Que montre la page Créations de processus ?

Il est très rare, voire inexistant, qu'un attaquant réalise une attaque entière depuis un seul processus.

Le fait qu'un outil d'attaque ou une bibliothèque Windows utilise plusieurs processus et programmes Windows est parfois invisible aux utilisateurs du logiciel malveillant (c'est-à-dire les criminels).

Les comportements des processus représentent une source importante de variables dans la prise de décision de Cyber Crucible, laquelle s'appuie sur des indicateurs comportementaux provenant de diverses sources.

Ces comportements de processus peuvent parfois aboutir à une suspension de processus liée à un vol de données ou à un chiffrement par ranançongiciel, et peuvent être retracés depuis le point d'entrée de l'attaquant dans le système jusqu'à l'exécution finale du logiciel d'extorsion.

Dans d'autres cas, le traçage des processus peut permettre d'identifier un accès distant non autorisé, une fraude, une menace interne ou un logiciel inattendu, mais sans extorsion de données. Il ne s'agit donc pas nécessairement de quelque chose que le logiciel de prévention de l'extorsion de données de Cyber Crucible suspendra automatiquement, mais c'est tout de même une information que vous voudrez connaître.

Que les données de processus fassent partie d'une attaque d'extorsion de données, qu'elles concernent un autre élément notable, ou qu'il s'agisse simplement d'un comportement de programme, les informations sur la source et la destination des programmes, y compris les arguments des programmes, sont mises à disposition. Cela fournit un ensemble riche de données permettant de retracer les attaquants, y compris ceux qui utilisent des tactiques de « living off the land ».

Vous trouverez ci-dessous une capture d'écran du type de données pouvant être recueillies à partir des créations de processus.

CC_process_creation_demo.mp4

Revision #1
Created 2026-07-24 06:42:00 UTC by Dennis Underwood
Updated 2026-07-24 06:42:00 UTC by Dennis Underwood