Rendu CyberSécurité

Antonin, Ghazi, Siwar, Thiméo

US 1:Mise en place d’un environnement sécurisé
EN TANT QUE analyste malware,
JE VEUX exécuter le Malware dans un environnement isolé,
AFIN DE protéger le système hôte et observer le comportement réel du malware.

Critères d’acceptation :

- Environnement isolé (VM / sandbox)
- Absence de fuite réseau non contrôlée

Réflexion

Avant d’exécuter le malware, il était nécessaire de réfléchir à un moyen d’isolation efficace. L’utilisation d’une machine virtuelle sous Windows 10 s’est imposée comme une solution adaptée, car elle permet d’isoler le système analysé du poste hôte. Le réseau représente un vecteur de fuite ou de propagation majeur ; il devait donc être configuré de manière à limiter strictement les communications tout en conservant un accès minimal pour l’administration du système.

Ce que nous avons fait

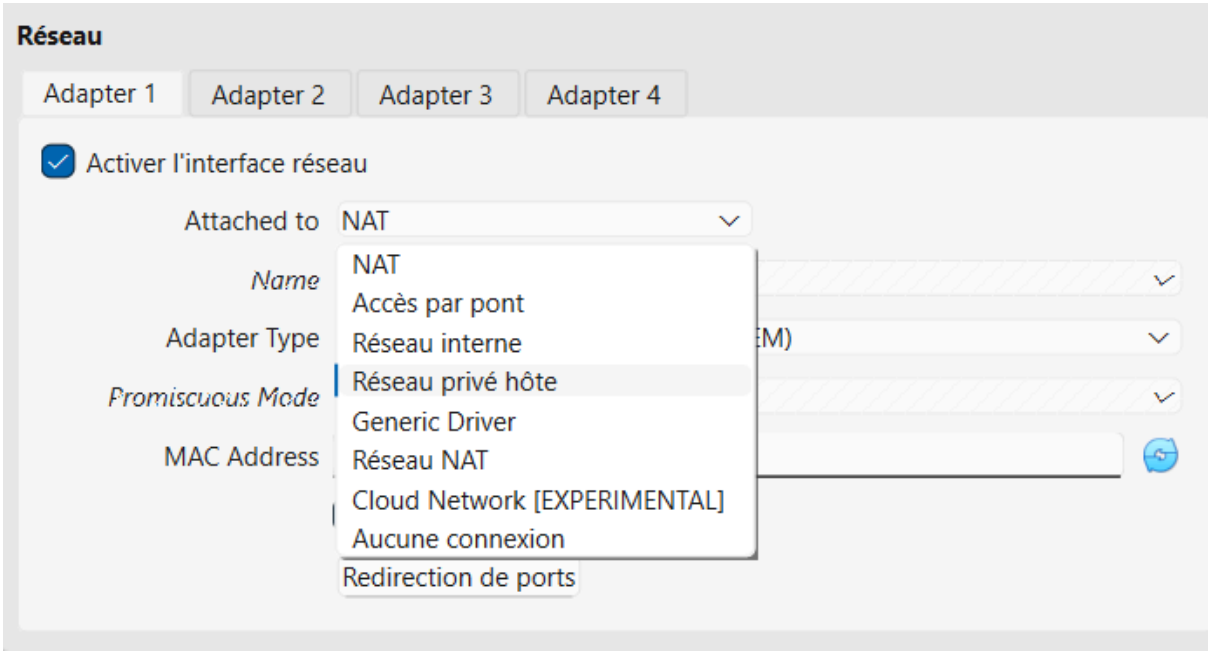
Nous avons commencé par installer une machine virtuelle Windows 10 à l’aide de VirtualBox.
Le réseau de la machine virtuelle a ensuite été configuré de manière contrôlée, avec une connexion limitée via SSH, afin d’éviter toute fuite réseau non maîtrisée.
Une fois l’environnement prêt, le malware a été installé sur la machine virtuelle.
Enfin, le malware a été exécuté exclusivement au sein de cette VM.

Ce que nous avons obtenu

Le malware a pu être exécuté dans un environnement isolé, sans impact sur la machine hôte. La configuration réseau mise en place a permis d’éviter toute fuite réseau non contrôlée. Cette étape a permis d’observer le comportement initial du malware en toute sécurité et de préparer les analyses suivantes dans un cadre maîtrisé.

Validation des critères d’acceptation

- **Environnement isolé (VM / sandbox)** : Validé
- **Absence de fuite réseau non contrôlée** : Validé


Réseau
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Activer l'interface réseau
Attached to
NAT
Name
Adapter Type
Promiscuous Mode
MAC Address
NAT
Accès par pont
Réseau interne
Réseau privé hôte
Generic Driver
Réseau NAT
Cloud Network [EXPERIMENTAL]
Aucune connexion
Redirection de ports

US 2:Vérification de la reconnaissance
EN TANT QUE analyste SOC,
JE VEUX vérifier si le malware est déjà connu,
AFIN DE déterminer s'il s'agit d'une menace nouvelle ou référencée.

