

|  |
| --- |
|  |
| **Windowns Malware Hunter Handbook**  Concepts et implémentations |
|  |

Page de service

**Référence :** n/a

**Plan de classement :** malware

**Niveau de confidentialité :** public

**Mises à jour**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Auteur | Description du changement |
| 1.0.0 | 20/01/2023 | Charly SIBOLD | Création |
| 1.0.1 | 21/01/2023 | Charly SIBOLD | Rappel du contexte, bibliothèque |
| 1.1.0 | 25/01/2023 | Charly SIBOLD | Process Explorer |
| 1.2.0 | 29/01/2023 | Charly SIBOLD | Process Monitor |
| 1.3.0 | 13/01/2023 | Charly SIBOLD | Empoissonnement DNS |
| 1.4.0 | 18/02/2023 | Charly SIBOLD | VirusTotal |

**Validation**

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

**Diffusion**

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

Sommaire

0 Sommaire

[1 Rappel du contexte 1](#_Toc125919940)

[2 Objectifs 1](#_Toc125919941)

[3 Voyage dans l’univers de Windows a la recherche au malware 1](#_Toc125919942)

[3.1 PROCESS EXPLORER. 2](#_Toc125919943)

[3.1.1 Surveillance des processus. 2](#_Toc125919944)

[3.1.2 Observation de la Mémoire 6](#_Toc125919945)

[3.1.3 Voir les ressources d’un processus 7](#_Toc125919946)

[3.2 Process Monitor 7](#_Toc125919947)

[3.2.1 1er Cas d’utilisation – Home page FireFox 7](#_Toc125919948)

# Rappel du contexte

Networking Solutions Inc. Ou d’où sont acronyme NSI est une société de service du Numérique (ESN[[1]](#footnote-1)) qui conçoit, réalise et maintient les infrastructures matérielles et logicielles de ses clients .

Cet entreprise propose d’hébergé votre site web en vous offrant de tout ce que vous avez besoin, que ce soit dans le développement de site web , aux média sociaux , à la publicité en plus et plus encore .

Mais aussi il peut vous aider pour votre entrepris, attirer de nouveaux clients , facturé les renouvellements .

# Objectifs

Depuis un certain temps jusqu’à aujourd’hui, il est nécessaire de faire fonctionnaire une machine avec un anti-virus . De fait, de multiple choix s’offre à nous ( cf. la comparaison des logiciels anti-virus publiée sur Wikipédia)

Tout a fois, les anti-virus[[2]](#footnote-2) ne sont pas fiables a 100% . En réalité, près de 75% des malwares passent au travers des défense instauré par l’anti-virus . Par exemple le Microsoft defender qui se retrouve a la traine contrairement à d’autre comme Avast, Avira etc… . C’est pourquoi la maîtrise des concepts et des outils qui permettent d’observer et  
d’analyser l’ensemble des fonctions et des actions des processus sur une machine est nécessaire.

# Voyage dans l’univers de Windows a la recherche au malware

Avant d’entré dans l’univers de Windows pour trouvé notre malware , il faut impérativement avoir un bon équipement sur soi , de bonne connaissance de la zone , de ceux qui y vive .

Donc dans cet partie, le lecteur/voyageur découvre quelque différent outils . Et dans une autre, on va se penché sur les principaux concepts d’un système d’exploitation , précisément dans une implémentation Windows :

* Processeur / processus | thread.
* Mémoire de masse – Fichiers.
* Mémoire vive.

Une boite à outils du nom de SysInternals est mis à disposition par microsoft pour user d’outils très puissant . Le logiciel est téléchargeable via ce lien : [https://docs. microsoft.co m/fr-fr/sysinternals/](https://docs.microsoft.com/fr-fr/sysinternals/)

SysInternals a été par un informaticien du de Mark Russinovich[[3]](#footnote-3) pour aidé à gérer, dépanné et diagnostiquer les systèmes et applications Windows Installé sur un ordinateur .

## PROCESS EXPLORER[[4]](#footnote-4).

 Logo de process explorer :

Nous pouvons voir que le logiciel a l’icone de démarrage de win7 a savoir le logo de Windows avec les 4 couleurs ( rouge , bleu , vert et jaune) avec un loupe qui se trouve par-dessus du logo .

Alors qu’est-ce qu’est process explorer ?

Process explorer est un gestionnaire de tâches bien plus performant que le gestionnaires de tâches standard de Windows déjà disponible sur les poste . Ce dernier permet[[5]](#footnote-5) :

* D’afficher et lister les processus chargés en mémoires ;
* Détailler les processus au niveau des threads ;
* Terminer ou arrêté les processus et/ou les threads ;
* Lister les ressources utilisées (handles, DLL , etc.) ;
* Analyser la performance du système d’un ordi ( CPU[[6]](#footnote-6), mémoire, GPU[[7]](#footnote-7),PID[[8]](#footnote-8) , etc.) ;
* Analyser un processus et de détecter la signature d’un virus s’il y a un présent ;
* Etc.

Une image contenant table

Description générée automatiquement

PID :il est un système de contrôle permettant d’améliorer les performances d’un asservissement.

CPU time : il représente la durée pendant laquelle une unité centrale de traitement est utiliser pour traiter les instruction d’un programme informatique ou d’un système d’exploitation.

Figure 1 : Process explorer, PID et CPU time .

### 3.1.1 Surveillance des processus.

Les processeurs sont au centre des systèmes informatique. Un processeur ou de son nom anglais process est le programme qui est chargé dans la mémoire d’un ordinateur. Il est défini de plus façon comme :[[9]](#footnote-9)

* Un ensemble d'instruction à exécuter, pouvant être dans la mémoire morte[[10]](#footnote-10), mais le plus souvent chargé depuis la mémoire de masse[[11]](#footnote-11) vers la mémoire vive ;
* Un espace d’adressage en mémoire vive pour stocker la pile, les données de travail, etc. ;
* Des ressources permettant des entrées sorties de données, comme des ports réseaux.

