Chapitre 4
Prise d'empreinte ou Information Gathering

1. Les attaques

1.1 Préambule

En cette période de crise, on constate depuis plusieurs mois une recrudescence des attaques cybercriminelles qui profitent de la vulnérabilité des installations et du manque d'expérience et d'attention des usagers pour s'infiltrer dans les réseaux d'entreprises, ceci afin d'y dérober, chiffrer tous types de données sensibles pour les monnayer de diverses manières.

En conséquence, les entreprises renforcent leurs exigences en moyens de protection et d'analyse et les audits de sécurité se démocratisent, que ce soit pour les grandes mais également moyennes et petites entreprises.

Ils sont désormais régulièrement intégrés dans le cahier des charges lors d'une prise de marché.

L'entrée en vigueur du RGPD (Règlement général sur la protection des données), il y a deux ans, a certainement contribué à la mise en évidence, chez les chefs d'entreprise, des enjeux de sécurité des données.

Un des effets immédiats de cette prise de conscience est la hausse non négligeable des besoins en compétences cyber et des certifications inhérentes (CISSP, CCSP, CEH, CHFI, CISM...).

1.2 Types et méthodologies des attaques

Avant de rentrer dans le vif du sujet et de détailler le déroulement d'une prise d'empreinte (ou collecte d'informations) sur une cible, il est nécessaire de bien comprendre la méthodologie d'une attaque que reprendra un test d'intrusion mis en place dans le cadre d'un cahier des charges prédéfini.

De même, il est important de comprendre que le test d'intrusion souvent appelé "pentest" n'est en fait qu'une étape de l'audit de sécurité comprenant également l'analyse fonctionnelle de l'organisation, l'examen des configurations du code et aussi l'analyse des risques sans laquelle l'audit serait limité.

1.3 L'évolution de la cybercriminalité

Le profil des cybercriminels a bien évolué depuis l'apparition dans les années 1970 des premiers hackers animés par la volonté de mieux sécuriser le réseau en incitant les éditeurs de solutions informatiques à apporter des correctifs aux failles découvertes. Ils étaient d'ailleurs communément appelés des *white hackers*.

Puis est apparu au début du XXI^{e} siècle le cybercriminel motivé par des idéologies et dont les actions étaient ciblées vers tout organisme défiant ces idéologies.

Les Anonymous sont un exemple représentatif et connu des groupes "hacktivistes" sur le Net.

1.4 Les motivations

Actuellement, force est de constater que les motivations idéologiques ont cédé en grande partie la place aux motivations d'ordre financières et à l'espionnage stratégique ou industriel.

Pour la première motivation, la demande est toujours la même : malware ou ransomware, vos données vous seront rendues moyennant une rançon en cryptomonnaie, celle-ci leur assurant un réel anonymat.

Pour le cas de l'espionnage, qu'il soit stratégique ou industriel, les moyens mis en œuvre sont plus sophistiqués.

En effet, ces attaques complexes nécessitent davantage de moyens financiers, matériels et humains.

Généralement organisées par des groupes d'État ou mafieux disposant de gros moyens de mise en œuvre, elles se présentent souvent sous forme d'attaque de type APT (*Advanced Persistent Threats*).

1.5 Les différents types d'attaques

On peut généralement résumer de la façon suivante les différents types d'attaques possibles, au vu des motivations citées précédemment.