Critères d'acceptation :

- Hash calculé
- Résultats de détection documentés
- Comparaison avec bases existantes

Réflexion

Pour répondre à cet objectif, il était nécessaire d'utiliser un outil capable de comparer un fichier malveillant à un grand nombre de bases antivirus et de sandboxes. Un service centralisé, reconnu et multi-éditeurs permet d'obtenir rapidement une vision globale du niveau de détection du malware ainsi que des informations sur son historique et ses comportements connus.

Ce que nous avons fait

Nous avons commencé par rechercher un outil permettant de scanner et d'analyser un malware. Nous avons choisi VirusTotal pour réaliser cette analyse.
Le fichier contenant le malware a été soumis sur la plateforme. Une fois le scan effectué, un score de détection est apparu et nous avons consulté les informations détaillées disponibles dans l'onglet *Details*.\n\nLes informations temporelles suivantes ont été relevées :

- **First Submission** : 2022-10-13 07:43:41 UTC
- **Last Submission** : 2026-01-20 20:49:41 UTC
- **Last Analysis** : 2025-12-02 09:08:07 UTC

Hash calculé

Les hashs du fichier ont été extraits afin d'identifier de manière unique l'échantillon et de pouvoir le comparer à d'autres bases (MITRE, MISP, MalwareBazaar, etc.) ou le retrouver ultérieurement :

- MD5 : 954f7191688a0d4eb5a60692bd27f1e3

- SHA-1 : 1d9e88ef0ab9003b4dc8f34cf0341105ac3cdb7e
- SHA-256 : alaf8eeaa7fda7ced591a72c572a12c2298ddb763defaa36ce5b17be14

Résultats de détection documentés

L'analyse montre que 43 moteurs antivirus sur 67 détectent le fichier comme malveillant. VirusTotal fournit pour chaque moteur le verdict (Malware, Trojan, Clean).

Comparaison avec les bases existantes

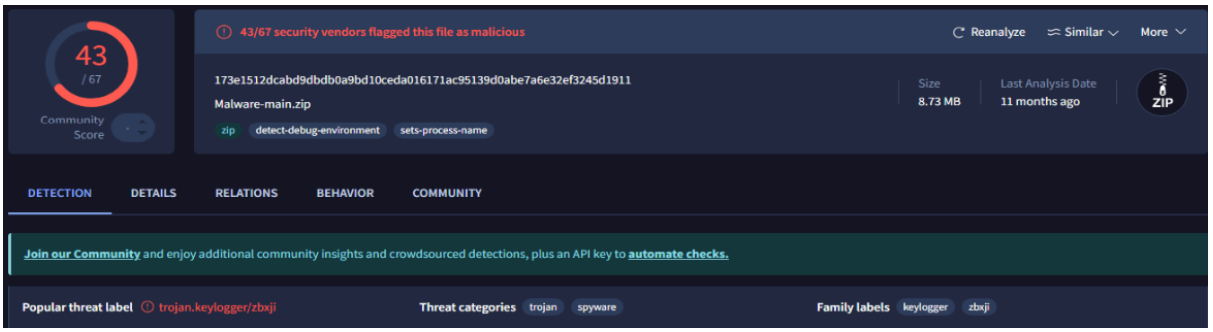
La comparaison avec les bases existantes montre que l'échantillon est déjà connu. Il est détecté par un grand nombre de moteurs antivirus qui l'identifient majoritairement comme un Trojan de type Keylogger (Win32).
Les résultats des sandbox (notamment CAPE Sandbox et Zenbox) ainsi que l'analyse MITRE ATT&CK mettent en évidence des techniques déjà documentées, telles que la persistance, la capture d'entrées clavier et l'accès aux identifiants. Ces comportements correspondent à des signatures et techniques déjà référencées dans les bases de sécurité existantes.