Ce schéma ci-dessous montre, de manière simpliste , le cycle de vie d’un processeur.



Figure 2 : cycle de vie d’un processeur.

Pour en savoir plus, l’invité peut consulter les note de bas page[[12]](#footnote-12) ou par ce lien : <https://www.lecluse.fr/nsi/NSI_T/archi/process/>

L’exécution du processus prend un certain temps, avec un début et une fin . Il peut être en attente , en exécution ,suspendu ou terminé par l’utilisateur via un autres processeur :

1. Le processeur se met en attente d’un évènement ;
2. L’ordonnanceur passe la main à un autre processeur ;
3. Ce même ordonnanceur choisi le processeur du schéma ;
4. Afin d’avoir l’évènement attendu se produise.

Tout « application » des utilisateurs installé sur un ordi est composer de processus[[13]](#footnote-13). On sait qu’une attaque informatique nécessite un ou des processus en cours d’exécution. Donc la surface d’attaque informatique dépend largement des application installé sur l’ordinateur de l’utilisateur.

Pour ça que process explorer compte les changements des d’état des processus en cas d’attaque etc.

Une image contenant table

Description générée automatiquement

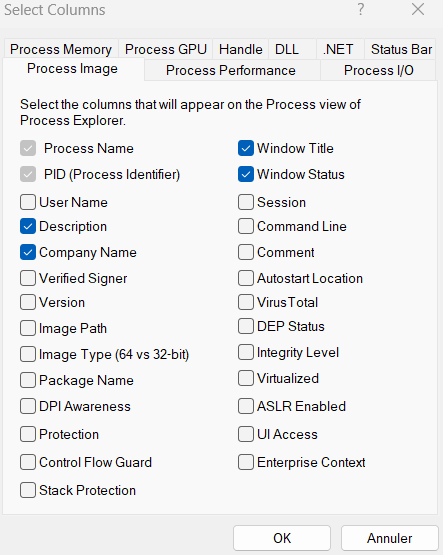
Context Switches (commutation de contexte): il consiste à sauvegarder l’état d’un processus ou d’un thread pour restaurer à la place celui d’un autre dans le cadre de l’ordonnancement d’un système d’exploitation multitâche.

Figure 3 : context switches et cswitch delta.

Chaque processeur à toujours aux minimaux un fil d’exécution mais il est possible qu’il en ait plus selon la façon dont le code du processus a été écrit et les choix architecture logicielle[[14]](#footnote-14) .

Les fils d’exécution se nomme thread[[15]](#footnote-15).

Pour une surveillance plus fine, il est possible de configurer Process Explorer .



Select Columns :

Depuis ces option, vous pouvez choisir les colonnes que vous voulez voir. Par exemple, j’ai cocher Window Title pour voir le titre de la fenêtre et Window statuts pour savoir si l’un des processus est en fonctionnement .

Mais vous pouvez avoir d’autres colonnes dans les autres partis comme les process Performance et/ou Process I/O.

Figure 4 : colonne de process image .

Les onglets permettent d’accéder à toutes les propriétés d’un processus. Dans Process Explorer , notre choix va se porté sur Verified Signer et Virus Total qui son deux indicateurs très important pour trouver la présence potentielle d’un logiciel dangereux .

Dans l’image ci-dessous, les processus d’un système Windows sont présenté sous forme d’une arborescence selon deux blocs précise :

Les processus en mode noyau[[16]](#footnote-16) et les processus en mode utilisateur.

Une image contenant table

Description générée automatiquement

En mode noyau : Tout le code qui s’exécute en mode noyau partage un seul [espace d’adressage virtuel](https://learn.microsoft.com/fr-fr/windows-hardware/drivers/gettingstarted/virtual-address-spaces). Par conséquent, un pilote en mode noyau n’est pas isolé des autres pilotes et du système d’exploitation lui-même. Si un pilote en mode noyau écrit accidentellement dans la mauvaise adresse virtuelle, les données qui appartiennent au système d’exploitation ou à un autre pilote peuvent être compromises. Si un pilote en mode noyau se bloque, l’ensemble du système d’exploitation se bloque.

En mode utilisateur : Chaque application s’exécute isolément, et si une application se bloque, le blocage est limité à cette application. Les autres applications et le système d’exploitation ne sont pas affectés par l’incident.

Figure 5 : copie d’écran de process explorer

Nous reviendrons plus loin dans ce document sur deux aspects importants sur la recherche du malware dans l’univers de Windows .

1. Premier point, la détection d’une empreinte virale avec VirusTotal, Développé par ispasec Sistemas . VirusTotal use de plusieurs moteurs antivirus en version ligne de commande avec des mise à jour régulièrement avec les fichiers de signature officiel des éditeurs publiés chacune respectifs. Mais en VirusTotal a été par Google[[17]](#footnote-17) en 2012.
2. Et deuxième point, la vérification de l’authenticité d’un code est fait par sa signature certifiée[[18]](#footnote-18)

### 3.1.2 Observation de la Mémoire

Chaque processus consomme de la mémoire sous plusieurs formes surtout en physique ou virtuelle. Le concept de mémoire virtuelle va de pair avec le concept multitâche. Il est strictement impossible d’exécuter simultanément plusieurs code exécutables sur un même processeur aussi, il est impossible de monter en RAM ( mémoire vive[[19]](#footnote-19)) tous les process en cours de fonctionnement sur une machine. Les systèmes d’exploitation modernes gèrent le concept de mémoire virtuelle[[20]](#footnote-20) qui étend la mémoire physique[[21]](#footnote-21).

