**US 1:**

- Installation de la machine virtuelle sur Oracle VirtualBox avec .iso Windows 10

- Lancement du Virus

**US 2:**   
  
Hash :

Différent hash du virus : MD5 D872A3086FBB82ED0BA8322C028692DC

SHA1 AF1D820E374ED50757DCDE26BDA069FA86B9B771

SHA256 49F891ADE48890BFA22D2B455494BE95E52392C478B67E10626222B6AEE37E1E

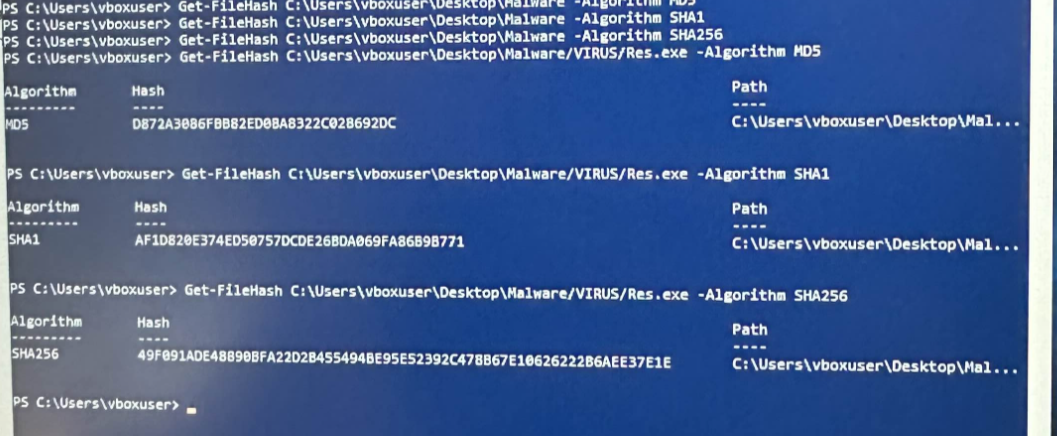
Mettre le fichier dans virustotal -> trojan.keylogger/zkxji