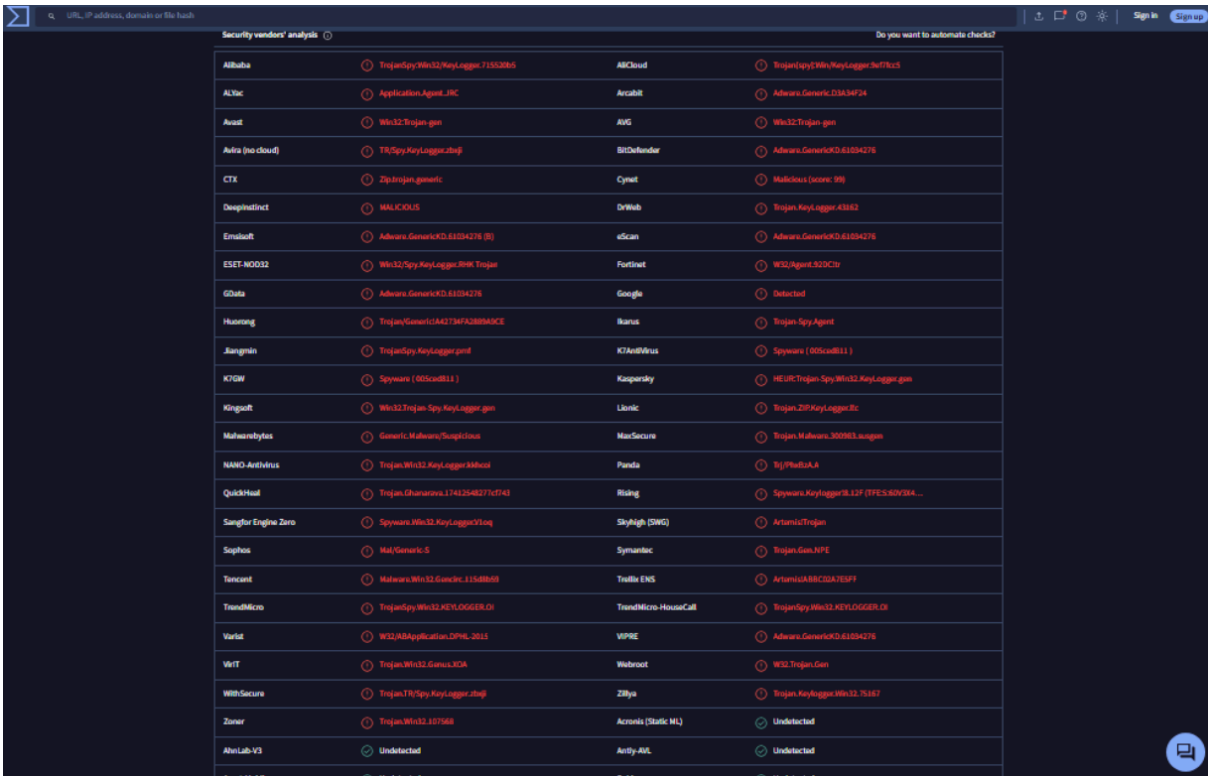
Ce que nous avons obtenu

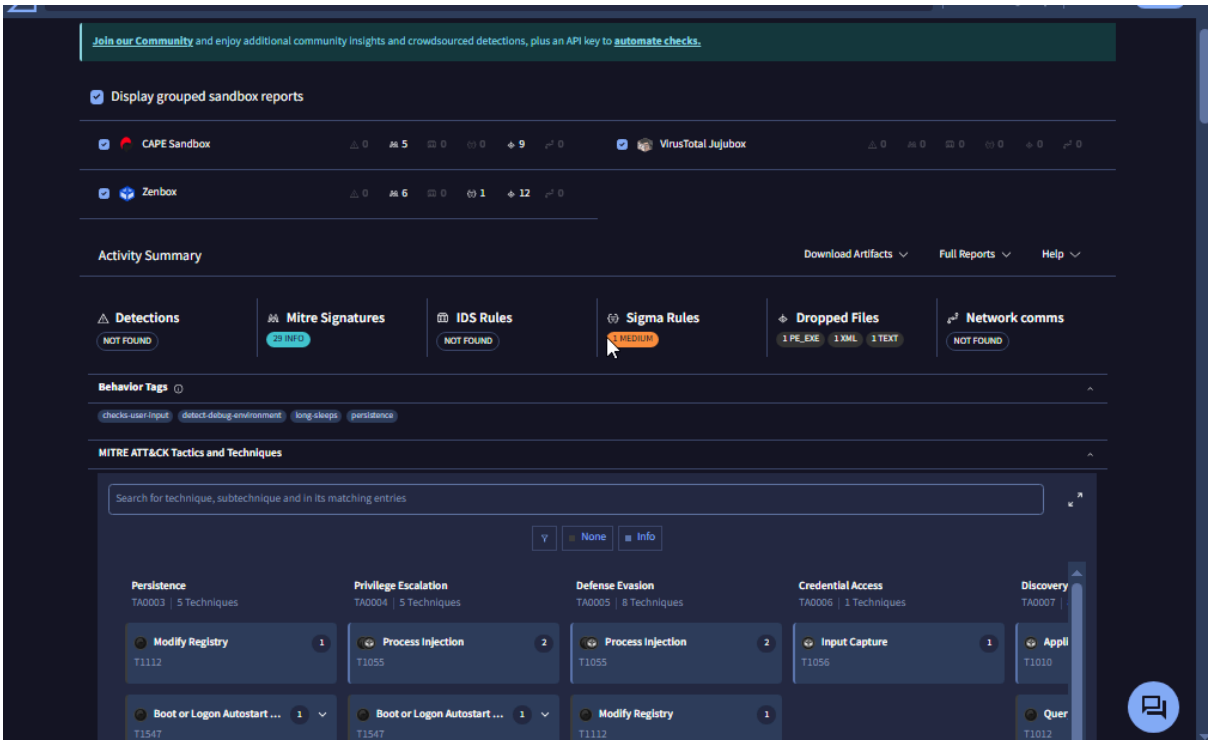
L'analyse permet de conclure qu'il ne s'agit pas d'une menace nouvelle, mais d'un malware déjà référencé. La forte détection par les moteurs antivirus, la classification récurrente comme keylogger et la correspondance avec des comportements MITRE ATT&CK connus confirment qu'il s'agit d'une menace connue et documentée.