Process Explorer permet de paramétrer l’affichage des données spécifique à la mémoire si nous cochons les colonnes que nous voulions .

Une image contenant texte

Description générée automatiquement

Virtual Size : Espace d’adressage virtuel .

Private Bytes : la quantité de mémoire demandé par les fils d’exécution du processus

Working Set Size : Mémoire physique totale (RAM) utilisée par le processus .

Figure 6 : Colonne de process memory

Une image contenant table

Description générée automatiquement

Figure 7 : privates bytes , working set et virtual size .

### 3.1.3 Voir les ressources d’un processus

Un processus ou un thread mobilise des ressource pour fonctionné .

## Process Monitor

Process Monitor[[22]](#footnote-22) est un logiciel de la suite de « Synternals » , ce logiciel nous donne la possibilité de monitorer/surveiller les actions de chaque processus en fonctionnement du système d’exploitation Windows d’un poste ou de votre poste en les capturant en temps réel

### 1er Cas d’utilisation – Home page FireFox

Dans ce premier cas d’utilisation , nous allons détaillé sur le comment faire pour identifier des processus malveillant/Intrus actifs qui sont présent sur un poste ou même le votre. Pour cela, nous allons présenter comment repérer un type d’attaque réalisable . L’un des exemple que nous pouvons données est un navigateur web pouvant modifier votre page d’accueil de votre logiciel de recherche comme Firefox vers un site malveillant.

Pour cette exemple , nous allons utiliser le navigateur Mozilla FireFox et on cherchera à trouver le fichier de configuration afin de remplacer la ligne concernant la page par défaut pour que Firefox démarre directement sur le site qu’on aura défini a savoir la page du site malveillant .

Alors , nous devons donc ouvrir le logiciel/programme « Procmon64.exe » ou « Procmon.exe » selon votre ordinateur. Une fenêtre va ouvrir et le programme commence instantanément à capturer les processus actifs et les listes sur la forme de tableau à plusieurs colonnes comme vous le voyer sur cet image ci-dessous.

Une image contenant texte

Description générée automatiquement

Path : Le chemin complet du répertoire d’où se situe le processus capturé

PID : L’identifiant unique du processus captuer

Process name : le nom du processus capturé

Time of day : le temps durant la journée actuel auquel le processus a été capturé

Result : le résultat de l’opération réalisé par le processus capturé

Detail : Diverses détails concernant le processus capturé .

Figure 8 : Process Monitor

Le logiciel possède une fonction de filtrage des processus selon divers critères que nous pouvons rajouté ou retiré . ça nous facilitera la tâche car nous pourrons afficher seulement les processus de Mozilla FireFox.

Pour avoir les processus de FireFox , il faut en préalablement l’ouvrir, puis cliqué sur le bouton qui est sur l’image ci-dessous qui est la capture en temps réel des processus.



Figure 9 : Capture des processus actif .

On remarque en placent le curseur l’icône de capture que l’action de capture des processus actifs peut être activer et désactiver via la commande Ctrl + E , ce qui permettra d’exécuter cette action plus rapidement si on la connait par cœur .

Un fois ça fait , nous allons cliqué sur le bouton filter montrer dans l’image ci-dessous .



Figure 10 : Bouton filter .

La page de filter va s’ouvrir , il aura trois champs à liste déroulants , l’un est le champ textuelle[[23]](#footnote-23) à renseigner et les bouton « Reset , Add , Remove , Apply , Cancel , Ok » ainsi qu’une boite au centre, nous montrant la liste des entré avec des case à cocher et des icones « booléennes[[24]](#footnote-24) » indicatifs .

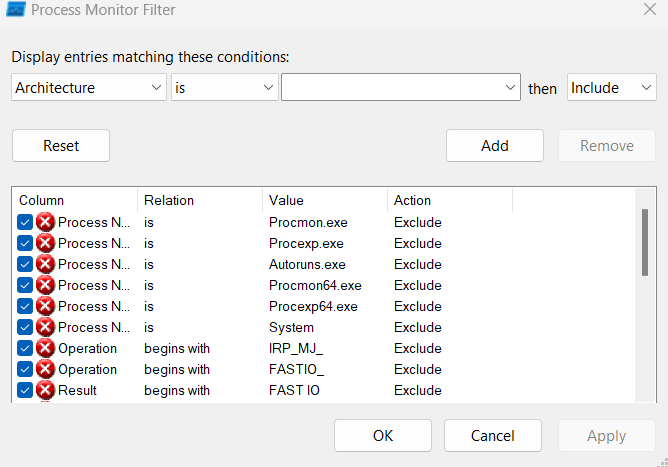


Figure 11 : fenêtre de filter .

Pour afficher uniquement les processus de FireFox , nous devrons renseigner les informations ci-dessous dans les trois champs et le champs textuelle .

* Process Name[[25]](#footnote-25) is firefox.exe Include
* Category is WRITE Include

Une image contenant table

Description générée automatiquement

Figure 12 : fenêtre de filter avec processus name firefox et catégory write .

Une fois cela fait , on peut fermer le filter ainsi de n’avoir que les processus de Firefox , donc il faut allez dans les paramètre de FireFox et changé au minimaux un paramètre , nous conseillons de changer seulement le paramètre de la page d’accueil , ça nous évitera de tout changé et ça nous facilitera la tâches .

Page d’accueil et nouvelle fenêtres : c’est le paramètres qui correspond a la page d’accueil et au nouvelle fenêtres de firefox que vous ouvrez

Une image contenant texte, moniteur, capture d’écran, écran

Description générée automatiquementFigure 13 : page de paramètre de Firefox .