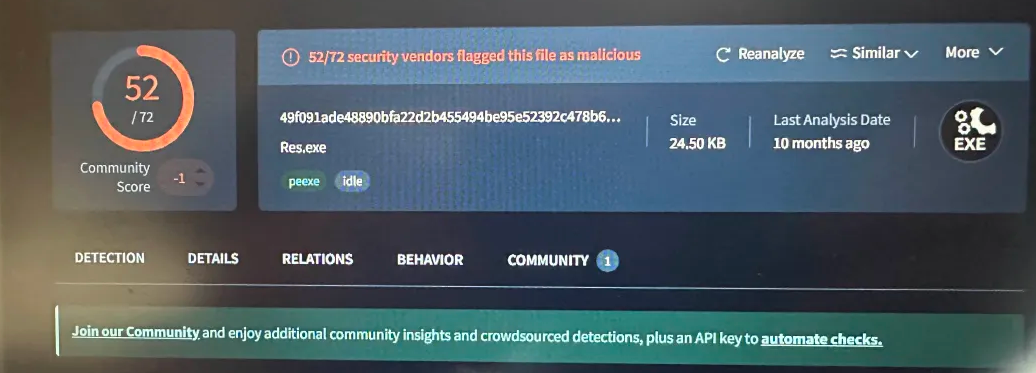
-> 54 Moteurs sur 70

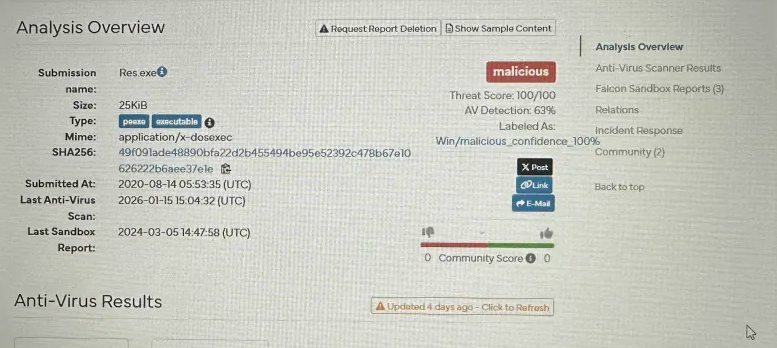
-> Trojan

Mettre le fichier dans Hybrid Analisis -> malicious

-> Trojan







**US 3:**   
Verifier le maware avec SysinternalsSuite :

-> Signature invalide

-> Type PE32

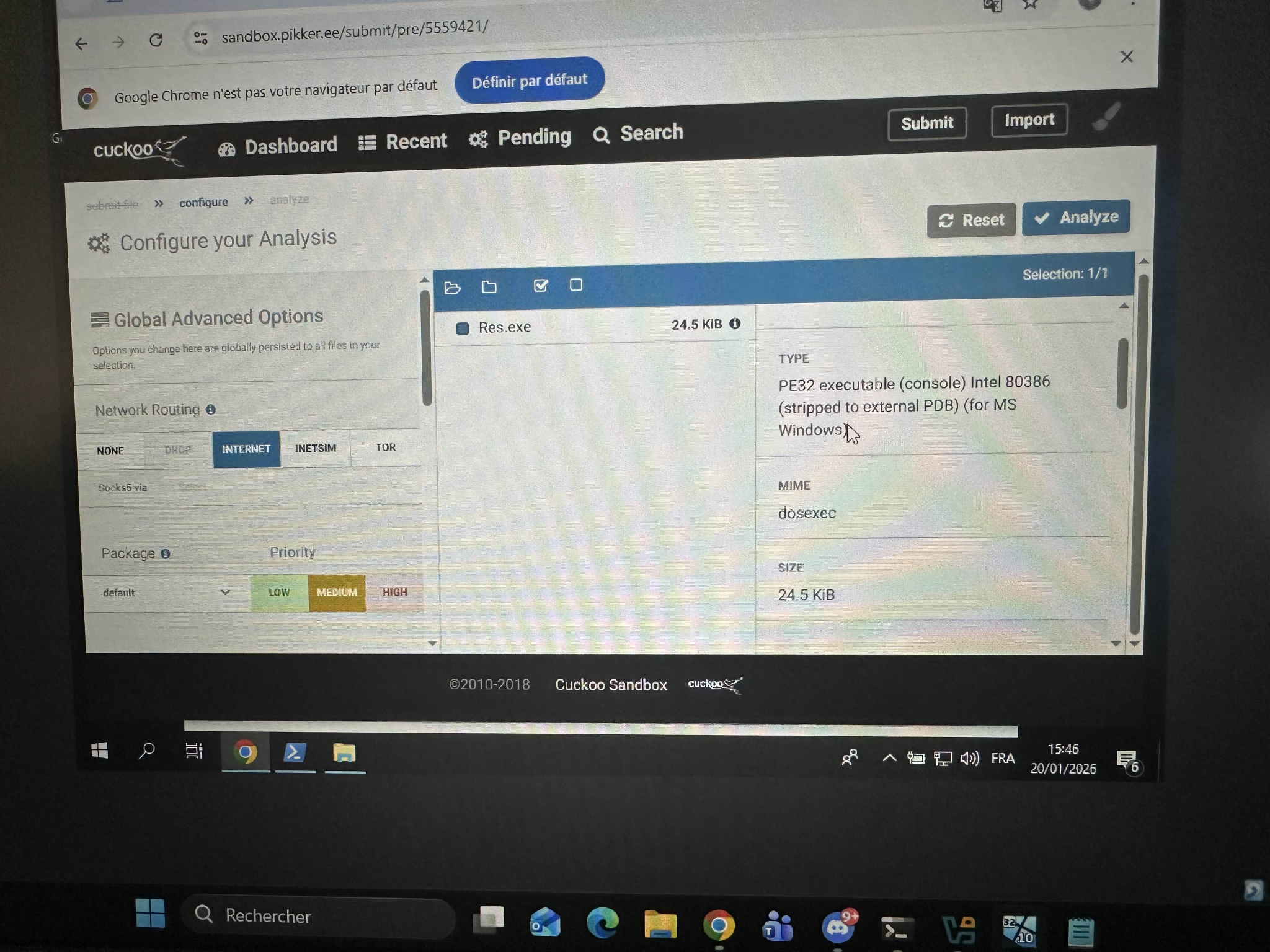
-> Architecture x86

Nous avons analyser le malware afin d'identifier sa structure et ses fonctionnalités

