WINDOWS MALWARE HUNTER HANDBOOK
Concepts et implémentations

PAGE DE SERVICE

Référence : n/a
Plan de classement : cybersecurity|malware|sysinternals
Niveau de confidentialité : publique

Mises à jour

Version	Date	Auteur	Description du changement
1.0.0	21/01/2023	Delettre Théo	Création
1.1.0	22/01/2023	Delettre Théo	Rappel du contexte
1.2.0	22/01/2023	Delettre Théo	Objectifs
1.3.0	23/01/2023	Delettre Théo	DETECTION DE MALWARE SOUS WINDOWS
1.4.0	29/01/2023	Delettre Théo	CAS D'UTILISATION N°2 – DNS EMPOISONNE
1.5.0	20/02/2023	Delettre Théo	VirusTotal

Validation

Version	Date	Nom	Rôle
1.4.0	29/01/2023	VALENTI Jérôme	
1.5.0	20/02/2023	VALENTI Jérôme	

Diffusion

Version	Date	Nom	Rôle

SOMMAIRE

Page de service 1

Sommaire 2

1 Rappel du contexte 3

2 Objectifs 3

3 Détection de malware sous Windows 3

3.1 Process Explorer 4

3.1.1 Surveillance des processus 4

3.1.2 Observation de la mémoire 7

3.1.3 Voir les ressources d'un processus 8

3.2 Process Monitor 9

3.2.1 CAS D'UTILISATION N°1 – HOME PAGE FIREFOX 9

3.2.2 CAS D'UTILISATION N°2 – DNS EMPOISONNE 12

3.3 VirusTotal 15

4 Table des illustrations 17

1 Rappel du contexte

NetWorking Solutions Inc. (NSI) est une Entreprise de Services du Numérique (ESN[1])
Network Solutions est l'un des principaux fournisseurs de services de nom de domaine et d'hébergement Web aux États-Unis. Elle a été l'un des premiers fournisseurs de services de nom de domaine aux États-Unis lors de sa création en 1979. Depuis, elle a élargi ses services pour inclure l'hébergement Web, les certificats SSL, les services de messagerie électronique et les outils de création de sites Web.
En ce qui concerne l'enregistrement de noms de domaine, Network Solutions propose une variété de extensions de domaines, y compris les domaines de niveau supérieur les plus courants tels que .com, .net, .org, ainsi que des extensions de domaine spécifiques à des pays ou des industries. Les clients peuvent également transférer leurs noms de domaine existants vers Network Solutions pour bénéficier de ses services.
L'hébergement Web de Network Solutions propose des plans d'hébergement partagé, VPS et dédié pour répondre aux besoins des différents types de sites web. Les plans d'hébergement partagé sont adaptés aux petits sites web et aux blogs, tandis que les plans VPS et dédiés conviennent aux sites web plus importants et aux applications en ligne.
Network Solutions propose également des certificats SSL pour protéger les informations sensibles des visiteurs, tels que les informations de carte de crédit ou les informations personnelles.
En ce qui concerne les services de messagerie électronique, Network Solutions propose des comptes de messagerie professionnels avec des fonctionnalités telles que l'accès Web, la synchronisation des contacts et des calendriers, et une boîte de réception de grande capacité.
Enfin, les outils de création de sites Web de Network Solutions permettent aux utilisateurs de créer un site web professionnel rapidement et facilement, sans aucune connaissance en codage. Il existe une variété de modèles et de fonctionnalités disponibles pour les utilisateurs de choisir, et les utilisateurs peuvent également utiliser leur propre nom de domaine pour leur site web.

60 % des cyberattaques exploitent des vulnérabilités logicielles connues, 40 % exploitent des identifiants volés, indique le rapport X-Force Threat Intelligence Index 2022 de IBM[2].

2 Objectifs

La détection de virus est un domaine crucial pour la sécurité informatique. Avec l'augmentation constante des menaces en ligne, il est de plus en plus important de se protéger contre les virus, les logiciels malveillants et les attaques de pirates.
Les anti-virus sont souvent utilisés pour détecter et éliminer les menaces, mais il est important de comprendre que ces logiciels ne sont pas infaillibles et qu'il existe des méthodes de détection autre que la signature de virus.
Ce document vous offrira une vue d'ensemble des différentes méthodes de détection de virus et des outils disponibles pour protéger efficacement votre ordinateur contre les menaces.

3 Detection de malware sous Windows

Avant de commencer la détection de virus, il est important de comprendre comment le système d'exploitation fonctionne pour comprendre comment les virus l'affectent et par quels moyens.

Les principales fonctionnalités d'un système d'exploitation Windows incluent :

La gestion des processus : cela permet aux utilisateurs de lancer et de gérer des programmes sur l'ordinateur. Le système d'exploitation alloue les ressources nécessaires à chaque processus et gère les conflits éventuels.

La gestion de la mémoire : cela permet aux programmes de stocker et d'accéder à des données dans la mémoire vive de l'ordinateur. Le système d'exploitation utilise également la mémoire pour stocker des informations temporaires.

[1] https://fr.wikipedia.org/wiki/Entreprise_de_services_du_num%C3%A9rique
[2] https://www.ibm.com/reports/threat-intelligence/

La gestion des entrées/sorties : cela permet aux programmes de communiquer avec les périphériques connectés à l'ordinateur, comme les claviers, les souris, les écrans, les disques durs, etc.

La gestion de fichiers : cela permet aux utilisateurs de stocker, de récupérer et de gérer des fichiers sur l'ordinateur. Le système d'exploitation gère également les autorisations d'accès aux fichiers pour maintenir la sécurité.

La gestion de la sécurité : cela permet de protéger les données et les ressources de l'ordinateur contre les accès non autorisés. Cela inclut les mécanismes de sécurité tels que les mots de passe, les autorisations d'accès, et les logiciels de sécurité.

Il existe une suite de logiciels puissants fournie par Microsoft. Cette suite complète s'appelle Sysinternals[3] Suite. Elle est téléchargeable ici : https://learn.microsoft.com/fr-fr/sysinternals/downloads/sysinternals-suite

La gestion, le dépannage et le diagnostique des systèmes et programmes Windows est aidée par la suite Sysinternals, créée par Mark Russinovich[4].