Maintenant , nous pouvons retourner dans processor monitor pour récupérer le dernier informations que nous avons besoin pour 1er cas d’utilisation . Vous pouvez remarquer que nous récupérons seulement les processus de Firefox et celui qui nous intéresser est le processus finissant par  « prefs[[26]](#footnote-26) » .

Ce sont les processus de Firefox qui apparaisse après avoir modifier ces paramètres et le filtrage de process monitor .

Une image contenant texte

Description générée automatiquement

Figure 14 : Processus de Firefox obtenus par le filtrage .

Pour facilement , récupérer le processus qui nous intéresse , on use de la fenêtre recherche de process monitor qui est représenté par une loupe ou d’ouvrir la fenêtres avec la commande « Ctrl + f »



Figure 15 : Icone représentant la recherche

Une nouvelle s’ouvre dans process monitor , c’est cet fenêtre qui sera utiliser pour trouver le process « prefs » . Pour cela , il faut mettre dans le champs « Rechercher » le mots « prefs » pour n’avoir que les processus en question .

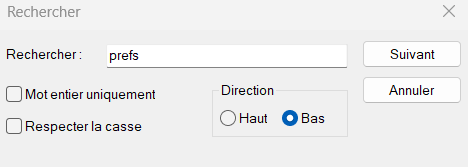


Figure 16 : Fenêtre de Recherche process monitor .

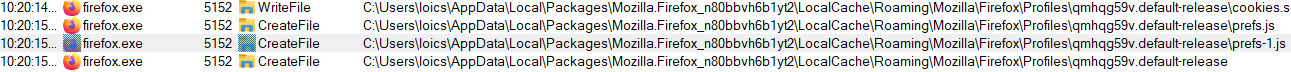


Figure 17 : Processus finissant par prefs .\*

Grace à cet fenêtre , nous trouvons le processus que nous voulions . **Attention** : Il ne faut pas prendre « prefs-1.js » , ce dernier correspond au préférence des nouvelles onglet , ce qu’on veux pas . Il faut prendre « prefs.js » qui correspond au paramètres modifier précédemment .

Pour copier le chemin , on doit faire clique droit sur le processus pour ensuite cliquer sur « properties » ou Ctrl+P.

Une image contenant texte

Description générée automatiquement

Figure 18 : properties .

Une nouvelle page s’ouvrira , ou on trouve tout les informations du processus « prefs.js » . On trouve « event properties[[27]](#footnote-27) » , « Process » et « Stack » .

L’information qui nous intéresse se trouve dans « event properties » qui se trouve ouvert dès qu’on ouvrir les propriétés du processus . C’est le path ( en français le chemin) qu’on va copier pour le rajouter dans le filtrage de process monitor .

Une image contenant texte

Description générée automatiquement

Path : c’est le chemin vers le fichiers de l’un des processus de Firefox .

Figure 19 : Event Properties d’un processus .

Pour le copier , il suffit prend le début du chemin jusqu’à la fin tout en restant sur le clique gauche ( Le chemin sera surligné en en bleu ‘’ ) puis faire clique droit pour allez sur le copier ou pour gagner du temps faire Ctrl + C[[28]](#footnote-28) .

Il aura plus qu’a retourner dans le filtrage pour rajouter le chemin du processus .

Une image contenant texte

Description générée automatiquement

Figure 20 : Filter et Path rajouter .

Une fois cela fait , il aura plus qu’a appliquer le filtrage pour n’avoir que les processus qui nous intéresse pour le cas . on devra avoir que les processus avec le mots « prefs.js » .



Figure 21 : Processus de Firefox avec prefs .

On voit que nous avons que les processus qu’on voulais filtrer , dans la colonne « Operation » , on remarque qu’il y a « CreateFile[[29]](#footnote-29) » ce qui signifie qu’un fichier de configuration a était créer lorsque que le processus de Firefox , ce lance .

On peut aussi supporter que si un fichier « prefs.js » était déjà présent alors ce dernier a du être écraser pour mettre le nouveau .

Maintenant , il est possible de récupérer le fichier et donc pour cela , nous avons cas faire clique droit puis cliquer sur « jump to[[30]](#footnote-30) » ou Ctrl + J Pour allez dans le dossier afin de copier le fichier « prefs.js »

Une image contenant texte

Description générée automatiquement

Figure 22 : Jump to…

Une image contenant texte

Description générée automatiquement

Figure 23 : Le dossier ou se trouve prefs.js .

Passez par process monitor , c’est de gagner du temps au lieu de passez par les différents dossier pour trouver notre fichier.js qui nous être très utile .

Il faudra faire un clique droit puis l’ouvrir avec Notepad++[[31]](#footnote-31) car on va l’utiliser pour notre exemple , si vous ne l’avez toujours pas installer sur votre poste de travail , passez par ce lien pour l’installé et une fois fait , faites les manipulation dit au-dessus et sur les image si-dessous : <https://notepad-plus-plus.org/downloads/>

