TP - **Projet d'Analyse malware**

January 27, 2025

Environnement de travail

Pour installer les fichiers à analyser : `$> /bin/bash -c "$(curl␣-fsSL␣https://raw.githubusercontent.com/securitylab-repository/scripts/refs/heads/main/install_projet_malware)"-s user_name`.

1 Mise en place de l'environnement d'analyse :

Flare et REMnux sont des outils utilisés en cybersécurité pour l'analyse de logiciels malveillants et l'ingénierie inverse. Flare fait partie d'une boîte à outils conçue pour aider à l'analyse des logiciels malveillants, tandis que REMnux est une distribution Linux contenant divers outils pour examiner les logiciels malveillants. Pour configurer un environnement d'analyse utilisant Flare VM et REMnux, suivez ces étapes :

1. **Configuration de Flare VM :**
   - Préparez une machine virtuelle Windows 10.
   - Téléchargez et exécutez le script d'installation de Flare VM depuis ce dépôt `https://github.com/mandiant/flare-vm/tree/main?tab=readme-ov-file`.
   - Suivez les instructions d'installation pour configurer Flare VM avec des outils d'ingénierie inverse.
2. **Configuration de REMnux :**
   - Suivez les instructions d'installation de REMnux pour installer via un installateur personnalisé REMnux `https://docs.remnux.org/install-distro/install-from-scratch` ou en utilisant l'appliance REMnux `https://docs.remnux.org/install-distro/get-virtual-appliance`.
   - Assurez-vous que tous les outils sont correctement configurés pour l'analyse de logiciels malveillants.

Combinez les environnements en les reliant dans votre configuration réseau pour permettre l'interaction entre les deux machines virtuelles.

2 Analyse du fichier APT

Réaliser une première analyse du fichier en suivant ces étapes et en répondant à ces questions :

1. Utilisez la commande `file` pour afficher le type du fichier `~/malware_samples/apt`

   ```
   $> file file_name
   ```

2. Quel est le type du fichier ?
3. Quelles menaces peuvent affecter ce type de fichier ?

4. En utilisant le script `oledump`, lister les objets contenus dans ce fichier:

```
$> oledump -a ~/malware_samples/apt
```

indication:

Pour installer oledump :

```
$> /bin/bash -c "$(curl␣-fsSL␣https://raw.githubusercontent.com/securitylab-repository/scripts/refs/heads/main/install_oledump)"-s user_name
```

Pour extraire un item et le décompresser:

```
$> oledump -a ~/malware_samples/apt -s AN -v #N = 1  9
```

5. Y-t-il un script ? Si oui, l'extraire.
6. Quel est son type ?
7. Analyser ce script pour extraire un fichier caché à partir du fichier originel `apt`.
   (a) Quel est le type de ce fichier caché ?
   (b) Est-il executable ? Si oui,
   (c) Comment est-il censé être lancé (donnez la commande) ?
   (d) A quel emplacement est-il sauvegardé ?
   (e) Comment est-il sauvegardé ?

indication: Pour rechercher une chaîne de caractères dans un fichier compressé

```
$> zipgrep -i "une␣chaine␣de␣caractres"/opt/debian/malware_samples/apt
```

Pour décopresser un fichier ZIP:

```
$> unzip /opt/debian/malware_samples/apt
```

Pour décoder un code en base64:

```
$> cat file | base64 -d
```

8. En suivant les étapes d'analyse de malwares vues en TP, analyse de manière statique le fichier extrait.

3 Analyse du fichier mal2.exe

1. Effectuez une analyse manuelle statique et dynamique de ce fichier.
2. Configurez un système d'analyse automatisé tel que Cuckoo, ou tout autre outil similaire. Il devrait être en mesure de réaliser une analyse tant statique que dynamique.
3. Réalisez à nouveau l'analyse en utilisant cet environnement automatisé.