Validation des critères d'acceptation

- **Hash calculé** : Validé
- **Résultats de détection documentés** : Validé
- **Comparaison avec bases existantes** : Validé




Security vendors' analysis
Do you want to automate checks?
Alibaba
ALYac
Avast
Avira (no cloud)
CTX
Deepinstinct
Emsisoft
ESET-NOD32
GData
Huorong
Jiangmin
K7GW
Kingsoft
Malwarebytes
NANO-Antivirus
QuickHeal
Sangfor Engine Zero
Sophos
Tencent
TrendMicro
Varist
VirIT
WithSecure
Zoner
AhnLab-V3
ABCloud
Arcabit
AVG
BitDefender
Cynet
DrWeb
eScan
Fortinet
Google
Ikarus
K7AntiVirus
Kaspersky
Lionic
MaxSecure
Panda
Rising
SkyHigh (SWG)
Symantec
Trellix ENS
TrendMicro-HouseCall
VIPRE
Webroot
Zillya
Acronis (Static ML)
Antiy-AVL
Undetected


Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Display grouped sandbox reports
CAPE Sandbox
VirusTotal Jujubox
Zenbox
Activity Summary
Download Artifacts
Full Reports
Help
Detections
NOT FOUND
Mitre Signatures
29 INFO
IDS Rules
NOT FOUND
Sigma Rules
1 MEDIUM
Dropped Files
1 PE_EXE
1 XML
1 TEXT
Network comms
NOT FOUND
Behavior Tags
checks-user-input
detect-debug-environment
long-sleeps
persistence
MITRE ATT&CK Tactics and Techniques
Search for technique, subtechnique and in its matching entries
None
Info
Persistence
TA0003 | 5 Techniques
Privilege Escalation
TA0004 | 5 Techniques
Defense Evasion
TA0005 | 8 Techniques
Credential Access
TA0006 | 1 Techniques
Discovery
TA0007
Modify Registry
T1112
Process Injection
T1055
Process Injection
T1055
Input Capture
T1056
Boot or Logon Autostart ...
T1547
Boot or Logon Autostart ...
T1547
Modify Registry
T1112

US 3:Analyse statique
EN TANT QUE reverse engineer,
JE VEUX analyser statiquement le malware,
AFIN DE comprendre sa structure, ses dépendances et ses fonctionnalités.

Critères d'acceptation :

- Fonctions principales identifiées
- Chaînes, imports, sections analysées
- Indicateurs de compromission extraits

Réflexion

Après l'exécution contrôlée du malware, il était nécessaire d'approfondir sa compréhension par une analyse statique détaillée. L'objectif était d'identifier les fonctions clés, les API utilisées, ainsi que les techniques de dissimulation mises en œuvre. Des outils spécialisés ont été retenus afin d'analyser la structure du binaire, ses chaînes de caractères, ses imports et ses sections, puis de confirmer ces éléments via un désassemblage plus poussé.

Ce que nous avons fait

Nous avons commencé par observer les effets généraux du malware sur la machine, notamment une forte utilisation de la RAM et du processeur, entraînant un ralentissement du système, ce qui indique l'exécution de traitements intensifs en arrière-plan.

Ensuite, nous avons utilisé PEStudio pour analyser la structure du malware.
L'analyse des imports a montré une forte utilisation de la bibliothèque standard C++ (libstdc++), suggéSrant que le binaire a été compilé en C++ avec abstraction des appels système.

Analyse des chaînes

L'analyse des chaînes a révélé la présence d'appels à des API Windows sensibles, notamment :

- `VirtualProtect`

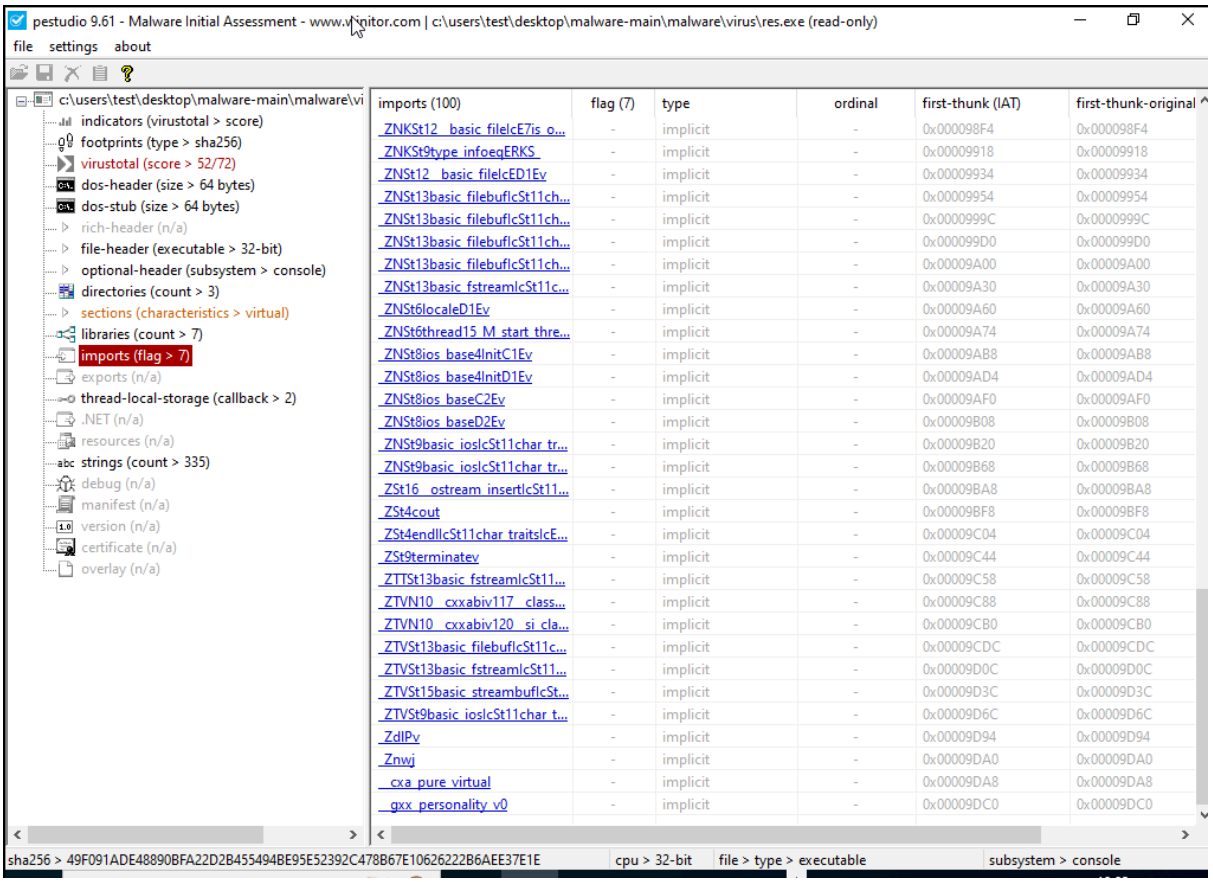
- `VirtualQuery`
- `GetAsyncKeyState`
- `GetKeyState`

