

TP 11 Guillaume Sanchez

IOC concernant WannaCry

Un IOC est un élément observable permettant d'identifier une compromission informatique. Il peut s'agir de fichiers, d'adresses IP, de domaines, ou encore de comportements suspects.

En nous appuyant sur la base de connaissances attack.mitre.org, le comportement de WannaCry peut être analysé à travers plusieurs techniques observables :

- Fichiers et exécutable :

WannaCry utilise un fichier malveillant, souvent nommé mssecsvc.exe, ce fichier peut être identifié par son hash MD5 (e8089341ee0442a2ecf82e4b70829143) et SHA256 (55bc52ead4c668b4dad978bebd80821a68eccd36b3927072a5d113cd5d79a27a).

- Adresses IP & Domaines :

WannaCry contacte des serveurs via des adresses IP spécifiques ou des domaines, y compris un *kill switch* (domaine qui désactive le ransomware s'il est actif).

- Mutex / Artéfacts en mémoire :

WannaCry utilise un mutex pour éviter plusieurs exécutions. Il a été observé dans des mémoires capturés avec un dump à l'aide des outils Volatility et SANS Memory Cheat Sheet.

- Clés de registre / Commandes

WannaCry supprime des copies de sauvegarde avec des commandes comme "vssadmin" "delete shadows" afin de rester invisible.

- Comportements réseau

WannaCry scanne des ports SMB (445) pour ce réprendre.

Types d'éléments nécessaires pour des IOC efficaces

Pour qu'un IOC soit réellement utile pour la détection et la réponse, il doit inclure :

1. **Hashes** (MD5/SHA1/SHA256) pour identifier précisément des fichiers malveillants.
2. **IP adresses** liées à C&C, serveurs Tor ou activités malveillantes.
3. **URLs / noms de domaine**, y compris domaines alternatifs, .onion et kill-switch.
4. **Fichiers spécifiques** : noms, tailles, chemins attendus (e.g. mssecsvc.exe).
5. **Mutexes**, signatures dans la mémoire pour pointer des infections en cours.
6. **Préfixes registre**, clés ou commandes attendues (shadow copy suppression via wmic, p.ex.).
7. **Comportements réseaux** : ports atypiques (445 SMB, Tor 9001), patterns connexions.
8. **Comportements systèmes** (TTPs selon MITRE ATT&CK : scan LAN, suppression shadow copies...).

Boite à outils

Voici une liste d'outils permettant de réaliser des dumps mémoires ou images disque, d'analyser pour détecter les IOC listés (hashes, mutex, fichiers malveillants), et de contre attaquer et se protéger :

- **Volatility** : Capture de mémoire (dump) et analyse mémoire avec ses plugins pslist, malfind, mutex.
- **SleuthKit** : Permet d'analyser les disques et les images disques
- **WireSharke** : analyse de paquets réseau qui permet de capturer, inspecter et diagnostiquer le trafic

Test de Sleuth Kit

Sleuth Kit est une bibliothèque et un ensemble d'outils en ligne de commande permettant d'analyser des images de disque. La fonctionnalité principale de TSK permet d'analyser les données des volumes et des systèmes de fichiers. La bibliothèque peut être intégrée à des outils d'investigation numérique plus importants, et les outils en ligne de commande peuvent être utilisés directement pour rechercher des preuves.

Mmls : Voici la commande mmls compris dans Sleuth Kit. On l'utilise dans les enquêtes forensiques numériques. Cette commande permet d'afficher la table de partition d'une image disque. Voici une explication de chaque élément de la sortie :

```
joshua@Icarus ~/Desktop/images $ mmls 4GB_USB.dd
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors
```

	Slot	Start	End	Length	Description
000:	Meta	0000000000	0000000000	0000000001	Primary Table (#0)
001:	-----	0000000000	0000011263	0000011264	Unallocated
002:	000:000	0000011264	0007886847	0007875584	Win95 FAT32 (0x0b)