3.1 Process Explorer

Process Explorer est un gestionnaire de tache beaucoup plus détaillé que celui par défaut sous Windows.
Process Explorer affiche les processus en cours d'exécution sous forme d'arbre, où chaque processus est représenté par un nœud. Les processus enfants sont regroupés sous les processus parent. Cela permet aux utilisateurs de visualiser les relations de dépendance entre les processus et de mieux comprendre comment ils interagissent entre eux.

Process Explorer affiche également des informations détaillées sur chaque processus, telles que :

- Les informations de base, comme le nom du processus, l'ID de processus, l'utilisateur qui l'a lancé, l'utilisation de la mémoire, les ressources système utilisées, etc.
- Les détails sur les threads et les modules chargés,
- Les informations sur les propriétés du processus, comme les informations de version, les informations de sécurité, les informations sur les dépendances, etc.

Process Explorer permet également aux utilisateurs de :

- Terminer un processus,
- Rechercher des informations sur un processus spécifique,
- Afficher les propriétés d'un processus,
- Afficher les modules chargés par un processus,
- Afficher les threads d'un processus,
- Afficher les informations sur les handles ouverts par un processus,
- Afficher les informations sur les pages de mémoire utilisées par un processus,
- Afficher les informations sur les ressources réseau utilisées par un processus,

3.1.1 Surveillance des processus

Un processus[5] informatique est une instance d'un programme en cours d'exécution sur un ordinateur. Il représente une tâche ou une activité qui est effectuée par le système d'exploitation pour accomplir une certaine fonction. Les processus informatiques sont gérés par le système d'exploitation, qui alloue les ressources nécessaires, comme la mémoire et les processeurs, pour les exécuter.

[3] https://learn.microsoft.com/fr-fr/sysinternals/
[4] https://en.wikipedia.org/wiki/Mark_Russinovich
[5] https://fr.wikipedia.org/wiki/Processus_(informatique)

Un processus informatique peut être composé de plusieurs threads, qui sont des sous-tâches qui peuvent être exécutées de manière indépendante les unes des autres. Les processus informatiques peuvent également interagir entre eux, en partageant des ressources ou en communiquant entre eux.

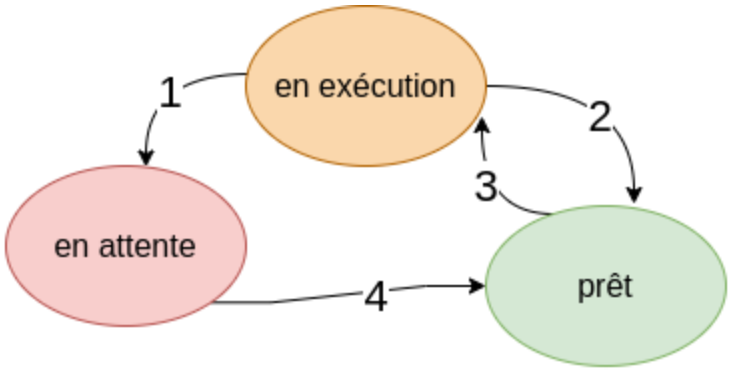

Figure 1 : schéma simplifié du cycle de vie d'un processus[6]

1. Le processus se met en attente d'un évènement
2. L'ordonnanceur passe la main à un autre processus
3. L'ordonnanceur choisit ce processus
4. L'événement attendu se produit

Les processus informatiques sont créés lorsqu'un utilisateur lance un programme ou lorsqu'un autre processus en crée un nouveau. Le système d'exploitation gère la mémoire et les ressources allouées à chaque processus, et peut également interrompre un processus pour allouer des ressources à un autre processus plus important.

Les programmes utilisateurs (applications) sont le plus souvent constitués d'une multitude de processus. Le nombre de programmes (et leurs failles potentielles) définit la surface d'attaque d'un ordinateur, d'une machine.

La colonne Context Switches indique le nombre de fois qu'un processus (ou thread) a été exécuté depuis l'ouverture de Process Explorer.
CSwitch Delta indique le nombre de fois qu'un processus s'est lancé sur un temps donné.

Un processus possède toujours au moins un fil d'exécution mais il peut y en avoir plusieurs

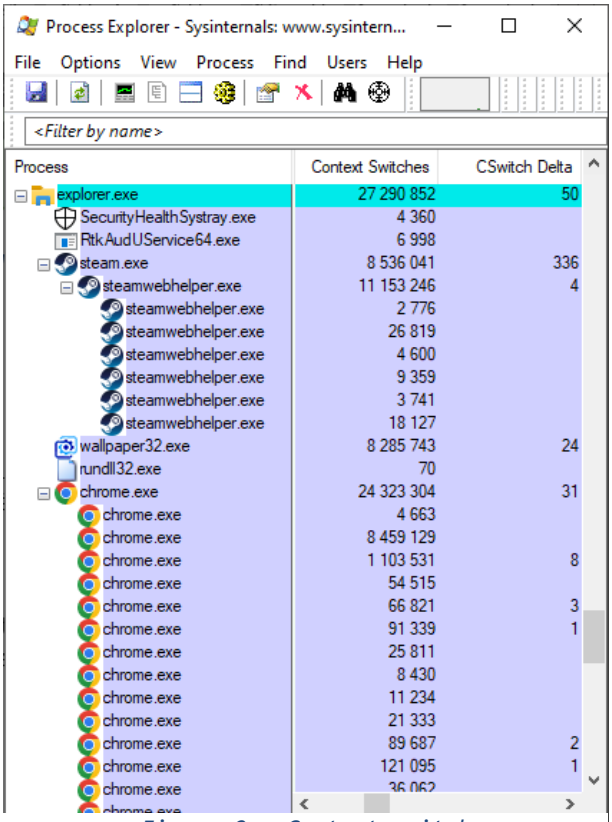

Figure 2 : Context switch

[6] https://www.lecluse.fr/nsi/NSI_T/archi/process/

suivant la programmation de celui-ci. Ces "sous-processus" sont des threads[7] (fils d'exécution).