1.5.1 L'attaque de type destructif

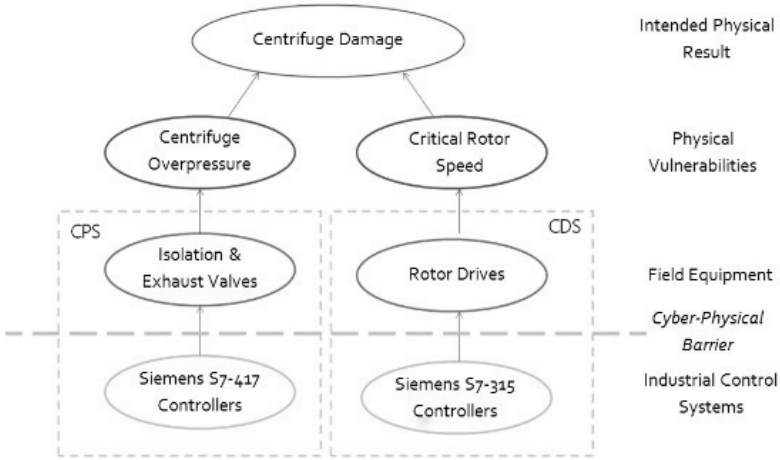
Une attaque de type destructif vise à ralentir ou à stopper le fonctionnement de l'organisation visée via par exemple un déni de service (syn, reflexion, spoof...). Elle est généralement revendiquée par des hacktivistes, les motifs étant politiques ou idéologiques, parfois suite à des défis techniques entre attaquants.

Ce type d'attaque exploite souvent des vulnérabilités connues, sur des systèmes non mis à jour, à des fins de propagande.

Avec l'avènement des systèmes SCADA (*Supervisory Control And Data Acquisition*) dans l'industrie, ces attaques peuvent désormais avoir des conséquences matérielles très graves.

Ce type d'attaque utilise les interactions entre la couche informatique, la couche de contrôle et la couche physique pour créer des destructions physiques.

Stuxnet est typiquement le cas d'école d'une attaque destructrice de matériel industriel : https://www.xmco.fr/actu-secu/XMCO-ActuSecu-27-STUXNET.pdf



Attaque Stuxnet sur les centrifugeuses iraniennes

Remarque

Plus récemment, une attaque de ce type a complètement privé d'électricité 230 000 usagers du réseau électrique du fournisseur d'électricité régional ukrainien Kyivoblenergo.

1.5.2 Les attaques à motivation financière

Un gain financier rapide est la principale motivation de ce type d'attaque. Le vol de données monnayables, qu'elles soient personnelles ou industrielles, ainsi que l'accès aux données bancaires ou la demande de rançon (ransomware) sont généralement les buts avoués de ce type d'attaque.

Entre février et avril 2020, les cyberattaques contre les banques ont marqué une hausse de 238 % suite au confinement et au télétravail mis en place par les entreprises, qui a vu augmenter considérablement ce que les spécialistes appellent la surface d'attaque.

Certaines attaques peuvent être très sophistiquées et orchestrées par des groupes mafieux bénéficiant d'une organisation importante (APT).

Un exemple de ce type d'attaque est celui de l'institut monétaire du Bangladesh qui a perdu près de 100 millions de dollars, la Banque centrale ayant été la cible de pirates informatiques, entraînant la démission du directeur de celle-ci.

Le groupe de cybercriminels Carbanak, bien connu pour ce genre d'attaque APT, a été fortement soupçonné.

1.5.3 Les attaques de type APT

Revenons un peu sur ce type d'attaque très sophistiquée. On appelle APT une attaque qui vise spécifiquement une organisation. Cela peut être une entreprise, un pays, une administration ou encore une ONG.

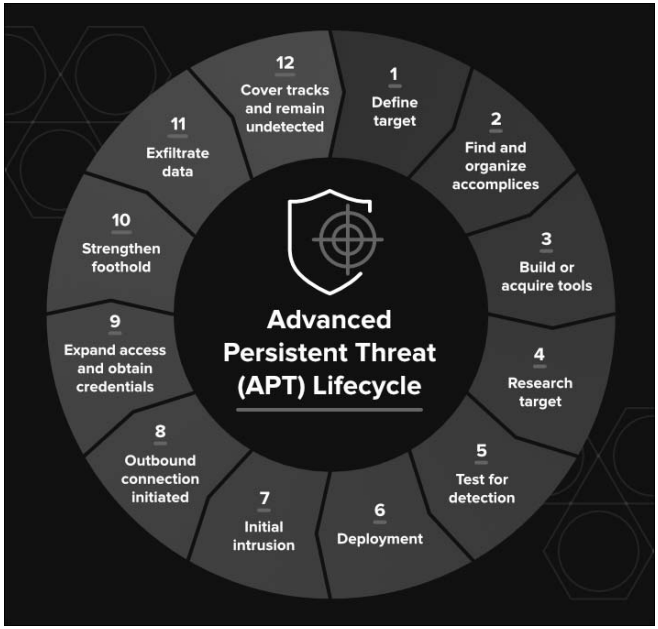
Nombreuses sont les entreprises qui ont été victimes ces dernières années de telles attaques sur leur système d'information.

