cyna
secure your future

Ransomware

Méthodologie de réponse à incident

IRM-0 08/09/2023

Introduction

Cette méthodologie de réponse à incident est une feuille de route dédiée aux gestionnaires et aux cellules de crise menant une investigation sur un problème de sécurité précis.

- La fiche IRM s'adresse aux personnes ou fonctions suivantes :
  - Les RSSI et leurs adjoints
  - Les DSI et leurs adjoints
  - Les administrateurs

Rester calme et contacter immédiatement l'équipe de réponse à incident Cyna.
Nos canaux de discussion :

- Cybersecurity@cyna-it.fr
- **+33 9 70 70 41 81 (Heure ouvrés)**

En cas d'urgence, veuillez insérer la balise [URGENT] dans l'objet du courriel. Veuillez noter que notre CERT est disponible 24 heures sur 24 et 7 jours sur 7, mais que l'assistance téléphonique n'est pas disponible en dehors des heures de bureau.

Identification & Processus d'endiguement

Objectif : Détecter l'incident, déterminer son ampleur et impliquer les acteurs appropriés.

1.1. Détection d'un ransomware

Comment détecter une attaque par Ransomware ?

1. **Changements d'Extension :**
   - Si les extensions de vos fichiers changent soudainement, ils pourraient être chiffrés. Exemple : « document.docx.locked »
2. **Messages d'Avertissement :**
   - Des messages demandant une rançon pour débloquer vos fichiers apparaissent.
3. **Fonds d'Écran Modifiés :**
   - Votre fond d'écran peut changer pour afficher des instructions de paiement.
4. **Fichiers "Lisez-moi" :**
   - Des fichiers texte inconnus apparaissent, indiquant des instructions de paiement.
5. **Fichiers Inaccessibles :**
   - Les fichiers ne s'ouvrent plus normalement.
6. **Activité Disque Intense :**
   - Votre disque dur est très actif sans raison apparente.
7. **Ralentissements :**
   - Votre ordinateur devient lent et peu réactif.

8. **Comportement Anormal du Navigateur :**
    - Votre navigateur agit étrangement avec des redirections inattendues.
9. **Connexions Réseau Suspectes :**
    - Vous repérez des connexions réseau inexpliquées.
10. **Processeur Surchargé :**
    - Votre CPU est fortement sollicité même lorsque vous ne faites rien.

1.2. Appliquer le bon processus

→ Dès qu'une machine semble être infectée :

- NE PAS ETEINDRE OU REDEMRARRE LA MACHINE
    - Suspendre une machine virtuelle
- Isoler la machine du réseau :
    - Débrancher le ou les câble Ethernet.
    - Désactiver le WIFI et le Bluetooth.
- Débrancher tous les périphériques de la machine.

Manipulations

Dans cette section nous verrons toutes les données qui sont à récupérer pour préparer les investigations des équipes CYNA.

Machines virtuelles

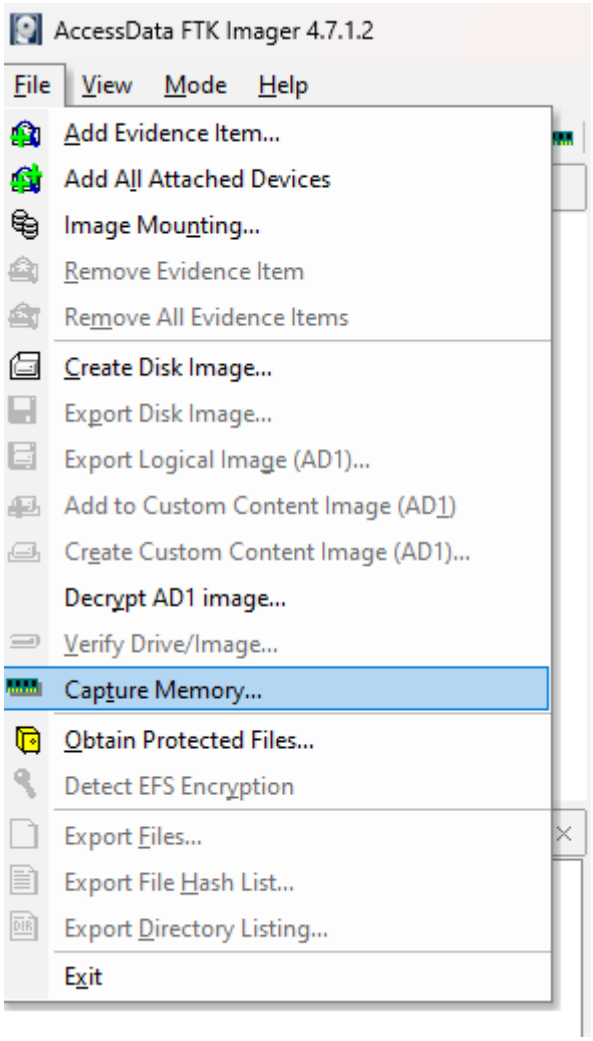
Si une machine virtuelle est infectée, il ne faut pas **L'ETEINDRE MAIS LA SUSPENDRE**. Cela permet de conserver les données contenues dans le fichier « RAM » de la VM. En cas d'arrêt de la VM redémarrage ce fichier « RAM » sera supprimé et recréé.