"C:\Cybersécurité\CyberMachine.vdi" (la VM)

VBoxManage clonemedium disk "C:\Cybersécurité\CyberMachine.vdi"

"C:\Cybersécurité\CyberMachineInfected.raw" --format RAW

  
**US 4:**    
  
  
 -> A vérifier

les processus :

- gestionnaire des tache : Processus

les fichiers :

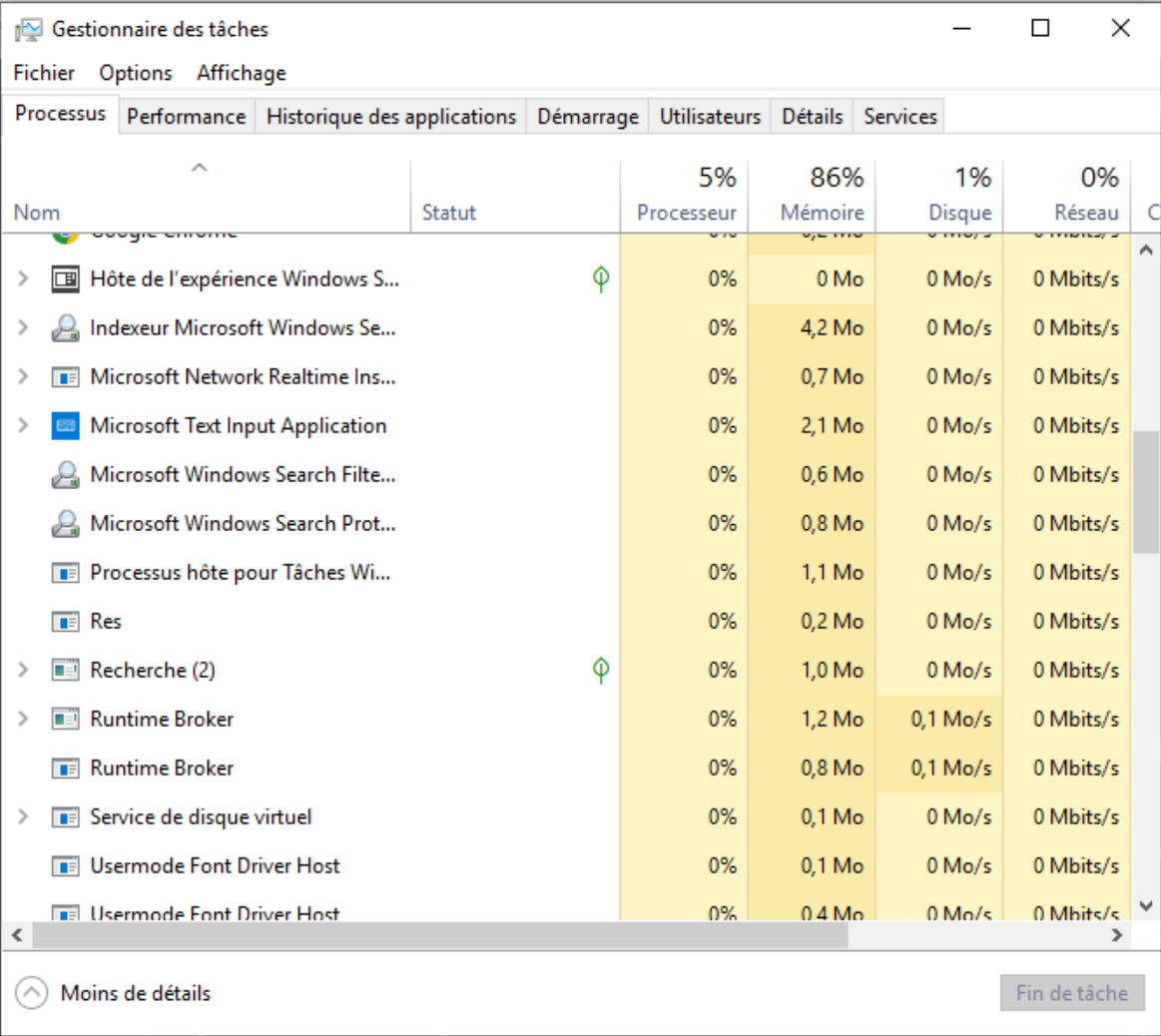
- ProgramData

- AppData

- Temp

Le réseau :