Analyse des imports

L'analyse des imports montre une utilisation quasi exclusive de bibliothèques standard C++, sans appel direct aux API Windows critiques. Cette absence d'imports explicites confirme une stratégie visant à dissimuler les dépendances système et à rendre l'analyse statique plus complexe.

Analyse des sections

Le binaire est composé de huit sections, avec une entropie globalement proche de 5. L'absence de sections à entropie élevée nous montre que la dissimulation repose davantage sur des techniques logicielles .



ascii	17	0x000053E4	x	GetCurrentProcess
ascii	19	0x000053F8	x	GetCurrentProcessId
ascii	18	0x0000540E	x	GetCurrentThreadId
ascii	14	0x00005558	x	VirtualProtect
ascii	12	0x0000556A	x	VirtualQuery
ascii	16	0x000056C6	x	GetAsyncKeyState
ascii	11	0x000056DA	x	GetKeyState

Nous avons ensuite utilisé IDA afin d'analyser le malware plus en profondeur.
Grâce à l'analyse du fichier .res, nous avons constaté que lors de l'exécution, le malware copie son propre dossier dans un autre emplacement du système afin de se dissimuler et de créer une mécanisme de persistance

```
_rdata          segment para public 'DATA' use32
                assume cs:_rdata
                ;org 405000h
aLibgcc_s_dw21_ db 'libgcc_s_dw2-1.dll',0 ; DATA XREF: .text:0040150F↑o
                                          ; .text:00401525↑o
a__register_fra db '__register_frame_info',0 ; DATA XREF: .text:00401540↑o
a__deregister_f db '__deregister_frame_info',0 ; DATA XREF: .text:00401558↑o
aLibgcj16_dll   db 'libgcj-16.dll',0    ; DATA XREF: .text:0040158B↑o
a_jv_registercl db '_Jv_RegisterClasses',0 ; DATA XREF: .text:004015A0↑o
                align 4
aCWindsystLog_t db 'c:\WindSyst\log.txt',0 ; DATA XREF: sub_401640+14A↑o
aMkdirCWindsyst db 'mkdir c:\WindSyst',0 ; DATA XREF: sub_401AA0+26↑o
                align 4
aXcopyLibgcc_s_ db 'XCOPY libgcc_s_dw2-1.dll c:\WindSyst /S',0
                                          ; DATA XREF: sub_401AA0+32↑o
aXcopyLibstdc6_ db 'XCOPY libstdc++-6.dll c:\WindSyst /S',0
                                          ; DATA XREF: sub_401AA0+3E↑o
                align 4
```

.

L'analyse du fichier .env a révélé la configuration d'un serveur de messagerie, avec un nom d'utilisateur et un mot de passe, permettant l'envoi automatique du fichier log.txt vers une adresse email contrôlée par l'attaquant via `smtp.gmail.com` dès l'exécution du binaire.

```
lea     eax, [ebp+var_28]
mov     [esp+270h+var_260], 0FFFFFFFFh
mov     [esp+270h+var_264], 0
mov     [esp+270h+var_268], offset aSmtp_gmail_com ; "smtp.gmail.co
mov     [esp+270h+var_26C], offset aMainwindow_0 ; "MainWindow"
mov     [esp+270h+var_270], eax
call    esi ; _ZN16QCoreApplication9translateEPKcS1_S1_i
lea     eax, [ebp+var_28]
mov     ecx, [ebx+28h]
mov     edi, ds:_ZN9QLineEdit7setTextERK7QString
mov     [esp+270h+var_270], eax
call    edi ; _ZN9QLineEdit7setTextERK7QString
mov     eax, [ebp+var_28]
sub     esp, 4
mov     edx, [eax]
test    edx, edx
jz      loc_407515
cmp     edx, 0FFFFFFFFh
jz      short loc_406F99
lock sub     dword ptr [eax], 1
jz      loc_407512
```

Enfin, l'analyse a permis d'identifier que l'origine du malware est située en Chine.

