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 répendre.

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

Test du logiciel Volatility :

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

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.