En faisant un clic-droit sur un processus, propriétés puis l'onglet Threads, on observe que la priorité[8] de base de ce processus est à 8.

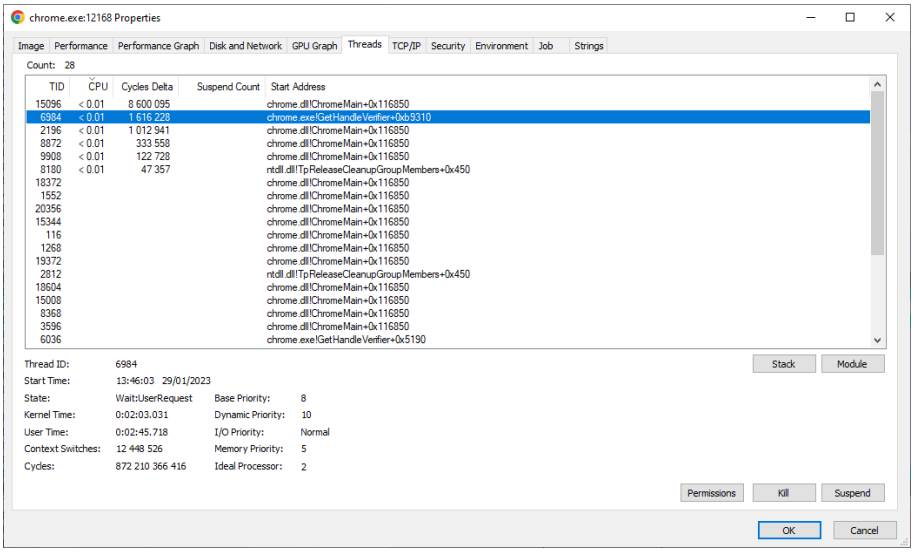

Figure 3 : Propriétés d'un processus

Le niveau de priorité varie entre 0 (basse priorité) et 31 (haute priorité). Il définit en partie à quelle fréquence ce processus est exécuté par rapport aux autres. Un processus système aura une priorité élevée par rapport à un processus d'un programme utilisateur comme un jeu vidéo.

Pour afficher plus de données en "vue globale", il est possible d'ajouter des colonnes. Il faut clic-droit sur les colonnes puis Select Columns…

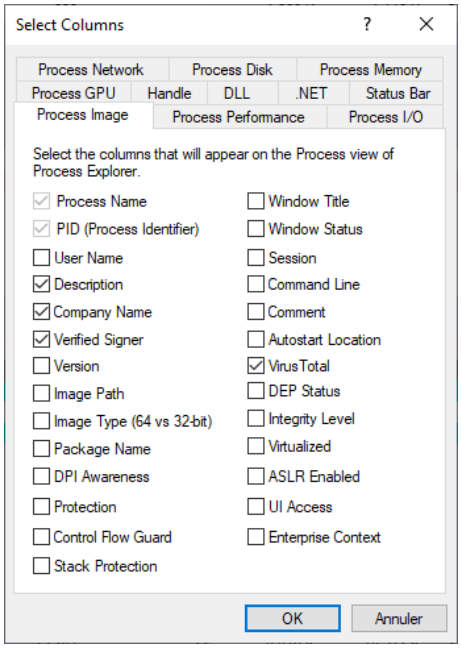

Figure 4 : configuration des données affichées par Process Explorer

[7] https://en.wikipedia.org/wiki/Thread_(computing)
[8] https://learn.microsoft.com/en-us/windows/win32/procthread/scheduling-priorities

Ici on choisit d'ajouter les colonnes Verified Signer et Virus Total pour correspondre à notre utilisation.

Les différents processus sont affichés en deux parties :

- Les processus exécutés au niveau kernel (noyau) (partie rose)
- Les processus exécutés au niveau utilisateur (partie en bleu sous les processus winlogon.exe et explorer.exe)