Ce que nous avons obtenu

L'analyse statique a permis d'identifier les fonctions principales du malware : capture des frappes clavier, mécanismes de persistance, dissimulation via résolution dynamique des API et exfiltration de données par email. Les chaînes, imports et sections confirment une conception visant à compliquer l'analyse et à masquer les intentions malveillantes. Ces éléments constituent des indicateurs de compromission clairs et démontrent que le malware est un keylogger structuré, conçu pour surveiller l'utilisateur et exfiltrer des données sensibles.

Validation des critères d'acceptation

- **Fonctions principales identifiées** : Validé
- **Chaînes, imports et sections analysés** : Validé
- **Indicateurs de compromission extraits** : Validé

US 4:Analyse dynamique
EN TANT QUE analyste dynamique,
JE VEUX observer le comportement du malware à l'exécution,
AFIN DE comprendre ses actions réelles sur le système.
Critères d'acceptation :

- Modifications système observées
- Activités réseau identifiées
- Création de fichiers / processus détectée

Réflexion

Après avoir identifié les capacités potentielles du malware lors de l'analyse statique, il était nécessaire de vérifier son comportement réel en conditions d'exécution. L'objectif était d'observer les effets du malware sur les performances du système et d'identifier les modifications apportées au système de fichiers.

Ce que nous avons fait

Nous avons exécuté le malware dans l'environnement isolé précédemment mis en place et observé le comportement du système pendant son exécution. Une surveillance des performances a permis de constater une surcharge du processeur, accompagnée d'une latence élevée et d'une surchauffe du système, traduisant une dégradation notable des performances de la machine.Nous avons également analysé les modifications apportées au système de fichiers. L'exécution du malware entraîne la création d'un dossier nommé « Windsyst » dans le répertoire système de Windows. Ce dossier est distinct du fichier malveillant initial présent sur le bureau.À l'intérieur de ce dossier, un fichier supplémentaire de type log ("log.txt") a été identifié. Ce fichier n'était pas présent dans le dossier téléchargé.

Ce que nous avons obtenu

L'analyse du contenu du fichier log a permis de constater qu'il enregistre l'ensemble des frappes clavier saisies par l'utilisateur. Chaque action de saisie est consignée dans ce fichier, ce qui confirme que le malware agit comme un keylogger.Ces observations démontrent la création de fichiers malveillants persistants sur le système ainsi que l'impact concret du malware sur les performances de la machine.

Validation des critères d'acceptation

- **Modifications système observées** : surcharge du processeur, latence, surchauffe – Validé

- **Activités réseau identifiées** : Non observées

- **Création de fichiers / processus détectée** : création du dossier *Windsyst* et du fichier *log* – Validé

US 5:Évaluation des risques
EN TANT QUE responsable sécurité,
JE VEUX évaluer l'impact du malware sur la machine,
AFIN DE définir des mesures de mitigation adaptées.

Critères d'acceptation :

- Description claire des impacts
- Niveau de risque évalué
- Recommandations de sécurité formulées

Ce que nous avons fait

Nous avons analysé les capacités du malware et ses effets concrets sur la machine. Il a été constaté que le malware agit comme un keylogger, capturant les frappes clavier de l'utilisateur. Ce comportement expose directement les identifiants, mots de passe et autres données sensibles.Nous avons également observé une dégradation des performances du système, avec un ralentissement global rendant la machine instable et difficilement utilisable. Par ailleurs, les informations collectées sont envoyées vers un serveur de messagerie et une adresse email contrôlée par l'attaquant situé en chine.

Ce que nous avons obtenu

Au regard de la nature du malware et de ses capacités de surveillance et d'exfiltration, nous pensons que le niveau de risque est évalué comme élevé. La compromission potentielle des identifiants et des données sensibles représente une menace majeure pour la sécurité de l'utilisateur et de l'environnement associé. Nous pensons qu'il est recommandé d'isoler immédiatement la machine infectée, de procéder à une suppression complète du malware, puis de réinitialiser l'ensemble des identifiants susceptibles d'avoir été compromis.

Validation des critères d'acceptation

- **Description claire des impacts** : Validé
- **Niveau de risque évalué** : Risque élevé – Validé
- **Recommandations de sécurité formulées** : Validé

US 6:Acquisition mémoire vive
EN TANT QUE analyste forensic,
JE VEUX réaliser un dump de la mémoire vive du système,
AFIN DE détecter des processus malveillants ou des traces d'attaque en mémoire.

