

Sommaire

[1. Contexte 1](#_Toc131068660)

[2. Réalisation du cas pratique 2](#_Toc131068661)

[3. Analyse de l’attaque à chaud 3](#_Toc131068662)

[4. Analyse de l’attaque à froid 4](#_Toc131068663)

# 1. Contexte

Pour commencer ce cas pratique nous allons rappeler le contexte. Nous avons une machine Windows Server 2016 qui s’est retrouvée infecté par un malware à la suite de l’exécution d’un script batch présent sur le Bureau (qui a pu être téléchargé dans une pièce-jointe de mail par exemple). À la suite du lancement de ce script nous allons devoir procéder à une récupération des données avant que le malware ne supprime tout et réaliser une analyse de l’attaque qui s’est produite.

Quand une machine se retrouve infecté il est important de savoir quelles données récupérer comme :

- Des trames réseaux en cas de capture

- Des journaux / logs

- La mémoire et le disque pour analyse à froid

Il est aussi possible de se rendre compte d’une cyberattaque de différentes façons :

- Une expérience utilisateur (une machine qui bug…)

- Utilisation d’IDS/IPS ou EDR

- Traffic réseau important

- Redémarrage fréquent d’une machine

- Détection par antivirus

- Utilisation d’une supervision

- Pièces-jointes reçues par mail

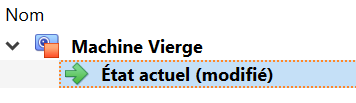
- Surveiller la base de registres Windows

- En analysant le stockage interne et externe

# 2. Réalisation du cas pratique

Pour commencer ce cas pratique nous avons téléchargé une OVA de machine Windows Server 2016 infecté par un malware.

Une fois l’OVA téléchargée nous devons l’importer dans un Virtualbox et prendre un snapshot de la machine à l’état « non infecté » avant le lancement d’un script :



Nous pouvons maintenant démarrer la VM, fermer le gestionnaire du serveur et exécuter le script batch qui se situe sur le Bureau :

Une image contenant texte, ciel, bleu

Description générée automatiquement

Une fois le script lancé nous perdons totalement le contrôle de notre machine :

Une image contenant texte

Description générée automatiquement

# 3. Analyse de l’attaque à chaud

**/ ! \ Avant d’effectuer toute analyse il est nécessaire de prendre beaucoup de capture d’écrans ou d’enregistrer l’écran en direct afin de garder un maximum de preuve car en cas de redémarrage de la machine ou fichier fermé les preuves peuvent disparaitre**

Nous pouvons voir qu’un bloc-notes est apparu avec les informations suivantes dedans :

Une image contenant texte

Description générée automatiquement

Cela nous dit que tous les fichiers sont devenus inutilisables et qu’il faut payer 100$ en bitcoin à une adresse très bizarre. Nous avons à faire à un ransomware.

Nous remarquons aussi que les boutons de la souris ont été inversés

L’écran ne fait que clignoter en continu et le clavier reste utilisable

Plusieurs CMD ont été exécutés

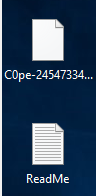
Si nous essayons de faire un CTRL+ALT+SUPP on se rend compte que le gestionnaire des tâches a été désactivé par l’administrateur :

Une image contenant texte

Description générée automatiquement

Une fois le gestionnaire des tâches bloqué le clignotement de l’écran disparaît

En minimisant toutes les fenêtres et en revenant sur le Bureau nous pouvons voir que 2 fichiers sont apparus :



# 4. Analyse de l’attaque à froid

Afin de pouvoir analyser l’attaque à froid il nous faut télécharger un logiciel qui va nous permettre de collecter toute la mémoire RAM actuelle.

