

|  |
| --- |
|  |
| **VIRUS HUNTER**  Processus and process |
|  |

Page de service

**Référence :**

**Plan de classement :**

**Niveau de confidentialité :** public | corporate | confidential

**Mises à jour**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Auteur | Description du changement |
| NSI-1 | 04/02/2024 | Nathan Gabriele | Chasse aux malwares et empoisonnement DNS. |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Validation**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Nom | Rôle |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Diffusion**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Nom | Rôle |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Sommaire

[1 Rappel du contexte 1](#_Toc157980636)

[I. Objectifs 1](#_Toc157980637)

[2 Bibliographie 1](#_Toc157980638)

[3 Les prérequis fondamentaux 1](#_Toc157980639)

[II. Outils principaux utiliser : 2](#_Toc157980640)

[4 Cas 1 : Attaque Phishing. 2](#_Toc157980641)

# Rappel du contexte

NetWorking Solutions Inc. (NSI) est une société spécialisée dans les services numériques, qui se concentre sur la conception, la mise en place et la maintenance des infrastructures matérielles et logicielles pour ses clients.

En réponse à une récente demande en matière de cybersécurité, une entreprise a sollicité les services de NSI pour réaliser une analyse de sécurité sur les terminaux utilisés par son personnel. Un expert en sécurité informatique se rendra sur place afin d'évaluer les ordinateurs de bureau et portables, en inspectant les logiciels installés et en surveillant les processus en cours pour détecter toute vulnérabilité potentielle ou présence de logiciels malveillants.

Dans le cadre de cette analyse, l'utilisation de deux outils spécifiques est recommandée : Process Explorer et Process Monitor. Ces logiciels permettront une surveillance approfondie des activités en cours sur les machines, facilitant ainsi l'identification des éventuelles failles de sécurité et l'existence de programmes malveillants. Une explication détaillée du fonctionnement et de l'importance de ces outils sera fournie lors des démonstrations pratiques.

@More

# Objectifs

Actuellement, il est crucial de maintenir des machines sécurisées en utilisant à la fois un antivirus et un pare-feu activés. Cependant, il est important de comprendre que même avec ces mesures en place, ils ne sont pas totalement invincibles. En 2023, les attaques par logiciels malveillants ont augmenté de façon significative, avec une augmentation trimestrielle de 110 %. Un grand nombre de ces logiciels malveillants parviennent à contourner ces systèmes de défense. Cette statistique met en évidence l'importance de ne pas se reposer uniquement sur ces outils de sécurité, mais plutôt d'adopter une approche plus complète qui inclut la sensibilisation des utilisateurs, les mises à jour régulières du système et une surveillance active des menaces.

# Bibliographie

La bibliographie de ce projet est accessible localement sous le répertoire ‘biblio’ du *build* du projet et en ligne sur le site de veille technologique du projet.

# Les prérequis fondamentaux

* Avant de se lancer en cybersécurité, il est nécessaire d’assimiler certaines connaissances qui vous serons indispensable pour avancer dans se domaine. Les connaissances dont vous aurez besoins toucherons trois thèmes tel que les processus, les attaques et les virus. Nous verrons que ces trois thèmes sont intrasecment lié dans le monde de la cybersécurité.

1. Les virus.

* - Un virus est un programme, un code malveillant, qui peut vous causer du tort de différentes façons, telles que l'altération du système d'exploitation par la suppression de fichiers, la corruption de données ou l'altération des performances de la machine. Un virus, aussi appelé malware, peut se présenter sous différentes formes :

• Le virus macro : celui-ci s'exécute à l'intérieur d'un document tel qu'un fichier Word ou Excel, se propageant via des macros et pouvant causer des dommages importants aux fichiers.

• Le virus boot : ce type de malware s'installe sur la zone de démarrage d'un disque et s'active dès le démarrage de l'ordinateur.

• Le cheval de Troie : il s'agit de programmes malveillants qui se dissimulent dans des logiciels légitimes pour accéder à des informations privées ou pour contrôler à distance le poste infecté.

