (etc.) serait-elle utile ?

Les outils antivirus et EDR basés sur des signatures recherchent des chaînes ou des octets de code observés lors d’attaques précédentes. Même si ce logiciel malveillant n’a jamais été observé auparavant, il pourrait, après un certain temps, être connu de la communauté de la sécurité. Ces outils d’analyse n’ont généralement pas besoin que le code soit dans un binaire correctement formaté pour signaler une association avec un logiciel malveillant connu.

Revision #1
Created 2026-07-24 06:57:21 UTC by Dennis Underwood
Updated 2026-07-24 06:57:21 UTC by Dennis Underwood