- réseau interne NAT



-> Observations :

Pour les processus en cour, dans le gestionnaire des tâches, il y a :

- 20 processus en arrière-plans pour la VM infecté

- 15 processus en arrière-plans pour la VM non infecté

Les processus qui se sont ajouté après l'exécution du Malware sont :

- Extended copy utility

- Interpréteur de commande

- Microsoft text input application

- Res

- Système settings broker

Pour les fichiers, dans le disque dur principal, dans l'explorateur de fichier il y a :

- 1 fichier ajouté après l'exécution du Malware.

- le fichier se nomme : " WindSyst "  
  
  
**US 5:**

Observation :

- Ralentissement

- Application du virus en arrière-plan visible dans le gestionnaire de tâches, mais impact très faible

- Se lance au démarrage

- Des pics d'utilisation du processeur de la mémoire observés

- des montées de % d'utilisation du processeur

- Type : Cheval de Troie

Impacts

Le malware impacte principalement la disponibilité du système.

La consommation anormale des ressources (CPU, mémoire et disque) entraîne un ralentissement de la machine, pouvant perturber l’utilisation normale du poste de travail et provoquer une indisponibilité partielle du système.

Évaluation du risque :

Le niveau de risque est évalué comme élevé, en raison de la facilité d’exécution du malware par l’utilisateur, de son lancement automatique, et de son impact direct sur la disponibilité du système.

Recommandations de sécurité :

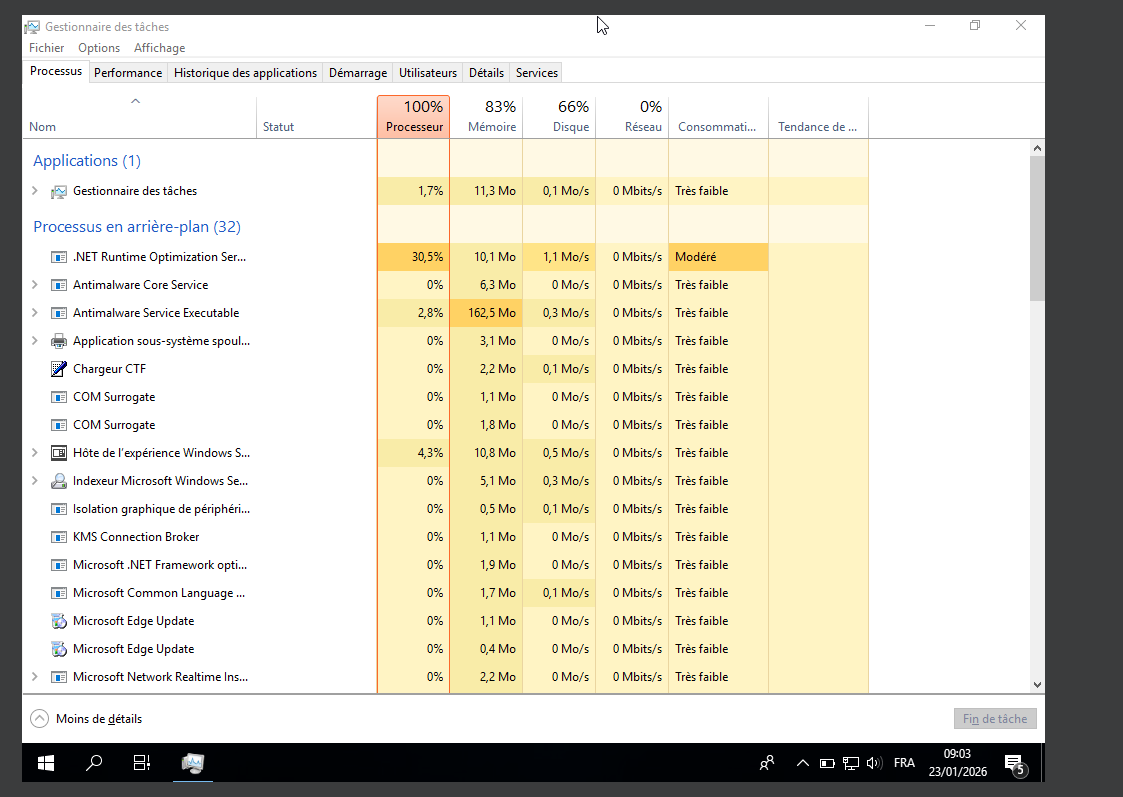
- Installer et maintenir un antivirus à jour