Ce type d'attaque est dit "avancé", parce qu'elle utilise tout un arsenal de techniques d'attaque et d'outils pour atteindre son objectif. Unitairement, les composants d'une telle attaque ne sont pas forcément évolués techniquement (phishing, malware, XSS, etc.). Des outils de génération de composants d'attaques existent (ex. Poison Ivy, etc.). La combinaison des méthodes et les outils d'attaques en font une attaque avancée.

Elle est *persistent* car basée sur une stratégie dont l'objectif est de rester cachée et indétectable au sein du système d'information.

L'attaque est scénarisée et des objectifs précis sont établis pour compromettre toute une chaîne de systèmes.

C'est bien sûr une menace (*threat*). Elle implique une coordination de moyens techniques et humains. Elle est généralement peu automatisée (bien que les compromissions de systèmes puissent l'être). Les attaquants ont des compétences techniques et généralement des moyens inhabituels.



Cycle de vie d'une attaque de type APT

1.6 La cyber kill chain ou les différentes phases d'une attaque

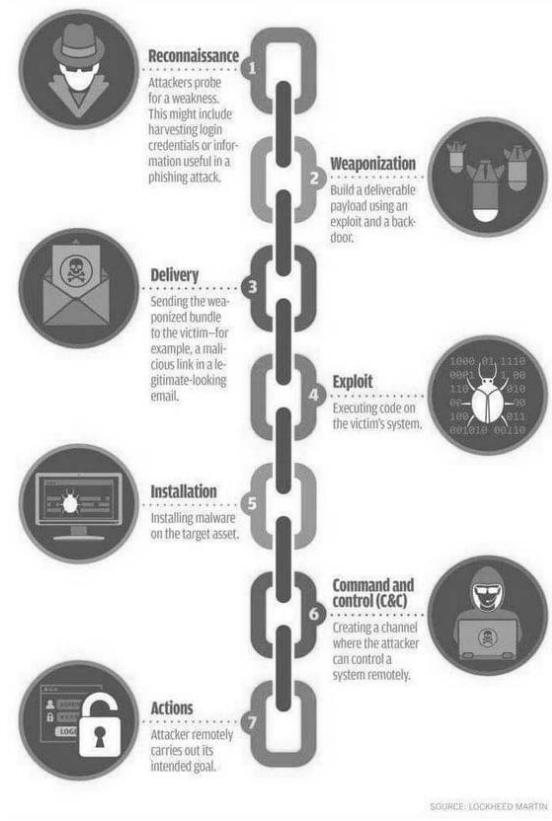
Les attaques informatiques suivent un schéma assez récurrent qui permet d'optimiser les chances de succès et l'ampleur de l'attaque.

Ces différentes étapes sont les suivantes, dans l'ordre :

- La collecte d'informations, encore appelée *information gathering* ou reconnaissance.
- L'intrusion, qui exploitera les résultats de la reconnaissance pour s'introduire dans le système et l'exploitation qui installe le ou les malwares et payloads.
- L'escalade de privilèges, qui leur donnera tous les droits sur le système.

– Le mouvement latéral, déplacement vers d'autres systèmes et comptes afin d'obtenir plus de leviers.
– La persistance, leur permettant de rester invisibles dans le système.
– L'exfiltration des données sensibles, qui pourront ensuite être monnayées.