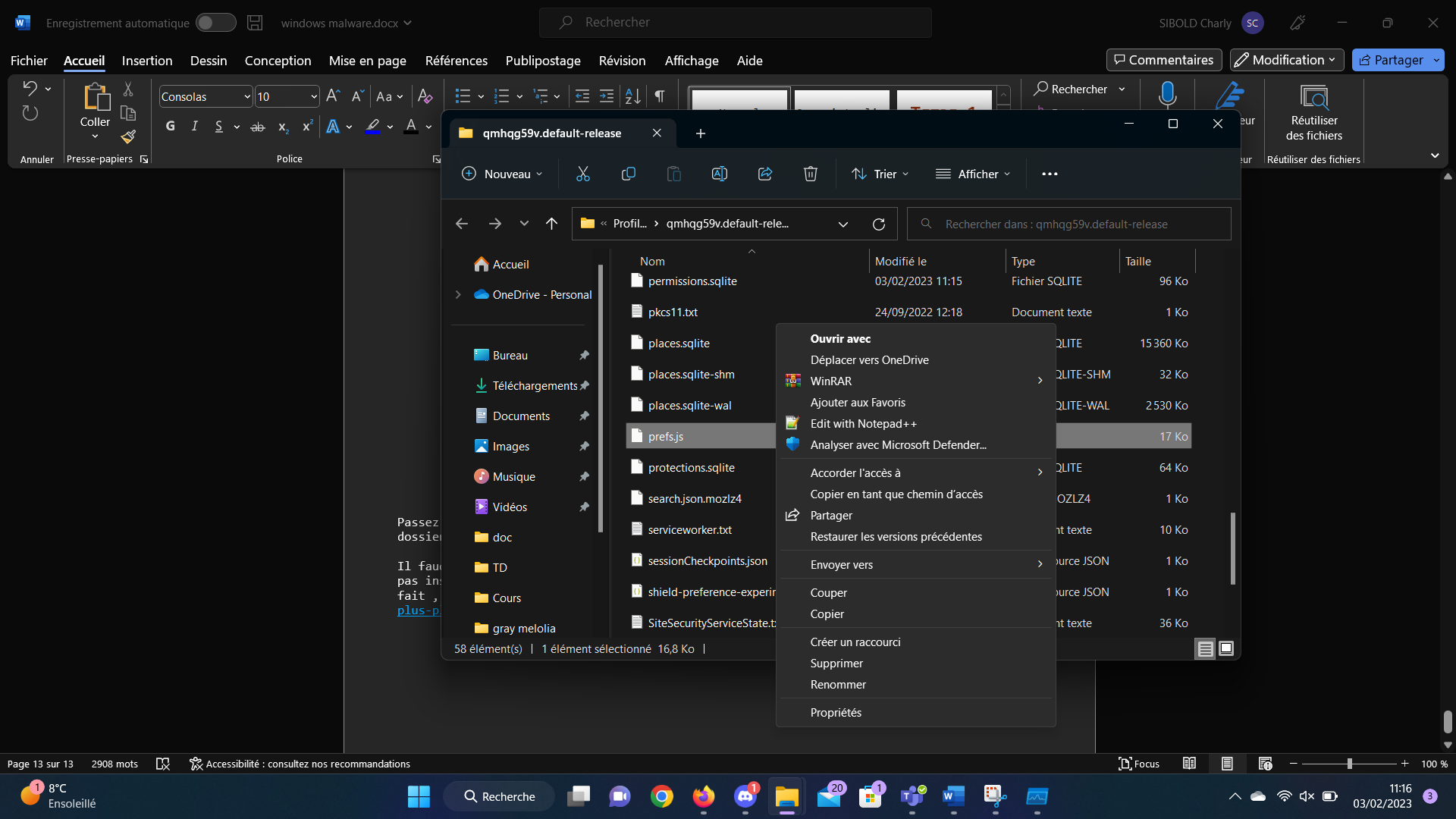
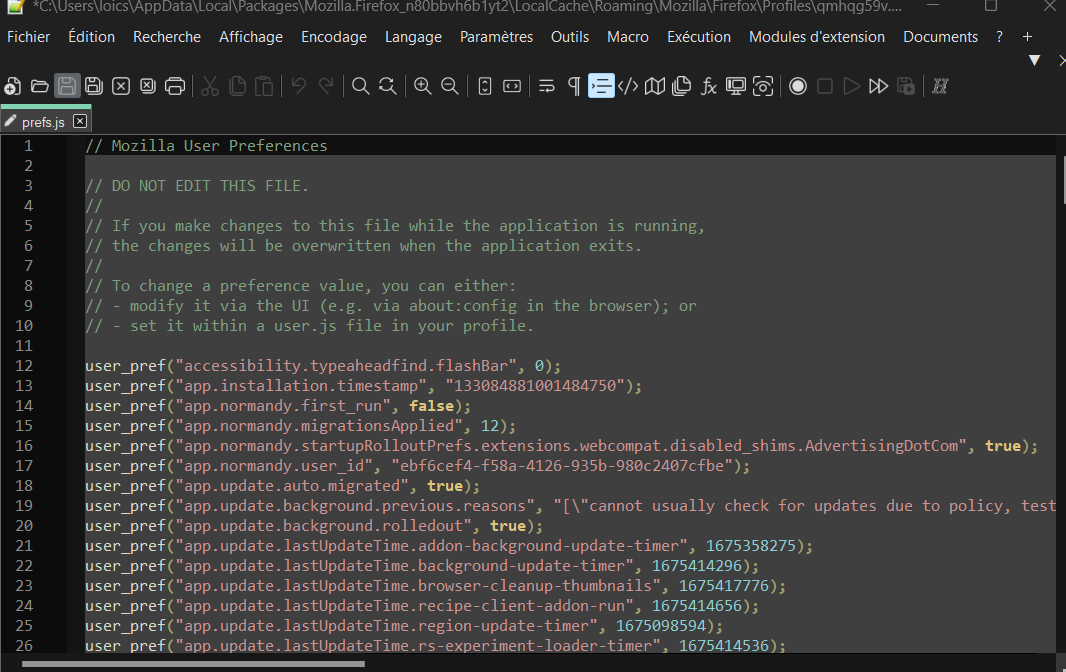


Figure 24 : edit with Notepad++ .

