Comment puis-je enquêter sur la cause profonde d'un événement ?

Il existe trois éléments de base d'analyse à votre disposition lors de l'investigation d'une alerte.

Il est actuellement plus probable qu'un attaquant mène diverses activités sur un système, en utilisant une combinaison de techniques en mémoire et de détournement de processus (injection ou hollowing), plutôt que d'exécuter un programme « hacker.exe » évident.

Analytique de la mémoire

Le premier élément de base se trouve sur la page Réponse ou Incident elle-même. L'analytique de la mémoire suit les comportements du processus en mémoire lors d'une inspection continue des comportements possibles d'extorsion de données (vol ou chiffrement).

Un état de mémoire indiquant une falsification probable est généralement révélateur d'un problème.

Ce n'est pas toujours malveillant en soi, car de mauvaises pratiques de programmation ou des bogues logiciels peuvent également entraîner la falsification de l'état de mémoire d'un programme en cours d'exécution.

63504385.png?width=680
Nous voyons ici un cas où un processus Adobe Acrobat présente des comportements possibles d'extorsion de données après l'ouverture d'un PDF téléchargé, et nous constatons que la mémoire du processus Acrobat avait été modifiée. Le processus Acrobat.exe sur le disque n'a été affecté

d'aucune manière.

L'analyse forensique de la mémoire impliquée avec l'Acrobat.exe suspendu indiquera probablement un problème préoccupant - possiblement un exploit en cours d'utilisation, sinon une injection de processus ou un hollowing de processus.

Pour les réponses d'extorsion dont la valeur Mémoire modifiée est Vrai, une icône de téléchargement est disponible dans la colonne Analyse de la cause profonde pour télécharger le fichier de différence mémoire (Memory Diff) pour la réponse :

63602693.png?width=680
Le fichier de différence mémoire (Memory Diff File) est le code source compilé de ce qui a été injecté dans le programme. Il contient probablement un logiciel malveillant et/ou du code d'exploit, à examiner par un analyste en malwares ou en sécurité. Notez que ce fichier ne contient pas le programme entier, seulement la partie qui a été modifiée par un exploit ou une technique d'attaque comme l'injection de processus. Apprenez-en plus sur ce fichier ici.

Analytique de l'injection de processus

Le premier indicateur qu'un événement d'injection de processus pertinent pour une réponse automatisée est peut-être présent est la colonne Threads distants non fiables (Untrusted Remote Threads) pour un incident/réponse. Cela indique qu'une analyse comportementale au niveau du noyau a révélé la présence d'un thread distant non fiable observé avec le processus menant un comportement de vol de données ou de type rançongiciel.

63471635.png?width=680
Une investigation plus approfondie peut être effectuée sur la page Injection de processus. La valeur True pour Threads distants non fiables est un bon indicateur pour décider de s'y rendre.

La colonne Analyse de la cause profonde comporte également une icône permettant de vous rediriger automatiquement vers la page Injections afin de n'afficher que les injections de processus liées à la réponse.

63602703.png?width=680
Après avoir cliqué sur l'icône des injections, vous serez dirigé vers la page Injections de processus, où vous verrez uniquement les injections de processus liées à la réponse :

63569930.png?width=680
Ici, sur la page Événements d'injection de processus, nous voyons le chemin et les arguments du processus injecteur, ainsi que le chemin et les arguments du processus injecté. Habituellement, les arguments jouent un rôle très important dans l'analytique de la mémoire, ou indiquent, par

exemple, quelles commandes PowerShell exécuter. Les identifiants de processus (PID) sont également présents, pour aider à retracer les injections itératives effectuées lorsqu'un attaquant passe de processus en processus, ou pour rechercher l'analyse de la cause profonde dans la page Création de processus.

63438879.png?width=680
Comment savions-nous que rundll32.exe était en réalité un éditeur d'antivirus ? Continuez votre lecture !