Fsstat : Cette commande donne des informations détaillées sur le système de fichiers FAT32 présent dans l'image disque 4GB_USB.dd, en commençant à l'offset 11264 (trouvé avec mmls comme point de départ de la partition FAT32).

```
joshua@Icarus ~/Desktop/images $ fsstat -o 11264 4GB_USB.dd
FILE SYSTEM INFORMATION
-----
File System Type: FAT32

OEM Name: MSDOS5.0
Volume ID: 0x4cb42013
Volume Label (Boot Sector): NO NAME
Volume Label (Root Directory):
File System Type Label: FAT32
Next Free Sector (FS Info): 1216544
Free Sector Count (FS Info): 4331984

Sectors before file system: 11264

File System Layout (in sectors)
Total Range: 0 - 7875583
* Reserved: 0 - 31
** Boot Sector: 0
** FS Info Sector: 1
** Backup Boot Sector: 6
* FAT 0: 32 - 7707
* FAT 1: 7708 - 15383
* Data Area: 15384 - 7875583
** Cluster Area: 15384 - 7875583
*** Root Directory: 15384 - 15391

METADATA INFORMATION
-----
Range: 2 - 125763206
Root Directory: 2
```

Fls : La commande fls (File List) de **Sleuth Kit** affiche le contenu d'un répertoire dans un système de fichiers, ici FAT32, à l'offset 11264 (comme indiqué précédemment avec mmls et fsstat).

```
joshua@Icarus ~/Desktop/images $ fls -o 11264 4GB_USB.dd
r/r 10: Python Crash Course_ A Hands-On, Project-ntroduction to Programming - Eric Matthes.pdf
r/r 16: Quality Assurance Management of a Digital Forensic Laboratory.pdf
d/d 17: FOUND.000
d/d * 18: _ASE001
r/r * 19: _UTOPS-1.MSI
d/d 22: Imager Lite 3.1.1
d/d 25: winMd5SumPortable
r/r 28: autopsy-4.1.1-64bit.msi
r/r * 32: .sbdirtestfile_XfpRVx7o2M.C20342
r/r * 33: PG.png
r/r * 37: Trans-gravity-falls-season-01.png
r/r * 42: trans-gravity-falls-season-01.png.crdownload
r/r * 46: trans-gravity-falls-season-01.png
r/r * 50: 560c672ea57e1f2dead096834d82a1db.jpg
r/r * 55: 560c672ea57e1f2dead096834d82a1db.jpg.crdownload
r/r 59: 560c672ea57e1f2dead096834d82a1db.jpg
r/r 61: Gow-0.8.0.exe
r/r 62: IMG_4363.JPG
r/r 65: IMG_4366 g.JPG
r/r 67: Strings.zip
r/r 70: testdisk-7.0.win.zip
r/r * 74: torbrowser-install-6.0.5_en-US.exe
r/r * 79: -crop-342-254-254px-nowatermark-Color-Step-8-2.jpg
```

Test du logiciel Volatility :

Voici une démonstration de l'analyse du fichier .dmp :

```
(venv) nkp@ppp-nk:~/Documents/oultis/volatility3$ python3 vol.py -f ~/Téléchargements/CC_Niveau2.dmp windows.info
Volatility 3 Framework 2.26.2
Progress: 100.00 PDB scanning finished
Variable Value
Kernel Base 0x82801000
DTB 0x185000
Symbols jar:file:/home/nk/Documents/oultis/volatility3/volatility3/symbols/windows.zip!windows/ntkrpamp.pdb/5B30884ED6464159B87117C711E7340C-2.json.xz
Is64Bit False
IsPAE True
Layer_name 0 WindowsIntelPAE
Memory_layer 1 FileLayer
KdDebuggerDataBlock 0x82929be8
NTBuildLab 7600.16385.x86fre.win7_rtm.09071
CSDVersion 0
KdVersionBlock 0x82929bc0
Major/Minor 15.7600
MachineType 332
KeNumberProcessors 1
SystemTime 2013-01-12 16:59:18+00:00
NtSystemRoot C:\Windows
NtProductType NtProductWinNt
NtMajorVersion 6
NtMinorVersion 1
PE MajorOperatingSystemVersion 6
PE MinorOperatingSystemVersion 1
PE Machine 332
PE TimeDateStamp Mon Jul 13 23:15:19 2009
```

On peut voir qu'après le passage de la commande "python3 vol.py -f ~/Téléchargements/CC_Niveau2.dmp windows.info", Volatility nous affiche les informations du fichier analysé.

Il existe une multitude de commande avec Volatility afin de réaliser des tests d'analyses.