• Le ver : il se propage automatiquement à d'autres ordinateurs sur un réseau ou sur Internet.

• Le rootkit : il se dissimule sur un système afin d'échapper à la détection des logiciels de sécurité.

Vous l’aurez compris, il existe donc différent virus avec des méthodes de propagations différentes.

1. Les processus.

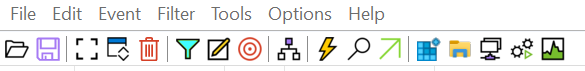
* Un processus peut être vu comme l’instance d’un programme en cours d’exécution sur un poste. Pour simplifier, à chaque fois qu’un programme est exécuté, un processus est créé. Celui-ci sera géré par le système, et on peut alors les considérer comme des tâches exécutées en arrière-plan ou en premier plan sur le poste. Un processus possède plusieurs attributs qui lui sont propres, tels que son ID de processus, la mémoire allouée et son état, c’est-à-dire en cours d’exécution ou en sommeil. Les processus peuvent être gérés et listés à l’aide de différentes commandes, par exemple la commande 'Get-Process' sur l’invite PowerShell. Celle-ci permet de lister tous les processus avec les exécutables associés, ainsi que les threads et les handles.

# Outils principaux utiliser :

Dans ce projet, nous allons explorer en détail les outils Process Explorer et Process Monitor, qui sont des logiciels cruciaux pour la détection et l'analyse des processus système. Ils seront particulièrement utiles dans le contexte de la chasse aux virus, car ils offrent une vue détaillée des activités en cours sur un système, permettant ainsi de repérer les comportements suspects associés à des infections. Nous procéderons à une démonstration pratique de leur fonctionnement sur un navigateur, afin d'illustrer concrètement leur utilité. Ensuite, nous simulerons une attaque réelle à l'aide d'un keylogger, un type de logiciel malveillant notoirement difficile à détecter pour les antivirus, en raison de sa capacité à rester discret. Cette démonstration mettra en lumière l'importance critique pour un technicien en cybersécurité de pouvoir repérer manuellement ce type de menace, soulignant ainsi l'importance de cet exemple dans notre étude.

# Cas 1 : Attaque Phishing.

* Dans ce premier cas d'utilisation, nous considérons plusieurs utilisateurs se plaignant de modifications de l'URL de la page d'accueil de leur navigateur Firefox. Une enquête est donc initiée. Dans cette situation, deux outils sont utilisés Process Explorer et Process Monitor : Dans un premier temps, l'utilisation de Process Explorer permettra d'identifier tout processus inconnu ou anormal sur le poste. Ensuite, l'utilisation de Process Monitor permettra de surveiller l'activité des processus en cours, notamment les entrées et sorties avec le système, telles que les opérations d'écriture ou de lecture.
* Une fois le programme suspect relevé, il est fort probable que vous souhaitiez connaitre ces interactions avec le système, pour cela, une capture d’évènements avec Process Monitor vous sera grandement utile, il vous faut vous rendre dans la barre d’outils en haut à droite :



* Ensuite, nous choisissons les options de filtre appropriées pour effectuer nos recherches :
* Une image contenant texte, capture d’écran, logiciel, affichage

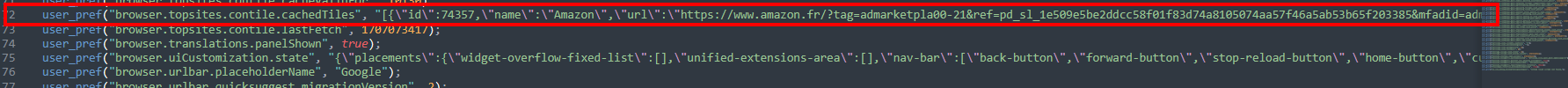
  Description générée automatiquement
* Ensuite, une fois les bons filtres en place, nous allons modifier la page d'accueil de Firefox pour simuler un empoisonnement SEO,
* L’empoisonnement SEO est une technique visant à manipuler les résultats des moteurs de recherche en utilisant des pratiques contraires aux directives établies, telles que la création de liens artificiels ou l'insertion de contenu trompeur, dans le but d'augmenter artificiellement le classement d'un site Web dans les résultats de
* Une image contenant texte, capture d’écran, Police, logiciel