Par analogie, un pentest se déroulera de la même façon, à la différence de l'exploitation des données qui ne seront pas monnayées mais qui serviront à étayer le rapport du test d'intrusion (*reporting*).



La cyber kill chain

2. L'analyse des risques

Comme il a été dit précédemment, un autre élément de l'audit de sécurité est l'analyse des risques du SI.

La gestion des risques est définie par l'ISO 27001 (révisée en 2013) comme l'ensemble des activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque. On dégage en général trois finalités à la gestion des risques pour les SI :

– Améliorer la sécurisation des systèmes d'information.
– Justifier le budget alloué à la sécurisation du système d'information.
– Prouver la crédibilité du système d'information à l'aide des analyses effectuées.

Bien qu'un grand nombre de celles-ci ne soient plus utilisées ou soient confidentielles, on estime qu'il existe plus de 200 méthodes de gestion des risques.

Cette multiplicité entraîne une très grande diversité dans les approches des risques de sécurité.

À côté de ces méthodes d'analyse des risques, il existe une famille de normes ISO, la norme ISO 27005 (révisée en 2011), qui fait une description développée des exigences en termes de gestion des risques liés à la sécurité de l'information.

Les trois méthodes les plus populaires sont actuellement les suivantes :

– EBIOS (expression des besoins et identification des objectifs de sécurité) : une méthode portée par l'ANSSI.
– MARION (méthode d'analyse de risques informatiques optimisée par niveau).
– MEHARI (méthode harmonisée d'analyse de risques) : maintenue en France par le CLUSIF.

En France, l'ANSSI préconise la méthode EBIOS, arguant du fait que cette méthode est opérationnelle, modulaire et alignée avec les normes françaises. C'est une boîte à outils indispensable pour toute réflexion sur la sécurité des systèmes d'information (SSI).

La méthode dispose de bases de connaissances riches et mises à jour, d'un logiciel libre et gratuit, de formations et d'une documentation variée (http://www.ssi.gouv.fr/ebios - http://www.club-ebios.org).

Chapitre 2
Malwares ciblant les systèmes Microsoft Windows

1. Introduction

Ce chapitre est dédié au système d'exploitation de Microsoft : Windows. Historiquement, ce système d'exploitation est le plus ciblé, car le plus populaire. Il est également le plus utilisé dans le domaine professionnel, ce qui en fait une cible de choix dans les campagnes contre les sociétés. Une bonne connaissance de ce système d'exploitation est primordiale pour comprendre le fonctionnement d'un malware qui le cible.

Ce chapitre présente la collecte de données sur un système suspicieux afin d'identifier un potentiel malware. Grâce à ces données, l'analyse de la mémoire du système sera possible. Ce chapitre présentera également comment créer un laboratoire d'analyse pour finalement réaliser cette première analyse.

2. Collecte d'informations

2.1 Introduction

Avant d'analyser un malware, il est nécessaire de le trouver. Pour pouvoir l'identifier, il faut collecter diverses informations sur la machine potentiellement infectée. Pour une telle collecte, il est préférable de déconnecter le disque dur de la machine infectée pour le connecter sur une machine saine et travailler à partir de celle-ci. Il ne faut pas travailler sur la machine infectée, les malwares peuvent très bien altérer le fonctionnement de la machine et cacher des informations à l'analyste.