- Appliquer les mises à jour de sécurité

- Restreindre les droits administrateur

- Activer un pare-feu

Sensibiliser les utilisateurs aux risques liés aux fichiers inconnus et au phishing

  
  
  
**US 6:**    
  
- pour obtenir le dump de la RAM complet , il faut utiliser cette commande sur Volatility :

python vol.py -f CYBERMACHINE-20260121-090024.dmp windows.info

on observe des infos comme l' OS (Windows 10) ou l'architecture par exemple (32 bits)

- pour lister les processus actifs , il s'agit de cette commande :

python vol.py -f CYBERMACHINE-20260121-090024.dmp windows.pslist

on observe des fichiers suspects comme : res.exe / cmd.exe / xcopy.exe

-pour analyser les réseaux actif suspect , on utilise :

python vol.py -f CYBERMACHINE-20260121-090024.dmp windows.pslist

**US 7:**  
Etapes :

- Conversion du disque VDI → RAW

- Image bit-à-bit complète

- Identification du fichier suspect

- Analyse hors ligne

Outils utilisés :

- Oracle VirtualBox

- VBoxManage

- FTK Imager

Information du fichier :

- Nom : Malware-main

- Chemin : CyberMachine.raw/Partition [root]/Users/vboxuser/Downloads/Malware-main

- Date de création : 20/01/2026 12:06:27

- Date de modification : 20/01/2026 14:10:59

- Taille : 152 bytes

- Hash MD5 : capture d’écran

Ligne de commande utilisée :

