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.

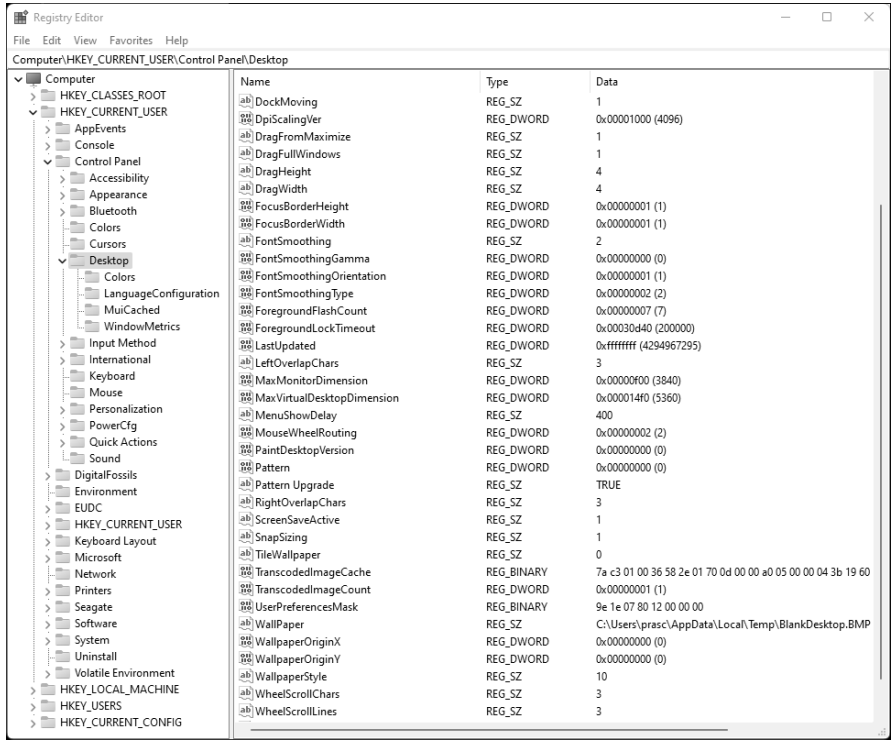
La collecte se fera directement sur le disque dur de la machine infectée. Sur ce disque dur, quatre éléments sont intéressants pour une analyse :

– 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
```

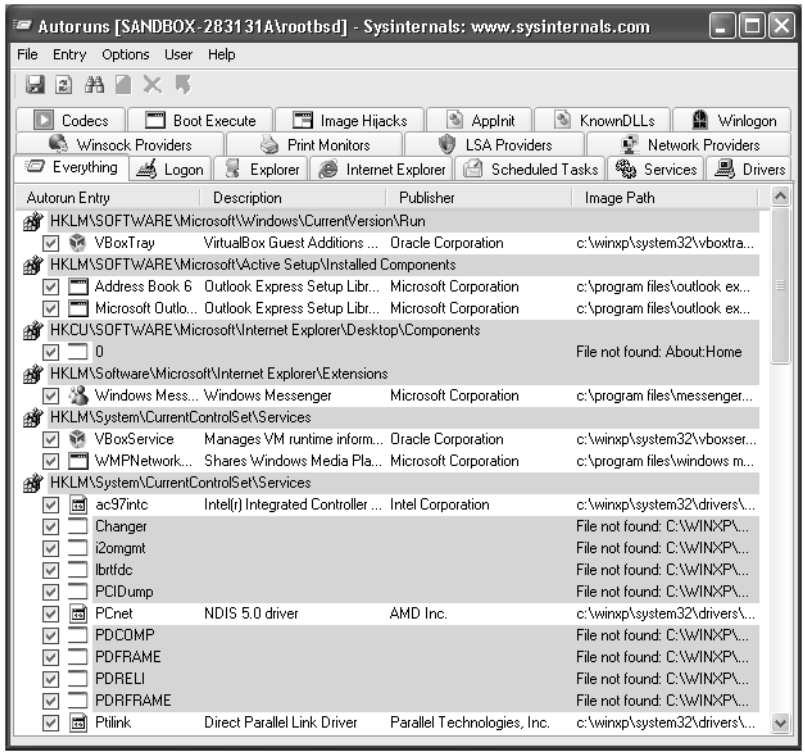
À présent, le fichier .csv peut être ouvert dans un éditeur de texte ou un tableur.

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
```