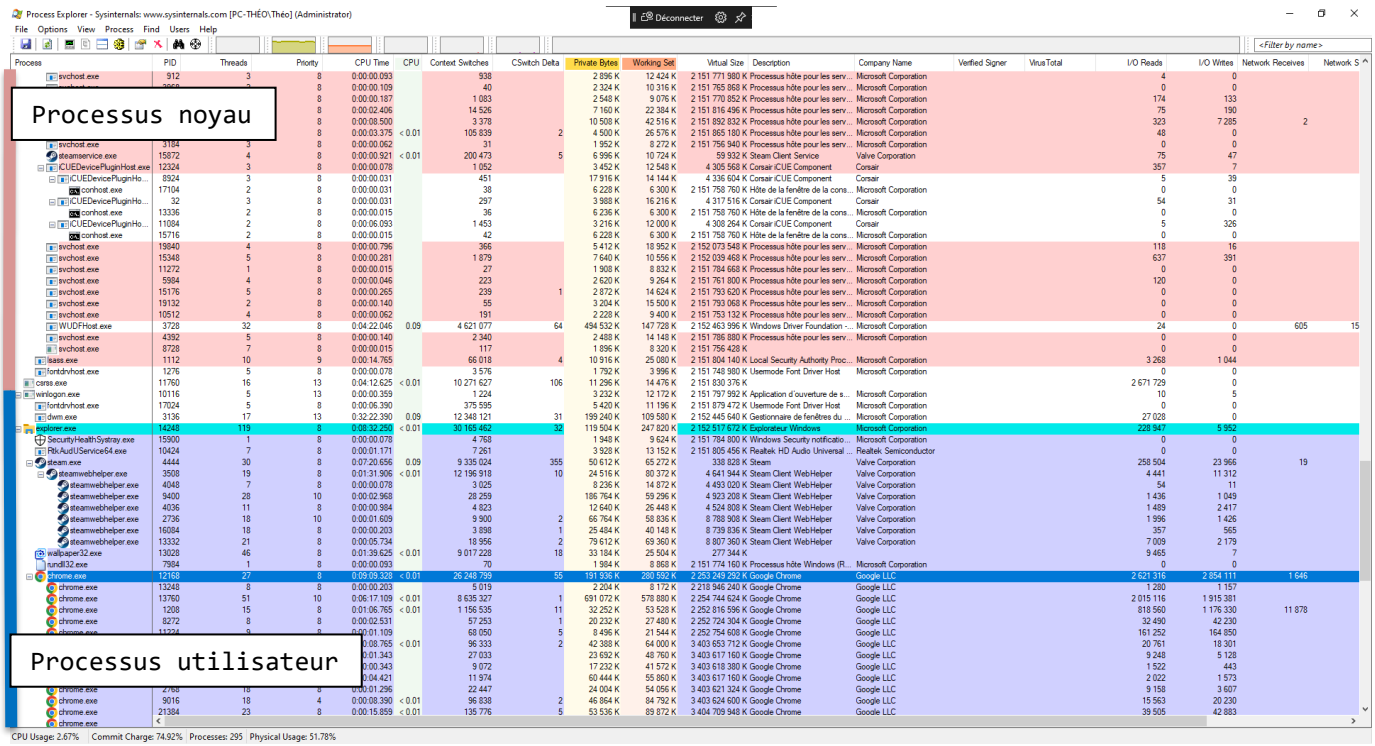

Figure 5 : Process Explorer - vue d'ensemble

3.1.2 Observation de la memoire

La mémoire sous Windows, comme dans tous les systèmes d'exploitation modernes, à plusieurs formes :

- Private Bytes : quantité de mémoire demandée par les fils d'éxécution
- Working Set : mémoire vive totale utilisée par un processus
- Virtual Size : mémoire vive virtuelle adressable

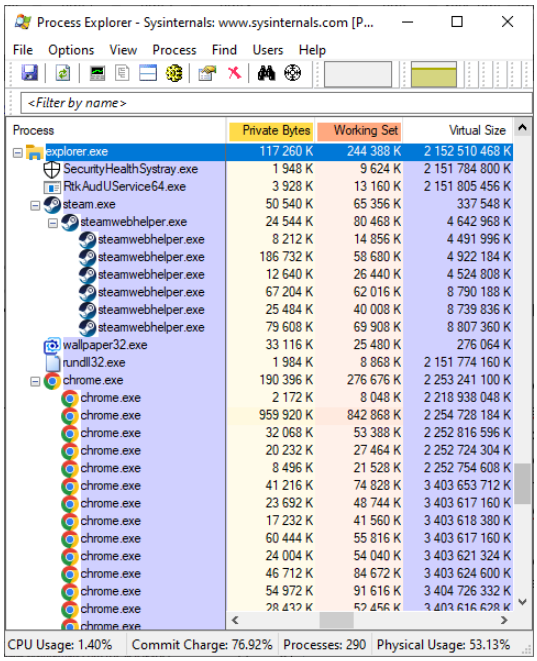

Figure 6 : Process Explorer - types de mémoires

3.1.3 Voir les ressources d'un processus

Maintenant que l'on sait les bases de fonctionnement des processus et threads, nous verrons le concept de handles apposés sur les différentes ressources mobilisées par ceux-ci.

Les handles (poignées) d'un processus sont des références utilisées par le système d'exploitation pour accéder aux ressources utilisées par un processus. Les ressources peuvent inclure des fichiers, des sections mémoire, des sockets réseau, des objets de la base de registre, entre autres. Chaque handle est identifié par un numéro unique attribué par le système d'exploitation, appelé numéro de handle.

Les handles sont utilisés pour permettre aux processus de partager des ressources de manière sécurisée, en donnant un accès limité à des ressources spécifiques plutôt que de donner un accès complet à toutes les ressources d'un système. Les handles peuvent également être utilisés pour permettre aux processus de communiquer entre eux, en donnant accès à des ressources partagées.

Les handles sont créés et gérés par le système d'exploitation, et chaque processus a accès à une liste de tous les handles qu'il a créés ou auxquels il a accès. Les handles peuvent être fermés explicitement par un processus ou automatiquement lorsque le processus se termine.

Un fichier verrouillé par handle est un fichier qui est en cours d'utilisation par un processus et pour lequel l'accès est limité ou empêché pour les autres processus. Cela signifie qu'un autre processus ne peut pas lire, écrire ou supprimer le fichier tant qu'il est verrouillé.

Le système d'exploitation utilise des handles pour verrouiller les fichiers. Lorsqu'un processus ouvre un fichier, le système d'exploitation lui attribue un handle unique qui est utilisé pour accéder au fichier. Ce handle est utilisé pour verrouiller le fichier et empêcher les autres processus d'y accéder.

Un fichier peut être verrouillé pour différentes raisons, par exemple pour éviter les conflits d'accès lorsqu'un processus lit ou écrit dans le fichier, pour empêcher la suppression d'un fichier en cours d'utilisation ou pour protéger le contenu d'un fichier contre des modifications non autorisées.

3.2 Process Monitor

Process Monitor est un utilitaire de surveillance de processus développé par Microsoft, également connu sous le nom de Procmon. Il permet de surveiller en temps réel les activités des processus sur un système Windows. Il peut être utilisé pour surveiller les accès aux fichiers, les registres, les réseaux, les processus et les services.

Avec Process Monitor, vous pouvez enregistrer les activités des processus et les afficher dans un format facile à lire. Il peut également filtrer les résultats en fonction de divers critères, tels que le nom du processus, le nom du fichier ou le type d'accès.

Il est particulièrement utile pour les administrateurs système, les développeurs et les utilisateurs avancés pour surveiller les activités des processus, identifier les problèmes et résoudre les erreurs. Il peut également aider à identifier les logiciels malveillants et les programmes indésirables.

Fonctionnement :
Dès que la capture est activée, tous les événements sont capturés puis affichés suivant les différents filtres appliqués. Il est très important de savoir choisir les bons filtres suivant les éléments recherchés : si le filtre est trop restrictif on risque de ne pas trouver l'événement, si trop large on se retrouve avec des centaines de milliers d'événements.

3.2.1 CAS D'UTILISATION N°1 – HOME PAGE FIREFOX

L'helpdesk niv.1 du client Vinci escalade plusieurs tickets vers vous. Ces tickets signalent tous la modification, sans intervention de l'utilisateur, de la page par défaut du navigateur Firefox. Pire, il apparait que cette page par défaut est une page de phishing qui imite quasi parfaitement la page de connexion de l'extranet Vinci (cf. copie d'écran ci-dessous).