- C:\Users\vboxuser\Downloads\

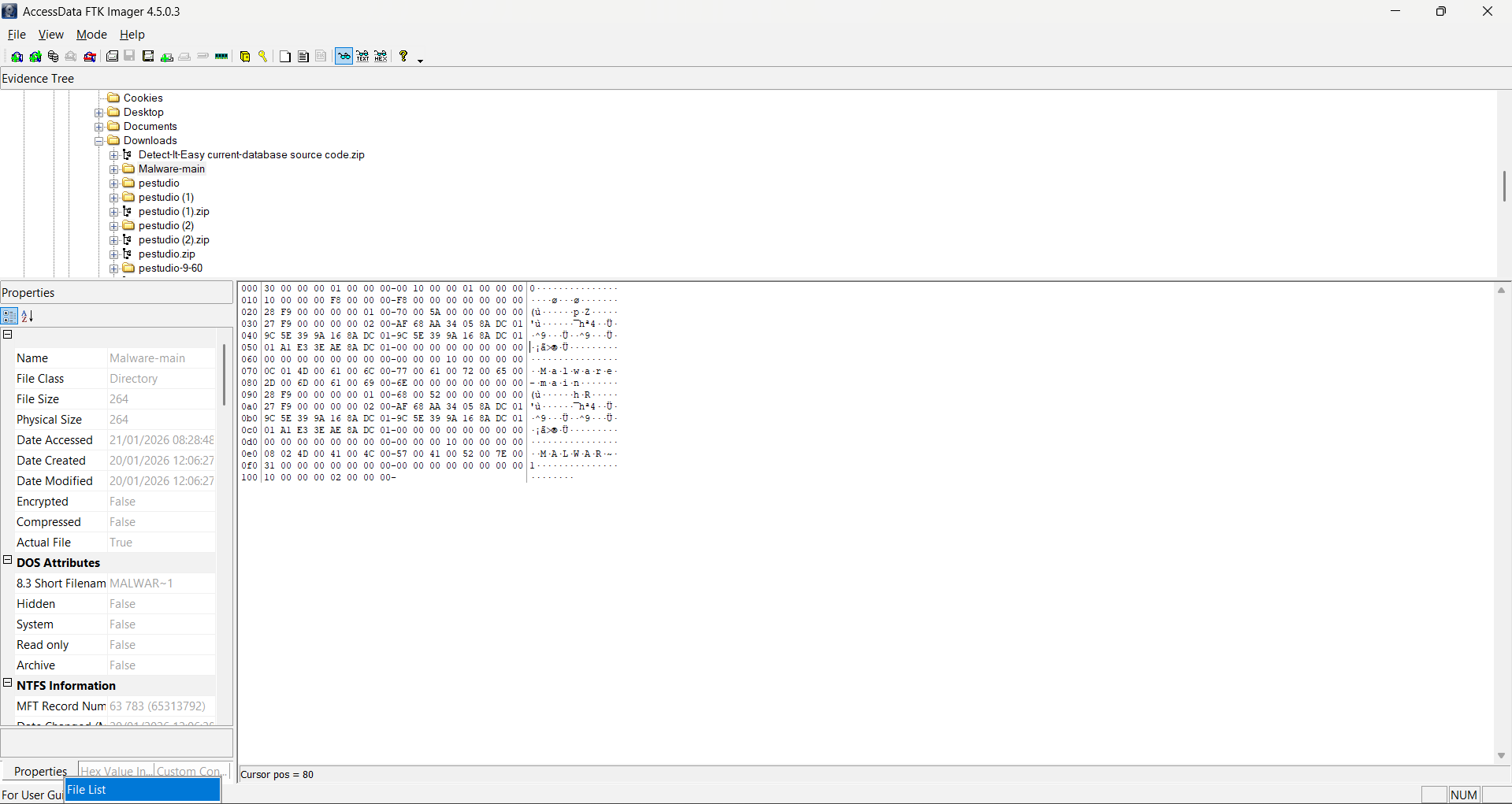
- VBoxManage clonemedium disk "C:\Users\Lucas BAUDIN\VirtualBox VMs\CyberMachine\CyberMachine.vdi" "C:\Cybersécurité\CyberMachine.raw" --format RAW

- Users\vboxuser\Downloads\Malware-main

Un fichier suspect nommé Malware-main a été identifié dans le répertoire de téléchargement de l’utilisateur vboxuser.

Le fichier a été créé le 20 janvier 2026 à 12h06, correspondant à la période d’infection.

Sa taille anormalement faible (152 octets) suggère un rôle de chargeur ou de script malveillant.

Les empreintes cryptographiques ont été relevées afin de garantir l’intégrité de la preuve.  
  
  
**US 8:**    
  
Cette analyse mémoire a permis d’identifier un processus malveillant nommé res.exe, avec le PID 2140.

Le PID (Process Identifier) est un identifiant unique attribué par le système d’exploitation à chaque processus en cours d’exécution.

Il permet de distinguer précisément un processus actif en mémoire.

Le chemin du binaire associé au processus a également été récupéré, permettant de faire le lien entre la mémoire et le disque.

La corrélation entre les données mémoire et les fichiers présents sur le disque a confirmé que le processus observé en RAM correspond bien à un fichier malveillant stocké sur le système.

Enfin, l’analyse des mécanismes de persistance a montré que le malware survit à un redémarrage de la machine. Cela indique la présence d’un mécanisme de persistance,

caractéristique d’un cheval de Troie, et confirme la compromission du système.

**US 10:**   
  
 Etapes :

- Création d'un disque dur virtuel

- Insertion du fichier Dump-memoire-main en format extrait

- Détachement du disque virtuel pour simuler éjection de la clef USB

- Observation du C:\Windows\INF\setupapi.dev.log afin de retrouver trace de la clef

Commande utiliser :

C:\Windows\INF\setupapi.dev.log

Dans le cadre de l’US 10, une image disque a été utilisée pour simuler une clé USB contenant des données sensibles.

Le disque virtuel a été monté, utilisé, puis détaché afin de générer des traces système.

L’analyse du fichier setupapi.dev.log a permis d’identifier des événements horodatés liés à la gestion des périphériques, contribuant à l’établissement d’une chronologie cohérente de l’utilisation du support.  
  
   
  