Critères d'acceptation :

- Les outils/commandes utilisés.
- Le dump RAM est complet et exploitable
- Les processus actifs sont identifiés • Les connexions réseau suspectes sont relevées

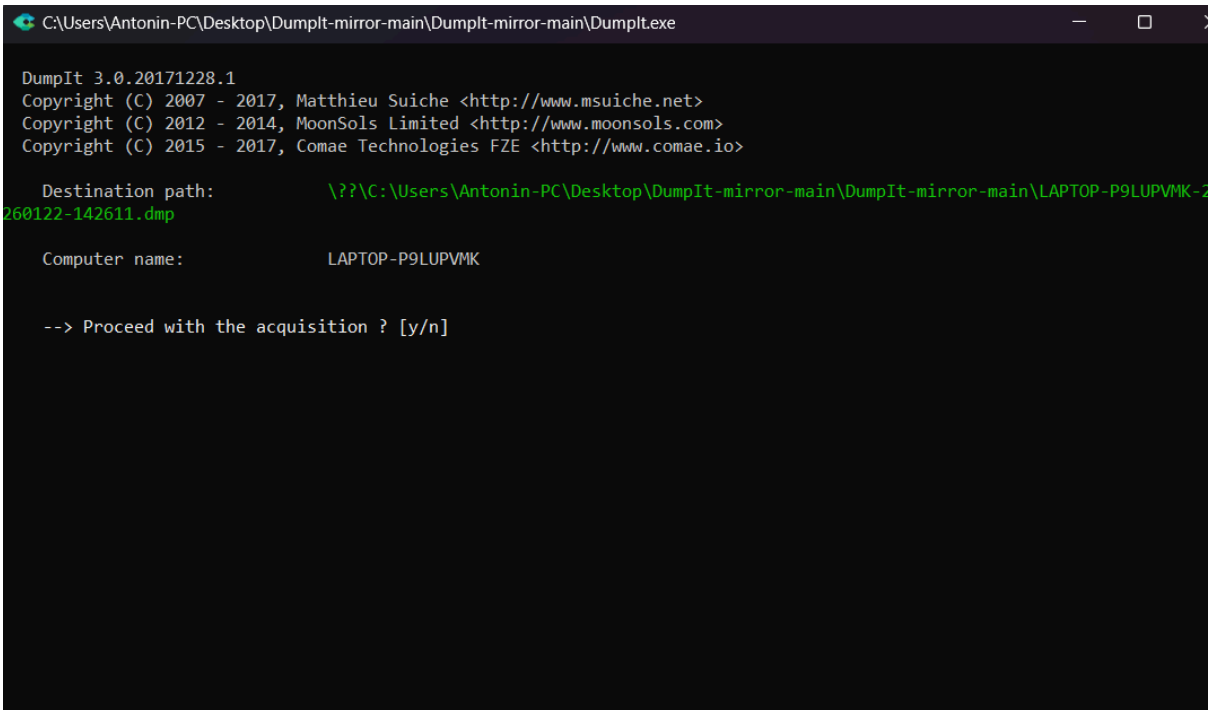
Réflexion

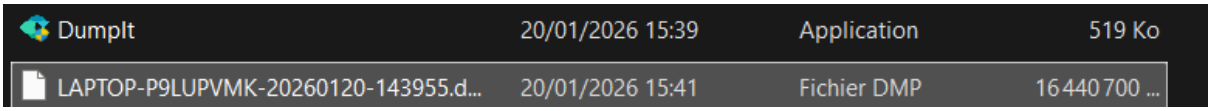
L'utilisation d'un outil reconnu et la vérification de l'exploitabilité du dump mémoire étaient indispensables pour s'assurer que les données collectées puissent être utilisées efficacement avec des outils d'analyse spécialisés. Nous avons donc utilisé DumpIT.

Ce que nous avons fait

Nous avons commencé par installer l'outil DumpIt v3.0. L'exécution du fichier `DumpIt.exe` a permis de générer un dump complet de la RAM du système.

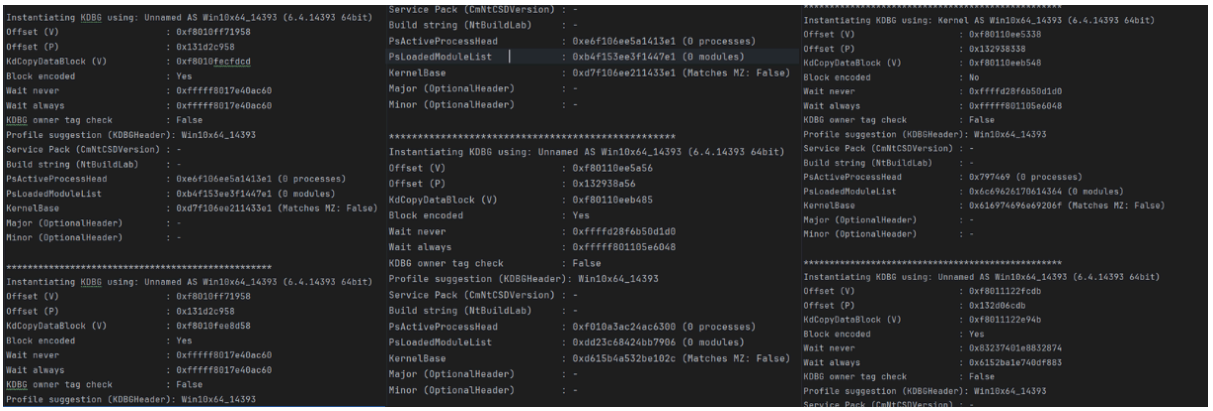
À la fin du processus, un fichier DMP et un fichier JSON sont crées :





Nous avons ensuite analysé ce dump à l'aide de Volatility, en utilisant la commande `kdbgscan`. Cette étape avait pour but d'identifier les structures noyau KDBG et de déterminer le profil Windows compatible avec l'image mémoire.