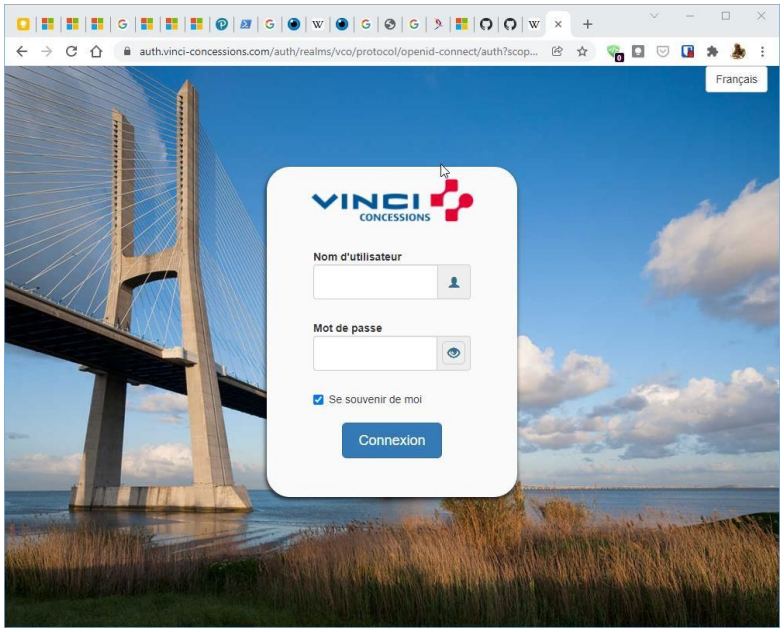

Figure 7 : page d'hameçonnage reproduisant le portail de connexion Vinci officiel

Pour détecter la modification de la page par défaut de Firefox nous allons utiliser Process Monitor.

A l'ouverture du programme, la capture est déjà active, cela ralenti l'ordinateur car des milliers d'événements sont affichés et aucun filtre n'est appliqué.

Mettre en pause la capture :

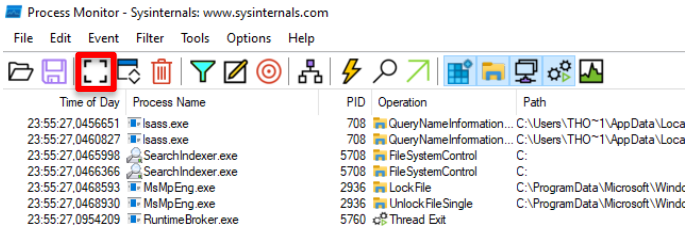

Figure 8 : Process Monitor - Pause capture événements

Vider l'historique d'événement :

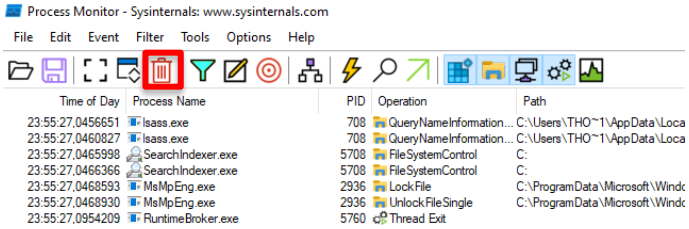

Figure 9 : Process Monitor - Vider historique d'événements

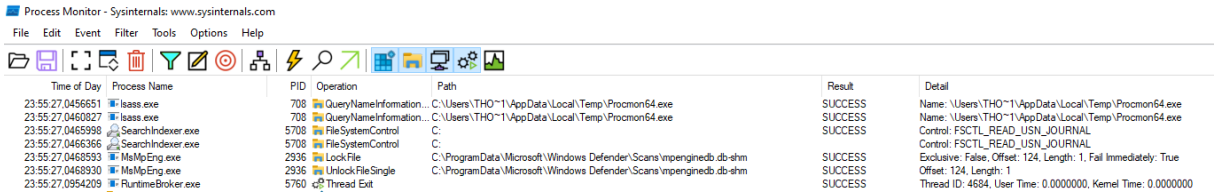

Figure 10 : Process Monitor - Colonnes par défaut

Avant de continuer, voici une description des différentes colonnes par défaut :

- Time of Day : horodatage de l'événement capturé
- Process Name : Nom du processus capturé
- PID : Identifiant unique du processus
- Operation : Type d'opération effectué par le processus
- Path : Chemin complet de la ressource modifiée / lue
- Result : Résultat de l'opération réalisé par le processus
- Detail : Details concernant la ressource accédée par le processus

Nous pouvons maintenant appliquer les différents filtres requis pour la capture.

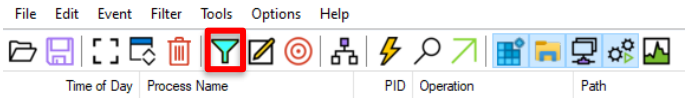

Figure 11 : Process Monitor - Boutons d'actions

Il nous faut trouver le fichier contenant l'adresse de la page par défaut de Firefox.
Nous pouvons créer les filtres suivants :

Ne trouvant pas le fichier de configuration, je modifie un des filtres (Path contains) pour qu'il soit plus permissif.