En L’ouvrant avec Notepad++ , on tombe sur de nombre ligne de code commençant par des commentaires qui sont visible en vert .



Les « // » transforme le texte en commentaire pour évité de chamboulé vos code que vous créer .

Figure 25 : Les code du fichier prefs.js .

On peut voir que le premier commentaire[[32]](#footnote-32) ci-dessus par des préférence de l’utilisateur Mozilla .

Et juste en dessous , le commentaire nous demande de pas édit le fichier car ça pourrais avoir des conséquence sur Mozilla .

Cependant , ça ne serait pas intéressant de filtrer que les processus de Firefox car en , il faut surtout exclure le process Name « Firefox.exe » pour montrer que les processus actifs qui réalise les opération d’écriture sur le fichier « prefs.js » afin de repérer si la modification de la page d’accueil de Firefox est effectuer par un ou plusieurs processus malveillants.

Donc , pour obtenir ces processus , nous devons réouvrir la fenêtres de filtrage des processus par la commande Ctrl + L ou par l’icone d’entonnoir .

Une fois ouvert , on double clique sur : Process Name | is | firefox.exe | Include

Une image contenant texte

Description générée automatiquement

Figure 26 : Filter et le filtre de firefox.exe .

On obtient ceci et il y aura plus qu’a mettre « Exclure » à la place de « Include » , pour cela nous avons cliqué sur le include pour ouvrir une petite liste déroulante pour avoir le Exclure ainsi cliqué dessus .



Figure 27 : L’action de Process Name Firefox.exe est passé en Exclure .

Ensuiste , nous cliquons sur le « add » pour ajouter l’entré modifié .



Figure 28 : L’entré modifier .

Maintenant modifier , nous pouvons ensuite rajouter et inclure l’entré de Notepad++ afin d’afficher les processus de ce dernier qui ont réaliser des options d’écriture sur le fichier « prefs.js »

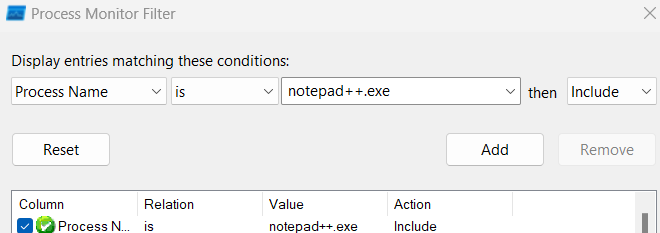


Figure 29 : L’ajoute de l’entrer NotePad++

Avant d’appliquer le filtre , nous devons réactiver la capture en temps réel des processus actif afin de captuer les processus de « Notepad++.exe » et dans Notepadd++ , on sauvegarde le fichier.js pour ensuite appliqué le filtre .

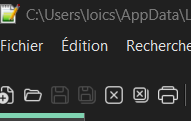


Figure 29 : Enregistrer le fichier .

Une fois faite , nous aurons trois processus de Notepad++ apparait dans Process Monitor .

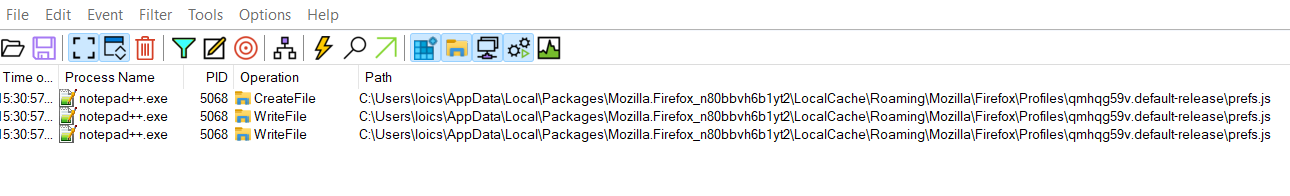


Figure 30 : Les processus de Notepad++.

On remarque que le premier processus de Notepadd++ à créer le fichier prefs.js dans le même chemin que le processus de Firefox Qu’on avait capture bien avant , puis le deuxième et troisième ont écrit dans le fichier prefs.js , les modifications qu’on a réalisées.

De plus , la colonne « Detail » , on remarque de nombreuses informations pouvant être intéressante afin ce que le processus à fait .

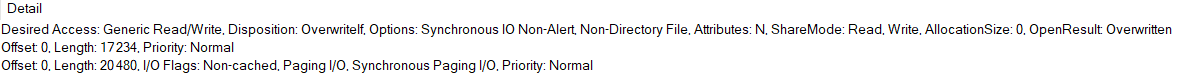


Figure 31 : Colonne Detail .

Le processus « CreateFile » de Notepad++ à eus la permission générique , de lire et écrire dans le fichier prefs.js sans avoir les droits administrateur car le chemin qui permet d’allez vers le fichier est modifiable par Notepadd++. Certain n’avait pas besoin des droits élevées pour pouvoir lire et écrire dans le répertoire « Roaming » d’où le nom « Generic Read/Write » sauf si un processus ayant des droits élevé sur le un des dossiers décide de bloqué la modification des fichiers .

Et chaque Détail « Disposition : OverwriteIf ; Options : Synchronous IO Non-Alert, Non-Directory File ; Attributes : N ; ShareMode : Read, Write ; AllocationSize : 0 ; OpenResult : Overwritten »

Cette procédure nous permet d’identifier quel autres processus que FireFox lui-même, ont modifier le fichier prefs.js sans que l’on ne le sache. Si l’on souhaite afficher tout les processus sans en spécifier un dans le filtre, il suffira de supprimer les entrées « Process Name » qui sont inclus dans le filtre.