Analytique de la création de processus

Il est très rare qu'un attaquant n'utilise qu'un seul processus au cours de son attaque. Il se peut même qu'il ne sache pas que les outils qu'il utilise génèrent de nouveaux processus, et qu'il utilise divers outils d'administration sur le système infecté.

La page Création de processus suit tous les processus qui ouvrent d'autres processus (ou le même), les arguments utilisés, ainsi que les identifiants de processus, ou Pids, pour chaque source et destination.

Cela est effectué au niveau du noyau, ce qui signifie que rien n'est manqué.

Remarque : la télémétrie de Microsoft dispose d'une partie de ces données, mais pas de toutes. Nous choisissons de ne pas utiliser cette source de données, car nous avons constaté que cette source de télémétrie a été observée manquer des événements importants, ou être désactivée par des attaquants lors d'une attaque.

Quelle est la qualité de notre visibilité ?

Tout assembler - une investigation de bout en bout

Quelle est la qualité de notre visibilité, et à quelle vitesse pouvez-vous effectuer une analyse de la cause profonde ? Découvrez cet exemple - un antivirus disposant sans doute de l'un des niveaux de permissions les plus élevés sur un système a été observé en train d'essayer d'injecter du code dans notre logiciel Cyber Crucible. Nous espérons que c'était pour examiner notre logiciel, mais nous entrons tout de même en mode d'auto-protection (ainsi, cela a conduit notre logiciel à rejeter la falsification de l'antivirus... il n'existe aucune porte dérobée permettant à des parties externes d'accéder, de modifier ou d'utiliser notre logiciel).

Alors, commençons ici, avec une réponse automatisée :

63569937.png?width=680
Évidemment, Cyber Crucible n'est pas un rançongiciel. Nous voyons ici qu'une tentative d'injection de processus impliquant un comportement de thread distant suspect, en conjonction avec des comportements de type extorsion de données.

D'accord - regardons ce qui se passe dans les Événements d'injection de processus en cliquant sur l'icône des injections. 5 secondes plus tard - nous avons notre réponse !

63471644.png?width=56463438879.png?width=680

Mais attendez - rundll ? Ce n'est pas un hacker, n'est-ce pas ? Ce n'est sûrement pas un programme hacker.exe. Effectuons un peu de filtrage, pour obtenir notre réponse sur la page Création de processus. Nous n'avons pas de capture d'écran ici, mais les identifiants de processus sont disponibles pour toutes les réponses et injections de processus. Retournons à la page des réponses, et cliquons sur l'icône des créations de processus pour être dirigés vers la page Créations de processus et filtrer automatiquement la grille pour afficher les créations de processus liées à cette réponse.

63537184.png63438886.png?width=680

Rapidement et facilement, nous constatons maintenant que la « racine » (sans jeu de mots) était WebRoot, un éditeur d'antivirus, qui avait généré un processus rundll32.exe pour charger l'une des DLL de WebRoot, laquelle a ensuite tenté de faire *quelque chose* avec le logiciel de Cyber Crucible, pour le forcer à itérer à travers les fichiers comme un outil de vol de données.

Pourquoi avons-nous choisi de présenter cet exemple ?

Nous disposons d'exemples abondants du savoir-faire des attaquants, avec des niveaux de compétence variables de leur part. Les antivirus atteignent un niveau de permissions sur un système qui exige un très haut niveau de compétence, de technologie et de préparation de la part des attaquants. Le fait que Cyber Crucible détecte des comportements « de type hacker » de la part d'un outil de sécurité grand public, puis les arrête automatiquement, démontre certains des plus hauts niveaux d'excellence en ingénierie et en sécurité de notre part, sans se perdre dans des exploits individuels ou le savoir-faire des attaquants.

Revision #1
Created 2026-07-24 06:41:41 UTC by Dennis Underwood
Updated 2026-07-24 06:41:41 UTC by Dennis Underwood