Si la machine est une machine virtuelle :

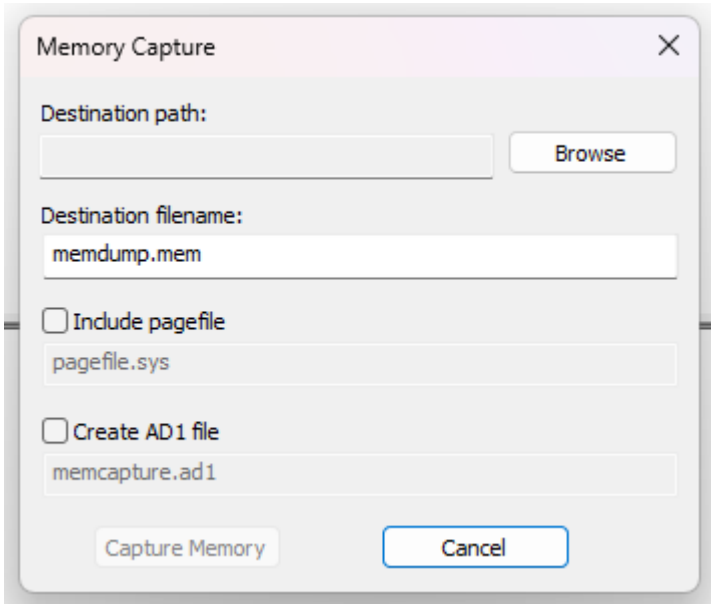
- Pour les machines sur un hyperviseur VMware: récupérer le fichier .vmem d'une machine suspendue. C'est le contenu de la RAM de la machine virtuelle.
- Pour les machines sur un hyperviseur Hyper-V: récupérer le fichier .bin d'une machine suspendu. C'est le contenu de la RAM de la machine virtuelle.

Si cette une machine physique vous aurez besoin de FTKImager afin d'extraire les données présentes dans la RAM. Pour ce faire télécharger le logiciel sur internet depuis un autre poste et déposé l'exécutable via une clé USB sur la machine infectée. Installez ensuite le logiciel et ouvrez-le.

Pour extraire les données contenues dans la RAM de la machine :