### 3.2.2 CAS D’UTILISATION M.2 – EMPOISONNEMENT DNS :

L’empoisonnement DNS[[33]](#footnote-33) ou d’où sont autre nom « Usurpation de DNS » qu’est que c’est en général , et bien il consiste à entrer de fausses informations dans le cache DNS d’un poste afin que les requêtes DNS ne renvoient qu’une réponse incorrecte et que les utilisateurs ne soient dirgiés que vers de mauvais sites web pour les piéger .

Pour montrer ce type de cas , on va de nouveau utiliser process monitor plus le panneau de configuration ou Control Panel en anglais de découvrir le cas d’un empoissonnement DNS

Pour trouver le panneau de configuration puis ensuite de l’ouvrir , Il suffit de soit écrire dans la barre de recherche « panneau de configuration[[34]](#footnote-34) .

Une image contenant texte, capture d’écran, ordinateur, moniteur

Description générée automatiquement

Figure 32 : Recherche de control panel .

Ou de cliquer sur l’icone de windows et de cherche panneau de configuration , si vous ne le trouvez pas , fait la premier solution qui sera plus rapide .

Une image contenant texte

Description générée automatiquement

Figure 33 : Panneau de configuration .

Vous trouver cet fenêtres montré sur l’image si dessus . Une fois ouvert , il suffit de cliquer sur « Réseaux et Internet » ( en anglais « Network and internet » , puis « centre Réseaux et partage » en français ( en anglais « Network and sharing center » ) .

Une image contenant texte

Description générée automatiquement

Figure 34 : Centre Réseau et partage .

On tombera sur cette partage qui va être très important pour la suite .

Une image contenant texte

Description générée automatiquement

Figure 35 : Page de centre Réseau et partage .

On cliquera sur « modifier les paramètres de la carte » ( « change adapter setting » en anglais) afin d’accéder à la liste des cartes installés sur le poste .

Une image contenant texte

Description générée automatiquement

Figure 36 : Modifier les paramètres de la carte .

On peut voir qu’il y a actuellement deux cartes sont présente ( Il est possible d’avoir une troisième , pour ma part c’est l’Ethernet qui est présente) . Il y a la carte Bluetooh[[35]](#footnote-35) qui permet de connecter tout appareil à distance tel que des casque , manettes etc… et une carte Wi-Fi qui permet au poste utiliser de se connecter en Wi-Fi . ce poste est connecter à la Livebox-1EE9.

Une image contenant texte

Description générée automatiquement

Figure 37 : Carte du poste ( Wi-Fi , Bluetooth et Ethernet) .

Pour la suite , nous allons clique droit sur Wi-fi pour ensuite cliquer sur ses propriétés .

Une image contenant texte, capture d’écran, moniteur, ordinateur

Description générée automatiquement

Figure 38 : accès au propriété de Wi-Fi .

La fenêtre de propriété de Wi-Fi va s’ouvre et cherche « Internet Protocol Version 4 (TCP/IPv4) pour enfin faire un double clique dessus .

Une image contenant texte

Description générée automatiquement

Figure 39 : Propriété de Wi-Fi .

Une fois dans ses propriété , on coche « Utiliser l’adresse de serveur DNS suivante » ensuite on entre dans « Serveur DNS préféré » n’importe quel nombre tant qu’il ne dépasse pas 255 .



Figure 40 : Propriété de Protocole internet version 4

Il aura plus cas cliquer sur « OK » pour valider et on retourne sur process monitor . Il faut ouvrir de nouveau la fenêtre de filtrage que ce soit , en cliquant sur l’icone de filtre ou par la commande Ctrl+l . Quand la fenêtres est ouvert , on rajoute l’entrée : Opération | Is | RegSetValue| Include . ( Faites que vous n’avez que les process de cet entrée)

Une image contenant texte

Description générée automatiquement

Figure 41 : Filter RegSetValues



Figure 42 : L’entré RegSetValues est rajouté .

Quand l’entrée est rajouté , on applique le filtre avant d’ouvrir la fenêtre de recherche des processus en cliquant sur la loupe ou par la commande Ctrl + F .



Figure 43 : L’icone de recherche .

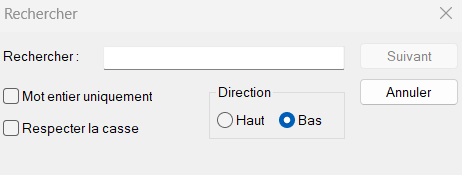


Figure 44 : Fenêtres de recherche .

La fenêtre de recherche s’ouvre , maintenant on doit renseigner les information donc dans le champ recherche , on doit inscrire « NameServer » et on coche « Bas » pour trouver le processus qui contient le mot NameServer » quelque part /

Après avoir cliquer sur suivant process monitor nous renvoie sur des

## 3.3 Virus Total :

Maintenant , nous allons nous pencher sur un outils de scan viral intégrer a process explorer : VirusTotal[[36]](#footnote-36) .

Ce dernier est un site accessible par tous par Firefox , Chrome etc… il appartient a google et ce dernier permet d’analyser tout fichier suspect en plus de facilité la détection rapide de cas ( Virus , Cheval de troie[[37]](#footnote-37) .) ainsi que de logiciel malveillant . Mais aussi VirusTotal est un outils intégré a process explorer ce qui nous sera bien utile .

Pour nous , nous allons créer notre propre code pour vérifier ou trouver un fichier en question .

Vous pouvez utiliser netbeans ou visualStudiocode pour créer votre python .



Figure 45 : fichier python

La premier chose a faire est de créer votre fichier python , pour visualstudiocode il suffit de faire créer un fichier puis a la fin du nom mettre « .py » ce qui le considéra comme un fichier python .