Process Name	IS	firefox.exe	Include
Category	IS	WRITE	Include
Path	Contains	prefs.js	Include

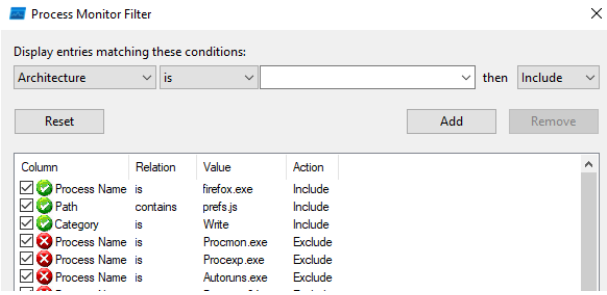

Figure 12 : Process Monitor - Filtres

Après avoir lancé la capture et modifié la page par défaut, nous obtenons cet événement :

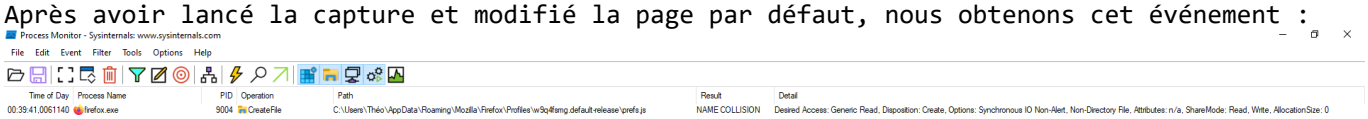

Figure 13 : Process Monitor - Capture modif. page par défaut

Nous savons maintenant le chemin exact du fichier de configuration contenant l'adresse de la page par défaut. Il faut maintenant vérifier que c'est bien ce fichier qui nous intéresse. Pour cela, clic-droit dessus puis Jump-to.

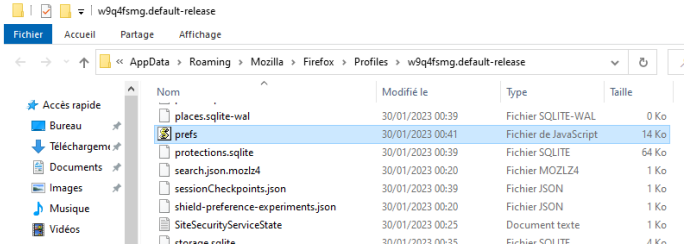

Figure 14 : Répertoire du fichier de configuration

Le fichier est ouvert avec un éditeur de texte pour en afficher le contenu, la page par défaut à été réglée sur l'adresse https://www.google.fr, on y retrouve bien cette adresse.

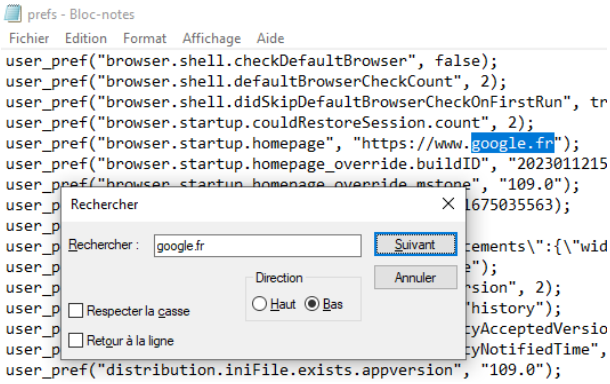

Figure 15 : Contenu du fichier prefs.js

On peut confirmer que ce fichier contient l'adresse de la page par défaut.
Maintenant, pour détecter la modification de la page par défaut par un programme malveillant, il suffit de modifier un des filtres comme suit :

Process Name	IS	firefox.exe	Exclude
Category	IS	WRITE	Include
Path	IS	C:\Users\Théo\AppData\Roaming\Mozilla\Firefox\Profiles\w9q4fsmg.default-release\prefs.js	Include

Le premier filtre permet d'exclure Firefox de la recherche et le dernier est le chemin exact du fichier de configuration.

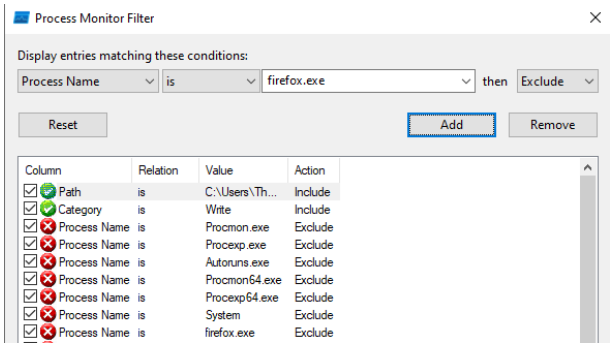

Figure 16 : Process Monitor - Filtres

Process Monitor va maintenant capturer toutes les écritures sur le fichier prefs.js, exemptés celles du processus firefox.exe.

Ici, la page par défaut à été modifiée en utilisant le bloc-note.
La page par défaut est maintenant https://www.youtube.com/.
Process Monitor à capturé l'événement de modification.

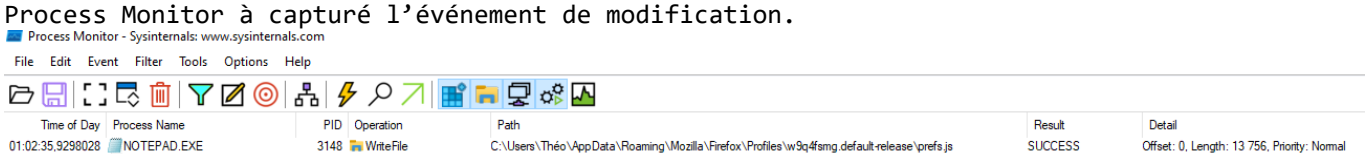

Figure 17 : Process Monitor - Capture prefs.js

En ouvrant Firefox, la nouvelle page par défaut se charge, donc YouTube.

Figure 18 : Nouvelle page par défaut

3.2.2 CAS D'UTILISATION N°2 – DNS EMPOISONNE

L'empoisonnement de DNS (Domain Name System) est une technique utilisée pour rediriger les requêtes DNS vers des serveurs malveillants. Cela permet aux attaquants de rediriger les utilisateurs vers des sites Web malveillants ou d'autres types de contenu malveillant lorsqu'ils tentent de visiter des sites légitimes.

Process Monitor est toujours utilisé dans ce cas.
Pour commencer, les filtres suivants sont appliqués pour trouver la ressource contenant les IP des serveurs DNS.

Process Name	IS	svchost.exe	Include
Category	IS	WRITE	Include
Details	Contains	1.1.1.1	Include

Le filtre "Details contains 1.1.1.1 include" permet de capturer les événements dont les détails contiennent l'IP 1.1.1.1 qui sera réglée dans le panneau de configuration. Ensuite nous obtiendrons le chemin exact de la ressource modifiée. A partir de là, nous pourrons détecter toute modification effectuée sur la ressource et trouver le programme malveillant.