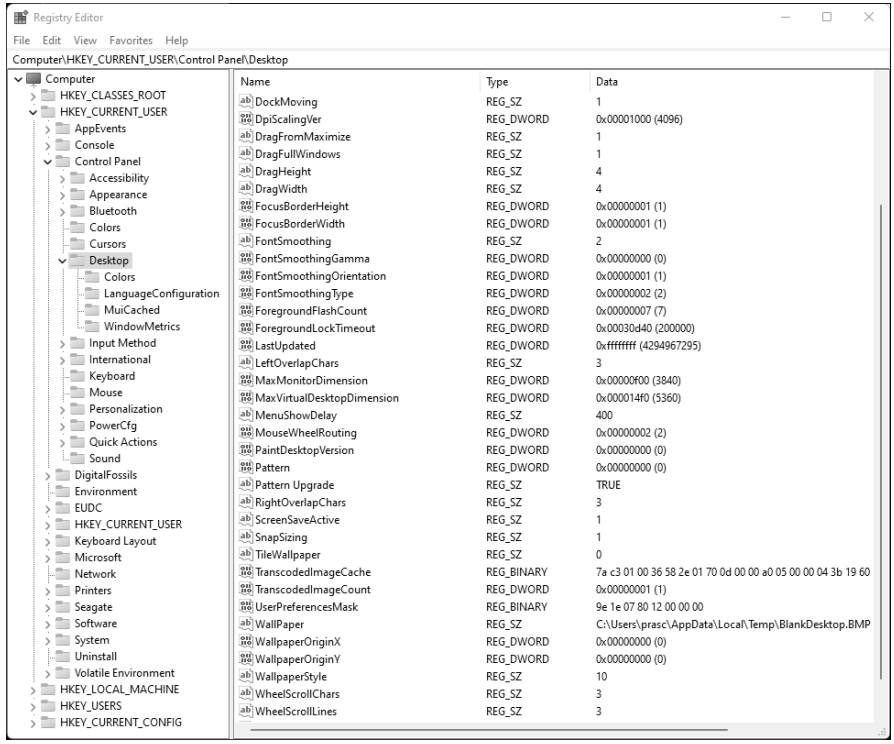
La collecte se fera directement sur le disque dur de la machine infectée. Sur ce disque dur, quatre éléments sont intéressants pour une analyse :

– la base de registre (uniquement sous Windows)
– les journaux d'événements
– les fichiers exécutés au démarrage
– le système de fichiers

2.2 Collecte et analyse de la base de registre

La base de registre est une base de données utilisée par Windows. Elle contient tous les paramètres de configuration du système d'exploitation. Elle prend la forme d'un arbre. Chaque branche contient un ou plusieurs noms, puis un type par nom et une valeur pour chaque nom. La configuration de nombreux outils se trouve dans la base de registre. Par exemple, la configuration du fond d'écran se trouve dans la branche *HKEY_CURRENT_USER\Control Panel\Desktop*. Elle a pour nom *Wallpaper*, elle est de type *REG_SZ*, et a pour valeur le chemin vers le fichier de fond d'écran.

Depuis Windows, elle peut être consultée via la commande `regedit.exe`.



La base de registre est stockée dans des fichiers. Ces fichiers sont accessibles sur le disque dur de la machine. Voici l'emplacement pour chaque base :

– *HKEY_USERS* :
  \Documents and Setting\User Profile\NTUSER.DAT
– *HKEY_USERS\DEFAULT* :
  C:\Windows\system32\config\default
– *HKEY_LOCAL_MACHINE\SAM* :
  C:\Windows\system32\config\SAM
– *HKEY_LOCAL_MACHINE\SECURITY* :
  C:\Windows\system32\config\SECURITY
– *HKEY_LOCAL_MACHINE\SOFTWARE* :
  C:\Windows\system32\config\software

– *HKEY_LOCAL_MACHINE\SYSTEM* :
C:\Windows\system32\config\system
– *HKEY_USERS* :
\User\User Profile\NTUSER.dat depuis Windows Vista

Ces fichiers ne sont pas des fichiers texte. Il faut utiliser un outil pour en visualiser le contenu. Il existe des clients graphiques tels que *Windows Registry Recovery* disponible sur www.mitec.cz ou des clients en ligne de commande comme reglookup disponible sur http://sentinelchicken.org/.