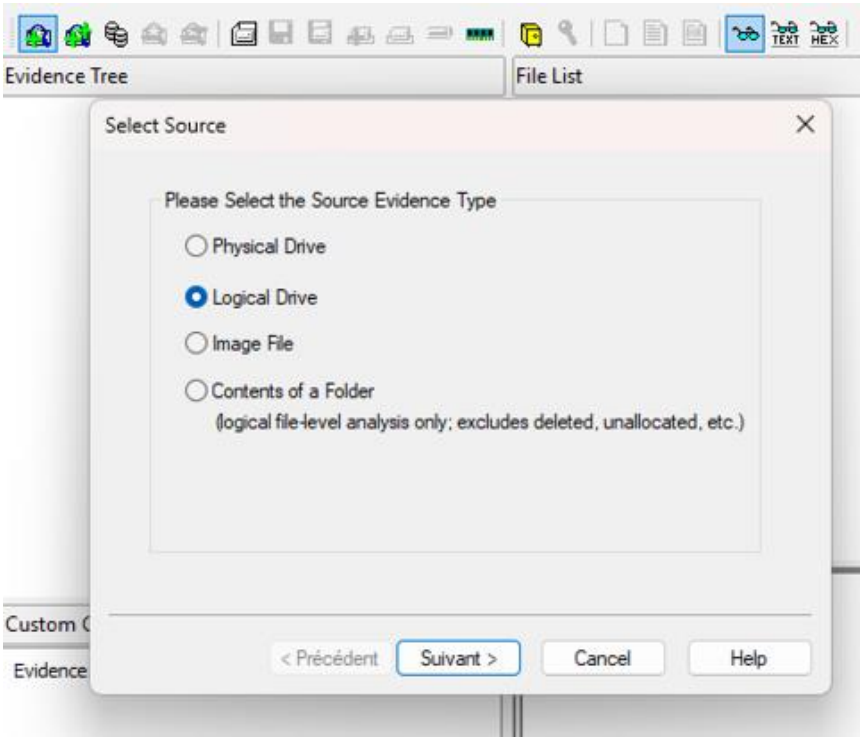
➡ Cliquez sur « File » puis sur « Capture Memory… »

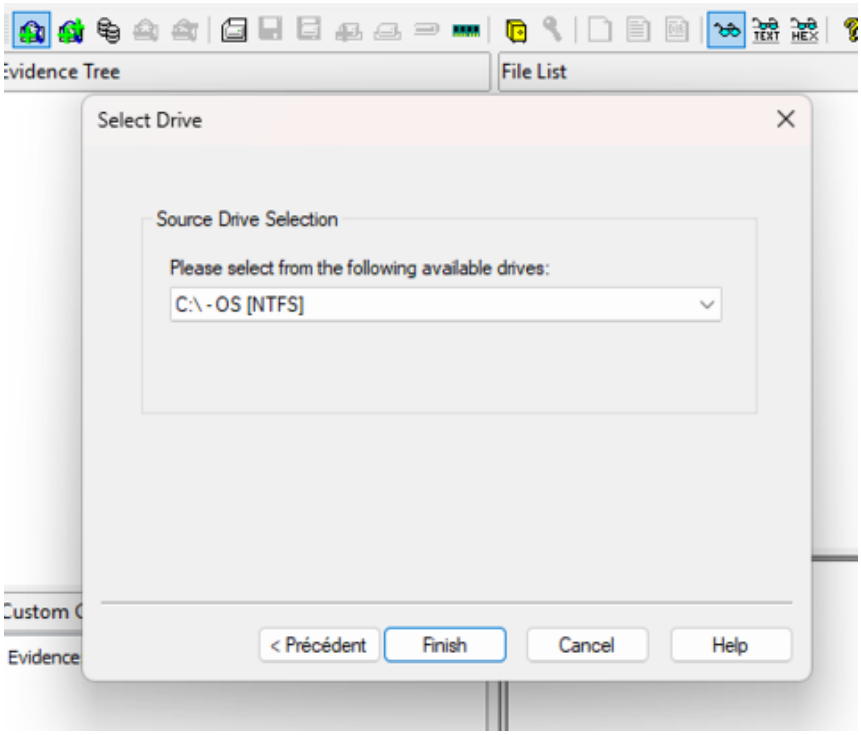


➡ Définissez le nom du fichier et où vous voulez le déposer. ATTENTION, il est possible que la machine plante pendant le processus et qu'elle redémarre. Dans ce cas, la donnée est perdue mais nous pouvons encore récupérer les données des tables MFT.

Manipulations Disques/Fichier MFT

Pour récupérer le fichier contenant les données de la table MFT, vous pourrez utiliser le logiciel FTKImager.
Pour ce faire il faudra ajouter une « evidence » pour examiner votre disque :





➡ Sélectionnez le disque voulu

Vous voyez ainsi le disque sélectionner. Dans la section « OS », puis « root » vous trouverez en défilant le fichier « $MFT ». Faites un clic droit sur ce fichier puis cliquez sur « Export ». Choisissez ensuite où déposer ce fichier. C'est un des fichiers qui servira aux analystes pour les investigations.