La collecte d’informations est l’un des premiers reflexes que nous devrions avoir car comme nous l’avons dit au-dessus en cas de redémarrage de la machine nous pouvons tout perdre

Le logiciel se nomme MRCv120. Pour l’envoyer vers notre VM nous pouvons faire un dossier partagé entre la machine physique et la VM

**/ ! \ Attention : Il faut bien créer un dossier vide et séparé des autres dossiers de la machine physique afin d’éviter toute attaque dessus**

Ici nous pouvons créer un dossier sur la machine physique dans le disque D : (D:\tmp/vm/)

Dans ce dossier on insère l’exe du logiciel et nous pouvons retourner sur la VM

Maintenant sur la VM nous pouvons aller dans l’onglet périphérique -> dossiers partagés -> réglages et ajouter le dossier crée juste au-dessus :

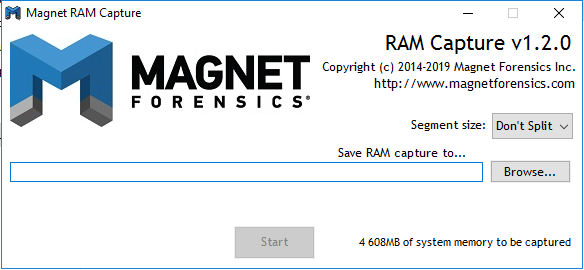
Une image contenant texte

Description générée automatiquement

Dans la VM on exécute ([\\VBOXSVR\vm](file:///\\VBOXSVR\vm)) ce qui nous permet d’ouvrir le dossier partagé et d’exécuter le logiciel :



Dans le logiciel nous définissons l’endroit où nous allons faire une capture de la mémoire en cliquant sur « browse » :



Une image contenant texte

Description générée automatiquement

Et pour finir on donne un nom au fichier enregistré

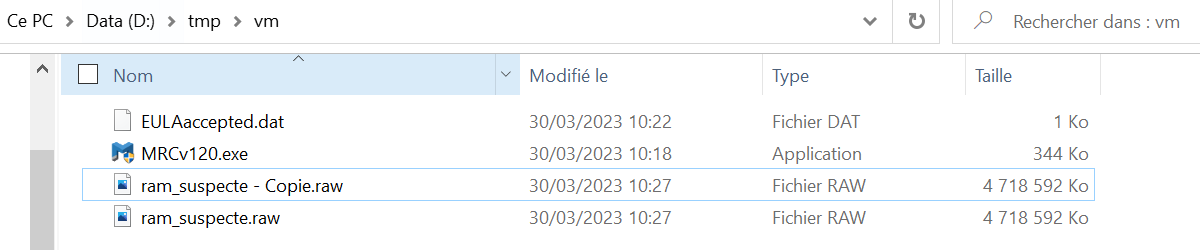
Maintenant nous pouvons revenir sur notre machine physique et nous pouvons commencer notre analyse

**/ ! \ Attention : Il faut toujours travailler dans une copie du fichier car en cas d’erreur nous avons toujours l’original**

**De plus il faut s’assurer que le fichier soit bien protégé par un chiffrement ou un hash et qu’il soit signé**

**Le fait de signer un fichier permet de prouver l’authenticité d’une personne et le hash permet de vérifier l’intégrité du fichier**

Copie du fichier :

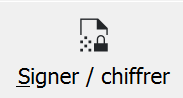


Pour signer le fichier nous pouvons utiliser l’outil gpg sous Linux ou gpg4win sous Windows

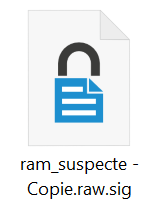
Nous devons générer une paire de clé publique/privée protégé par un mot de passe :



Ensuite nous pouvons signer le fichier (sans le chiffrer) :



Fichier obtenu après signature :



Il est important de signer nos fichiers si nous devons les échanger par exemple avec des laboratoires qui vont s’occuper de l’analyse

Cela permet de prouver que c’est bien la bonne personne qui nous a fourni le fichier

Nous pouvons aussi vérifier que la signature est bien conforme :

Une image contenant texte

Description générée automatiquement

Maintenant que le DUMP est bien effectué nous pouvons envoyer le fichier signé ainsi que notre clé publique au laboratoire pour analyse