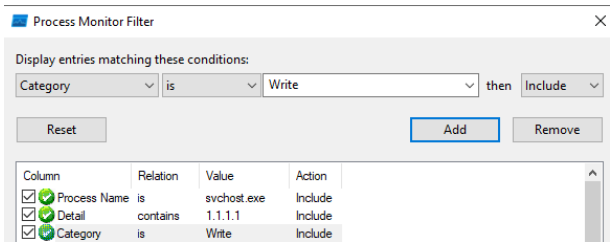

Figure 19 : Process Monitor - Filtres

Après avoir modifié l'IP du DNS en 1.1.1.1 dans les propriétés de la connexion réseau rien ne s'affiche dans les résultats de capture, je désactive donc deux filtres, les filtres suivants sont appliqués :

Details	Contains	1.1.1.1	Include

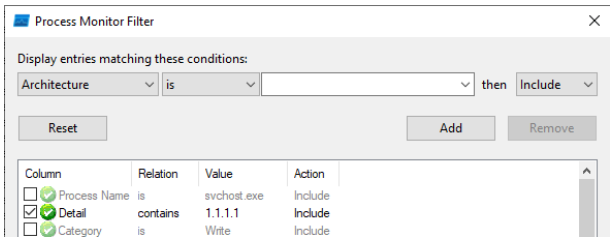

Figure 20 : Process Monitor - Filtres

Avec ces nouveaux filtres nous obtenons les résultats suivants :

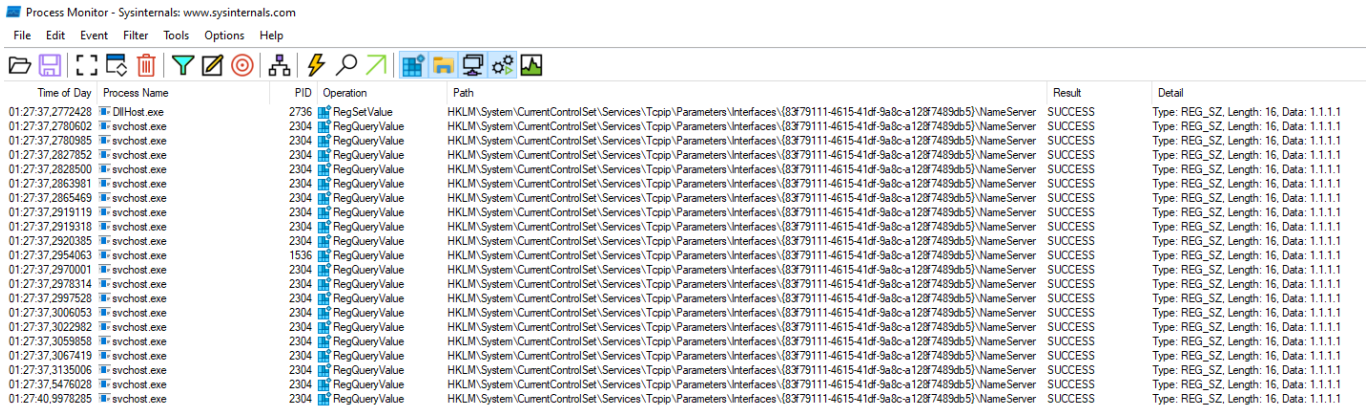

Figure 21 : Process Monitor - Résultats

Dans ces événements, celui qui nous intéresse est la première opération qui est une écriture sur le registre.
Nous avons maintenant le chemin exact de la clé registre contenant les IP des serveurs DNS.
Pour en observer le contenu, faire un clic-droit dessus puis Jump To.
L'éditeur de registre s'ouvre à l'emplacement de la clé.

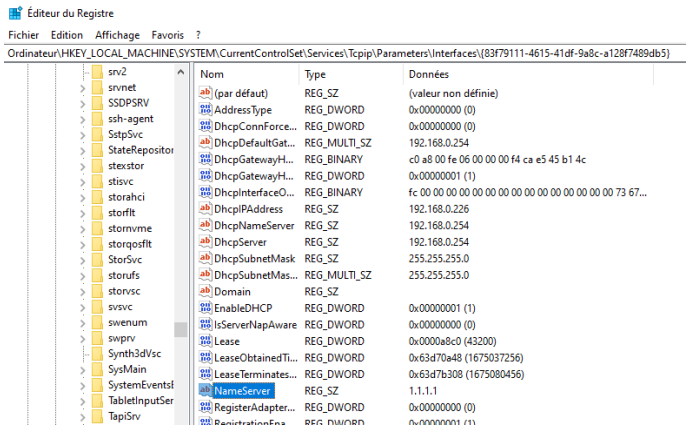

Figure 22 : Editeur de registre

Enfin, double clic sur la clé NameServer.

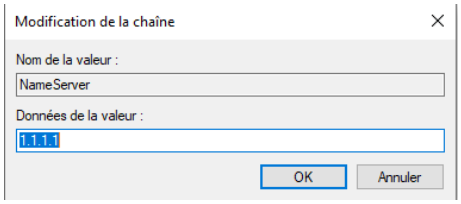

Figure 23 : Modification clé registre

Pour tester le fonctionnement, on remplace 1.1.1.1 par 8.8.8.8 (DNS de google).

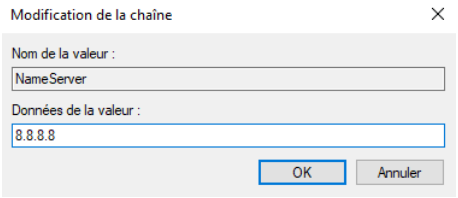

Figure 24 : Modification clé registre en 8.8.8.8

En réouvrant les propriétés IP de la connexion réseau on constate que le DNS est maintenant sur 8.8.8.8.