Voici une utilisation simple de `reglookup` :

```
rootbsd@lab:~$ reglookup NTUSER.DAT | more
PATH,TYPE,VALUE,MTIME
/,KEY,,2012-05-16 21:20:30
/AppEvents,KEY,,2012-05-16 14:16:20
/AppEvents/EventLabels,KEY,,2012-05-16 14:16:20
/AppEvents/EventLabels/.Default,KEY,,2012-05-16 14:16:20
/AppEvents/EventLabels/.Default/,SZ,Default Beep,
/AppEvents/EventLabels/.Default/DispFileName,SZ,@mmsys.cpl%2C-5824,
/AppEvents/EventLabels/AppGPFault,KEY,,2012-05-16 14:16:20
/AppEvents/EventLabels/AppGPFault/,SZ,Program error,
/AppEvents/EventLabels/AppGPFault/DispFileName,SZ,@mmsys.cpl%2C-5825,
```

2.3 Collecte et analyse des journaux d'événements

Les journaux d'événements contiennent l'historique des événements apparus sur la machine. Ces journaux regroupent aussi bien les événements système que les événements applicatifs ou encore les événements liés à la sécurité.

Ces journaux permettent de retracer toute l'activité de la machine : la création de comptes, la création et le redémarrage de services, les connexions distantes... En cas de compromission d'une machine, il est important de pouvoir les lire et de comprendre l'origine de l'attaque.

Ces journaux sont au format *.evt* (ou *evtx* depuis Windows Vista) et sont généralement inscrits dans le répertoire *C:\Windows\system32\config*. Ces fichiers ne sont pas des fichiers texte. Pour les convertir en .csv, il est possible d'utiliser l'outil *log2timeline*.

Voici une utilisation de `log2timeline` :

```
rootbsd@lab:~$ log2timeline SysEvent.Evt > SysEvent.csv
-----------------------------------------------------------------
      [WARNING]
No timezone has been chosen so the local timezone of this
machine is chosen as the timezone of the suspect drive.

If this is incorrect, then cancel the tool and re-run it
using the -z TIMEZONE parameter to define the suspect drive
timezone settings (and possible time skew with the -s parameter)

(5 second delay has been added to allow you to read this message)
-----------------------------------------------------------------
Start processing file/dir
[Downloads/uTools/Tools/Tools/Tools/essai/SysEvent.Evt] ...
Starting to parse using input modules(s): [all]
Local timezone is: Europe/Paris (CEST)
Local timezone is: Europe/Paris (CEST)
Loading output module: csv
```

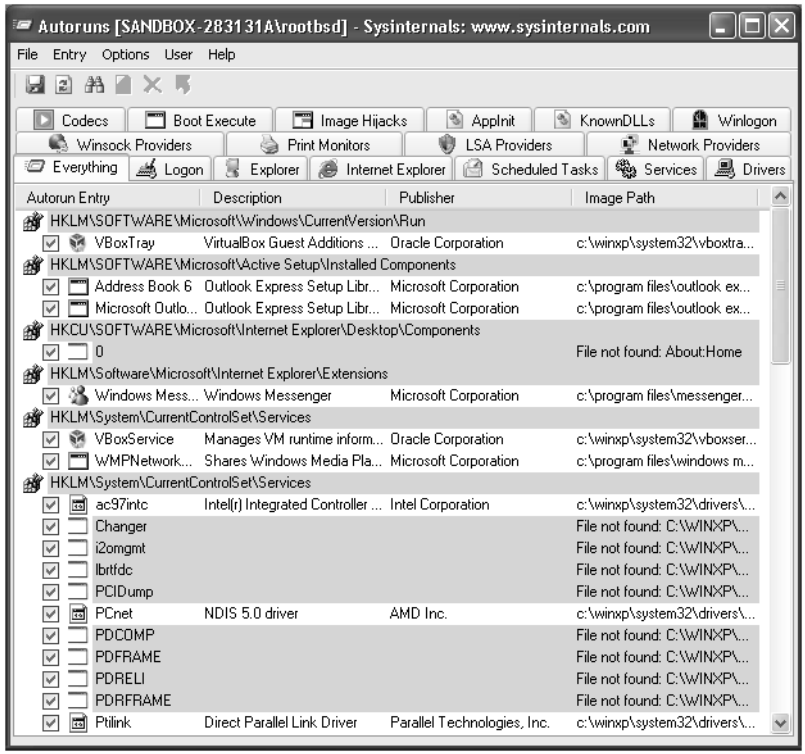
À présent, le fichier .csv peut être ouvert dans un éditeur de texte ou un tableur.