  Description générée automatiquement
* Ensuite, on peut remarquer qu'il est clairement indiqué que Firefox a effectué une action de "write", c'est-à-dire d'écriture, sur le fichier de préférences de Firefox. Ce fichier est chargé au démarrage du navigateur et influence la page affichée lors de son lancement.
* Une image contenant texte, capture d’écran, nombre, Police

  Description générée automatiquement
* En regardant dans les propriétés de l'événement, on trouve le chemin d'accès directement indiqué, ce qui nous permet de localiser l'endroit où les modifications ont été effectuées.
* Une image contenant texte, capture d’écran, logiciel, Page web

  Description générée automatiquement
* Une fois que l'on a identifié l'action d'écriture, nous pouvons examiner les propriétés de l'action pour observer le fichier concerné par la modification de Firefox.
* Une image contenant texte, capture d’écran, logiciel, affichage

  Description générée automatiquement
* On peut constater ici que c'est la ligne de code qui sera chargée au démarrage de Firefox et qui déterminera la page sur laquelle l'utilisateur atterrit. Nous pouvons modifier ce lien à notre convenance pour effectuer un empoisonnement SEO, ce qui correspond au résultat trouvé juste avant.
* @More. Empoisonnement SEO avancé.
* On peut constater que sur la page d'accueil par défaut de Firefox, il y a des sites recommandés ou fréquemment utilisés par l'utilisateur. En examinant le code de notre fichier de préférences, il est possible de changer le lien pour détourner l'utilisateur vers le site Amazon de notre choix. Cela pourrait permettre aux pirates informatiques de récupérer diverses données, telles que les données bancaires. De plus, l'utilisateur ne remarquerait rien, car il accèderait au site de manière habituelle, sans se rendre compte de l'erreur. Il ne prêterait même pas attention au lien, car il utiliserait son raccourci habituel qu'il juge fiable. Cette situation est vraiment très dangereuse.
* Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

  Description générée automatiquement
* Il suffit de modifier le lien dans la ligne suivante avec l'adresse IP ou l'URL de notre choix, afin de diriger l'utilisateur vers l'endroit désiré.
* 
* Et l'utilisateur sera redirigé vers le site de notre choix.
* @More. Keyloger.exe
* Dans cette partie, nous allons développer un keylogger et tester l'efficacité de notre système de détection de virus en le confrontant à un virus réel dans un scénario authentique.
* Un keylogger est un type de logiciel malveillant conçu pour enregistrer et surveiller les frappes clavier d'un utilisateur sans son consentement, ce qui permet à un attaquant d'intercepter et de collecter des informations sensibles telles que les mots de passe, les numéros de carte de crédit et autres données confidentielles.
* Nous allons donc créer notre keylogger en Python :
* Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

  Description générée automatiquement

Maintenant, nous allons examiner les intégrations possibles du keylogger. Nous pouvons observer que dans un autre scénario, le keylogger agirait comme un cheval de Troie. On pourrait imaginer un fichier word.exe qui écrit de manière suspecte dans un fichier log.txt de manière persistante, alors qu'il n'a pas à effectuer une telle action. Nous pouvons ainsi constater qu'il interagit avec le fameux fichier log.txt :

* Une image contenant texte, capture d’écran, logiciel, nombre

  Description générée automatiquement
* Maintenant, si l'on ouvre ce fameux fichier log, on se rend compte qu'il contient les différentes touches que nous avons tapées au clavier, ainsi que certaines actions de la souris. Cela nous permet de constater que notre programme keylogger.exe avait bel et bien des actions suspectes.
* Une image contenant texte, capture d’écran, conception

  Description générée automatiquement