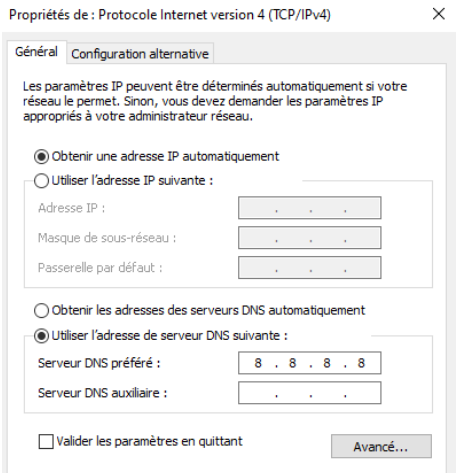

Figure 25 : Propriétés IP de la connexion

On peut confirmer que la clé registre NameServer contient les IP des serveurs DNS. Voici le chemin de la clé :
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{83f79111-4615-41df-9a8c-a128f7489db5}\NameServer

Maintenant que nous avons le chemin exact, nous pouvons lancer la détection de modifications malveillantes.

Les filtres sont modifiés pour être plus permissifs :

Process Name	IS	svchost.exe	Exclude
Path	IS	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{83f79111-4615-41df-9a8c-a128f7489db5}\NameServer	Include

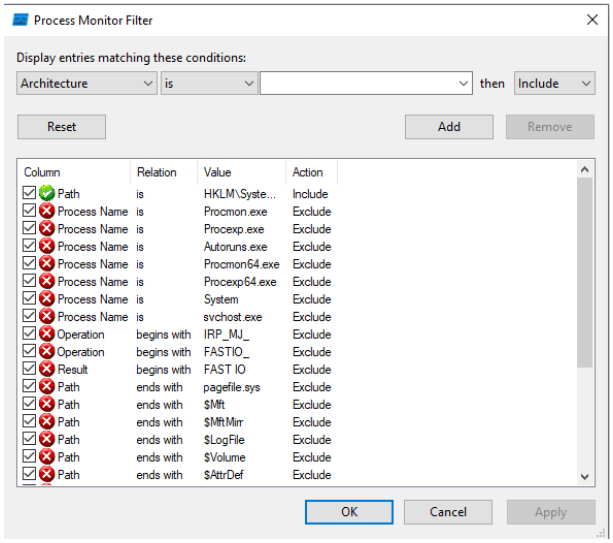

Figure 26 : Process Monitor - Filtres pour capture modif. clé NameServer

Ces filtres afficheront les événements concernant la clé NameServer en excluant le processus svchost.exe.

3.3 VIRUSTOTAL

VirusTotal est un service en ligne gratuit qui permet d'analyser des fichiers et des URL à la recherche de virus, de logiciels malveillants et d'autres menaces de sécurité. Fondé en 2004, VirusTotal est actuellement détenu par Google.

Le service permet aux utilisateurs de soumettre des fichiers ou des URL suspects pour une analyse de sécurité complète. VirusTotal utilise plus de 70 antivirus différents et d'autres outils de détection pour analyser les fichiers soumis. Les résultats de l'analyse sont ensuite présentés sous forme de rapports détaillés qui indiquent si le fichier ou l'URL est considéré comme malveillant par les différents moteurs d'analyse utilisés.

En plus de l'analyse de fichiers et d'URL, VirusTotal propose également une API (interface de programmation d'application) qui permet aux développeurs d'intégrer l'analyse de sécurité dans leurs propres applications et systèmes. Cette fonctionnalité permet aux développeurs de détecter rapidement les menaces potentielles et d'ajouter des fonctionnalités de sécurité à leurs applications.

Rappel :
Une API, ou Interface de Programmation d'Application (en anglais Application Programming Interface), est un ensemble de règles et de protocoles qui permettent à différentes applications ou services informatiques de communiquer entre eux.
L'API définit les types de requêtes et de réponses possibles entre les différentes applications, ainsi que les formats de données acceptés et les protocoles de communication à utiliser.

A partir de l'API fournie par VirusTotal nous pouvons donc réaliser un antivirus autonome, dans ce cas si, le moteur antivirus est un script python, ce script accède aux différentes ressources dont il a besoin : fichier de configuration contenant les chemins de répertoires/fichiers à analyser, API de VirusTotal, librairies Python supplémentaires…

Le script est divisé en 6 parties principales :

- Lecture du fichier de configuration (virus-hunter.cfg)
- Parcours des répertoires à scanner
- Scan de chaque fichier
- Traitement réponse API
- Traitement des alarmes
- Fin de traitement, envoi d'un récapitulatif par une API SMS

L'utilisation de l'API de VirusTotal est gratuite, il faut simplement s'inscrire sur le site officiel pour recevoir une clé API, celle-ci est unique et permet une identification de l'émetteur des requêtes.

4 TABLE DES ILLUSTRATIONS

Figure 1 : schéma simplifié du cycle de vie d'un processus 5
Figure 2 : Context switch 5
Figure 3 : Propriétés d'un processus 6
Figure 4 : configuration des données affichées par Process Explorer 6
Figure 5 : Process Explorer - vue d'ensemble 7
Figure 6 : Process Explorer - types de mémoires 8
Figure 7 : page d'hameçonnage reproduisant le portail de connexion Vinci officiel 9
Figure 8 : Process Monitor - Pause capture événements 10
Figure 9 : Process Monitor - Vider historique d'événements 10
Figure 10 : Process Monitor - Colonnes par défaut 10
Figure 11 : Process Monitor - Boutons d'actions 10
Figure 12 : Process Monitor - Filtres 11
Figure 13 : Process Monitor - Capture modif. page par défaut 11
Figure 14 : Répertoire du fichier de configuration 11
Figure 15 : Contenu du fichier prefs.js 11
Figure 16 : Process Monitor - Filtres 12
Figure 17 : Process Monitor - Capture prefs.js 12
Figure 18 : Nouvelle page par défaut 12
Figure 19 : Process Monitor - Filtres 13
Figure 20 : Process Monitor - Filtres 13
Figure 21 : Process Monitor - Résultats 13
Figure 22 : Editeur de registre 14
Figure 23 : Modification clé registre 14
Figure 24 : Modification clé registre en 8.8.8.8 14
Figure 25 : Propriétés IP de la connexion 14
Figure 26 : Process Monitor - Filtres pour capture modif. clé NameServer 15