2.4 Collecte et analyse des fichiers exécutés au démarrage

Les malwares sont persistants, cela signifie qu'en cas de redémarrage de la machine, ils doivent se relancer. Il y a plusieurs méthodes pour démarrer une application au démarrage de la machine. La base de registre permet d'exécuter des binaires au démarrage de la machine, mais également au démarrage d'une session par un utilisateur. Windows dispose également de services qui sont exécutés au démarrage de la machine. Certains fichiers sur le système de fichiers peuvent s'exécuter également au démarrage.

Microsoft fournit un outil nommé *Autoruns* qui permet de lister tout ce qui est lancé au démarrage de la machine. Cet outil fait partie de la suite Sysinternals de Microsoft. Il dispose d'une interface graphique, mais il peut également créer des fichiers *.csv* pour être utilisé par un script.

Voilà l'interface graphique de l'outil *Autoruns* :



Cet outil permet d'identifier les fichiers binaires qui ne devraient pas être lancés au démarrage et donc d'identifier le chemin menant à un malware.

Un malware peut cependant se cacher sous la forme d'un service au lieu d'un binaire afin de ne pas apparaître dans la liste des processus. Un service est une bibliothèque (.dll) attachée au processus `svchost.exe` qui gère tous les services de la machine. *Autoruns* permet d'afficher les bibliothèques chargées comme services dans l'onglet **Services**.

Un autre avantage de cet outil est qu'il est possible d'afficher la signature des binaires lancés au démarrage. Il sera plus facile de distinguer les binaires illégitimes des binaires légitimes du système d'exploitation. De plus, il est possible de vérifier si un fichier est connu de *VirusTotal* comme un malware.

Il est possible de sauvegarder le rapport au format CSV et de pouvoir analyser ce fichier via des scripts et d'automatiser certaines détections.

2.5 Collecte et analyse du système de fichiers

Windows utilise le système de fichiers NTFS. De nombreuses métadonnées sont présentes sur ce système de fichiers, comme la date de création d'un fichier, le dernier accès à un fichier... Si une activité suspecte a été identifiée grâce à l'analyse du journal d'événements, il peut être intéressant de savoir quels fichiers ont été créés durant cette période. *TZWorks* fournit un outil permettant de générer un fichier .csv avec toutes ces métadonnées : `ntfswalk` disponible sur http://www.tzworks.net. Cet outil parcourt la MFT (*Master File Table*) et affiche toutes les informations concernant chaque fichier sur le système de fichiers. L'outil permet également de filtrer par date et ainsi de se limiter à la plage de temps nécessaire.

Les options de `ntfswalk` :

```
usage:
 Running 'ntfswalk' on a live volume
  ntfswalk.exe -partition <drive letter> [options]
  ntfswalk.exe -drivenum <num> [-offset <volume offset>] [options]

 Running 'ntfswalk' on a disk/partition image captured w/ a 'dd'
type tool
  ntfswalk.exe -image <file> [-offset <volume offset>] [options]

 Running 'ntfswalk' on an extracted $MFT file
  ntfswalk.exe -mftfile <name> [-options]

 Filter options
    -filter_ext <file extension>
    -filter_name <partial name>
    -filter_start_time <start date time>  = time format "mm/dd/yy
hh:mm:ss"
    -filter_stop_time <end date time>     = time format "mm/dd/yy
hh:mm:ss"
    -filter_deleted_files

 Extraction of data options
    -action_copy_files <directory> [-raw] = extract copies of data
                                          = [-raw] includes slack
```