Un fois créer , nous pouvons commencer a écrire le code de ce fichier .

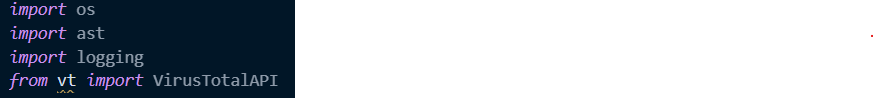


Figure 46 : Import

Les premier code que nous insérons dans le fichier est la commande import qui permet d’importé « os , ast et logging » .

Puis from qui est le pour la valeur vt , on importe VirusTotalAPI .

1. <https://fr.wikipedia.org/wiki/Entreprise_de_services_du_num%C3%A9rique>

   <https://www.passion-entrepreneur.com/679-esn.html>

   <https://www.monconseillerdentreprise.fr/quest-ce-quune-esn/> [↑](#footnote-ref-1)
2. <https://blog.advancia-itsystem.com/pourquoi-les-antivirus-ne-sont-plus-suffisants/#.Y86xFq2ZO3A> [↑](#footnote-ref-2)
3. <https://fr.wikipedia.org/wiki/Mark_Russinovich> [↑](#footnote-ref-3)
4. <https://learn.microsoft.com/en-us/sysinternals/downloads/process-explorer> [↑](#footnote-ref-4)
5. <https://www.malekal.com/process-explorer-gestionnaire-taches-avance/> [↑](#footnote-ref-5)
6. <https://fr.wikipedia.org/wiki/Processeur> [↑](#footnote-ref-6)
7. <https://www.inmac-wstore.com/guides-achat-composants-qu-est-ce-que-gpu/cp37537.htm> [↑](#footnote-ref-7)
8. <https://fr.wikipedia.org/wiki/R%C3%A9gulateur_PID> [↑](#footnote-ref-8)
9. <https://fr.wikipedia.org/wiki/Processus_(informatique)> [↑](#footnote-ref-9)
10. <https://www.lemagit.fr/definition/memoire-morte-ROM-Read-Only-Memory> [↑](#footnote-ref-10)
11. <https://fr.wikipedia.org/wiki/M%C3%A9moire_de_masse> [↑](#footnote-ref-11)
12. <https://www.heflo.com/fr/blog/bpm/cycle-de-vie-d-un-processus/>

    <https://www.researchgate.net/figure/Cycle-de-vie-du-processus_fig3_269969205> [↑](#footnote-ref-12)
13. <https://www.ibm.com/docs/fr/urbancode-deploy/6.2.2?topic=processes-overview-application> [↑](#footnote-ref-13)
14. <https://www.softfluent.fr/blog/architecture-logicielle-pour-application/> [↑](#footnote-ref-14)
15. <https://fr.wikipedia.org/wiki/Thread_(informatique)> [↑](#footnote-ref-15)
16. <https://learn.microsoft.com/fr-fr/windows-hardware/drivers/gettingstarted/user-mode-and-kernel-mode> [↑](#footnote-ref-16)
17. <https://fr.wikipedia.org/wiki/VirusTotal>

    [↑](#footnote-ref-17)
18. <https://fr.wikipedia.org/wiki/Signature_de_code> [↑](#footnote-ref-18)
19. <https://fr.wikipedia.org/wiki/M%C3%A9moire_vive> [↑](#footnote-ref-19)
20. <https://www.crucial.fr/support/articles-faq-memory/virtual-memory-settings-suggestions> [↑](#footnote-ref-20)
21. <https://fr.wikipedia.org/wiki/M%C3%A9moire_physique> [↑](#footnote-ref-21)
22. <https://learn.microsoft.com/en-us/sysinternals/downloads/procmon> [↑](#footnote-ref-22)
23. <https://support.microsoft.com/fr-fr/office/mise-en-forme-d-un-champ-de-texte-a5e5bcde-85da-4c7a-8164-1fe286636668> [↑](#footnote-ref-23)
24. <https://fr.wikipedia.org/wiki/Bool%C3%A9en> [↑](#footnote-ref-24)
25. <https://learn.microsoft.com/fr-fr/dotnet/api/system.diagnostics.process.processname?view=net-7.0> [↑](#footnote-ref-25)
26. Prefs : C’est le mots préférence en abrégé . [↑](#footnote-ref-26)
27. <https://www.quirksmode.org/js/events_properties.html> [↑](#footnote-ref-27)
28. <https://www.cerfi.ch/fr/Actualites/12-raccourcis-indispensables-dans-Word.html> [↑](#footnote-ref-28)
29. <http://www.cs.rpi.edu/courses/fall01/os/CreateFile.html> [↑](#footnote-ref-29)
30. Jump to : « sauter à » en français . [↑](#footnote-ref-30)
31. <https://fr.wikipedia.org/wiki/Notepad%2B%2B> [↑](#footnote-ref-31)
32. <https://www.larousse.fr/dictionnaires/francais/commentaire/17480> [↑](#footnote-ref-32)
33. <https://www.cloudflare.com/fr-fr/learning/dns/dns-cache-poisoning/> [↑](#footnote-ref-33)
34. <https://support.microsoft.com/fr-fr/windows/ouvrir-le-panneau-de-configuration-dans-windows-e8d6e3d8-4743-422c-7cf8-0b41f8f079a1> [↑](#footnote-ref-34)
35. <https://fr.wikipedia.org/wiki/Bluetooth> [↑](#footnote-ref-35)
36. <https://www.virustotal.com/gui/home/upload> [↑](#footnote-ref-36)
37. <https://www.kaspersky.fr/resource-center/threats/trojans> [↑](#footnote-ref-37)