Semaine 7 : Forensic Windows
IPL I317B Sécurité : labo

Olivier Choquet & Thibault Vanwersch

7 novembre 2023

Objectif

Le but de cette séance est la découverte des registres Windows par l'investigation d'un incident survenu sur une machine Windows. Un événement a eu lieu sur cette machine le dimanche 17 novembre 2019, nous allons mener une investigation autour de cette événement et dans le passé de cette machine pour en apprendre plus.

Support

Vous investiguerez sur le contenu d'un fichier zip distribué sur moodle et représentant l'image du disque de la machine sur laquelle est survenu l'événement.

Précisons que ce n'est pas de la forensique conventionnelle.Si nous voulions nous servir de son résultat comme preuve, une analyse forensique réelle nécessiterai une prise d'image disque exacte (clone), vérifiable (comparaison de hash) et en lecture seul. Nous opérons ici une double simplification : l'image a été nettoyée pour ne contenir que les registres qui nous intéresse et elle est distribuée dans une format zip facile à manipuler sur toutes les plateformes.

Registres Windows

La base de registre Windows est une base de données utilisée par le système d'exploitation (et d'autres logiciels) pour stocker des données de configuration.

Cette base de registre est séparer en plusieurs fichiers répartis sur le disque dur :

```
c:/
├── Users/
│   └── (pour chaque dossier utilisateur)
│       └── NTUSER.DAT
└── Windows/
    └── System32/
        └── config/
            ├── SAM
            ├── SOFTWARE
            └── SYSTEM
```

Outil

Vous allez parser/analyser les registres Windows avec l'outil *regripper*. Cet outil permet de parser les fichiers de registre de Windows afin d'en extraire de l'information pertinente.

https://github.com/keydet89/RegRipper3.0

Ce dépôt contient un exe exécutable directement sous Windows sans installation ainsi que du perl exécutable sous Linux[1].

Regripper se présente sous la forme d'une script perl (*rip.pl*) ou d'un exe (*rip.exe*) qui prend les paramètres suivants :

- -r Reg_hive_ file : le fichier hive à utiliser
- -p plugin_module : le nom du module à utiliser

```
PS E:\laptop\20_21\s09\RegRipper3.0> .\rip.exe -r ..\img_light\Windows\System32\config\SYSTEM -p compname
Launching compname v.20090727
compname v.20090727
(System) Gets ComputerName and Hostname values from System hive

ComputerName    = DESKTOP-7PCSTU8
TCP/IP Hostname = DESKTOP-7PCSTU8
PS E:\laptop\20_21\s09\RegRipper3.0>
```

Les paramètres suivants vous seront également utile :

- -l : liste les modules disponibles
- -h : affiche une aide

1
```
$ git clone https://github.com/keydet89/RegRipper3.0
(...)
$ export PERL5LIB=$(pwd)/RegRipper3.0/
$ ls
RegRipper3.0  img_light  img_light.zip  ipl_I317B_s07.pdf
$ cd RegRipper3.0/
$ perl ./rip.pl -r ../img_light/Windows/System32/config/SYSTEM -p compname
```

Module regripper

Le paramètres -l vous permet de lister tous les modules disponibles. Je vous invite fortement à explorer cette liste avec des grep ou des ctrl-f.

En attendant, voici, hive par hive, quelques modules intéressants :

- dans la hive SYSTEM
  - compname (info de base de la machine)
  - timezone
  - shutdown
  - mountdev
  - usb et usbstor
- dans la hive SOFTWARE
  - winver
  - networkcards
  - portdev
- dans la hive SAM
  - samparse : liste des utilisateurs
- dans les hive utilisateur
  - userassist
  - run

Questions

Pour chaque question, préciser

1. Dans un premier temps, nous allons profiler cette machine, commencez par récupérer les information suivantes :le nom de la machine, la version de Windows installée et la liste de ses utilisateurs. Parmi ces utilisateurs, quel est notre utilisateur principal ? ComputerName = DESKTOP-7PCSTU8
   winver = Windows 10 Pro
   .\rip.exe -r ..\img_light\Windows\System32\config\SAM -p samparse
2. Un élément essentiel dans une enquête manipulant des ressources informatiques est de s'assurer de la consistante des timestamps. .\rip.exe -r ..\img_light\Windows\System32\config\SYSTEM -p timezone
   - Sur quel timezone est configuré cette machine?
   - On voit régulièrement des timestamps qui finissent par Z comme :

     ```
     2019-11-14 11:56:22Z
     ```

     Que cela signifie-t-il ?
     fuseaux horaire (z = utc-0)
   - Quand cette machine a-t-elle été installée et éteinte pour la dernière fois ?
     .\rip.exe -r ..\img_light\Windows\System32\config\SYSTEM -p shutdown
3. Intéressons-nous maintenant aux différents objets auquel l'utilisateur principal à accédé. Vous trouverez ceux-ci dans la clé de registre UserAssist. Utilisez ces données pour établie une ligne du temps des actions de l'utilisateur en 2019.
   .\rip.exe -r ..\img_light\Users\MediaMonster\NTUSER.DAT -p userassist
4. Vous aurez pu constater au point précédent, l'utilisateur semble avoir utilisé d'autres disques que c :, vous pouvez récupérer de l'information partielle à la fois dans les hives SYSTEM et SOFTWARE et ce avec plusieurs modules : portdev, mountdev et usbstor. Utilisez ces informations pour identifier les disques externes et quand c'est possible la dernière lettre qui leur a été attribué.
5. Il est temps maintenant de nous raconter l'histoire du 17 novembre 2019 : que c'est-il passé sur cette machine ?