.\volatility.exe -f "C:\Users\Antonin-PC\Desktop\DumpIt-mirror-main\DumpIt-mirror-main\LAPTOP-P9LUPVMK-20260120-143955.dmp" kdbgscan



Ce que nous avons obtenu

L'exécution de la commande `kdbgscan` a permis d'identifier plusieurs structures KDBG compatibles avec un système Windows 10 x64. Les résultats confirment que le dump mémoire est exploitable pour une analyse forensic approfondie, comme pour l'étude des processus actifs, des modules chargés et des artefacts en mémoire.

Validation des critères d'acceptation

- Mémoire vive acquise avec succès : Validé
- Intégrité du dump garantie (SHA-256) : Validé
- Exploitabilité du dump confirmée avec Volatility : Validé

US 7:Acquisition du disque dur
EN TANT QUE analyste securité,
JE VEUX effectuer une image disque forensique,
AFIN DE analyser les fichiers, la persistance et les traces laissées par un attaquant.

Critères d'acceptation :

- Image disque bit-à-bit réalisée
- Les outils utilisés.
- Fichiers suspects identifiés

Réflexion

Nous avons donc utiliser un outil capable de réaliser une image bit-à-bit du disque, incluant l'espace alloué et non alloué. Le choix d'un format forensique standard, accompagné du calcul de hash cryptographiques, permet d'assurer la fidélité de l'acquisition et sa recevabilité dans un cadre d'investigation. Une fois l'image créée, un outil d'analyse forensique devait permettre de détecter automatiquement des fichiers suspects, notamment ceux présentant une entropie élevée, souvent associée à des contenus chiffrés ou obfusqués.

Ce que nous avons fait

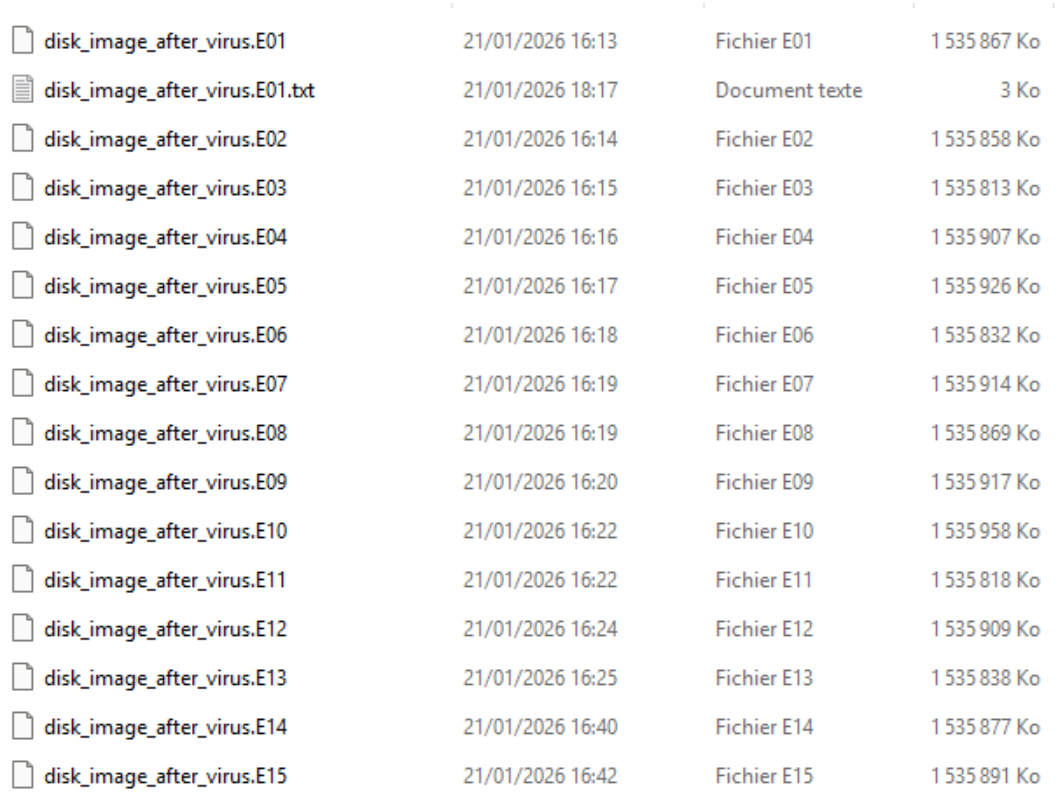
1. Acquisition disque

Nous avons d'abord recherché les outils adaptés à l'acquisition et à l'analyse forensique. Nous avons sélectionné FTK Imager pour l'acquisition disque et Autopsy pour l'analyse.

Les étapes réalisées avec FTK Imager sont les suivantes :

- Lancement de FTK Imager en mode administrateur
- Sélection de *File → Create Disk Image*
- Choix du type *Physical Drive* (disque entier)
- Sélection du disque source
- Choix du format E01
- Activation des calculs de hash MD5 et SHA-256
- Sélection du disque de destination
- Lancement de l'acquisition

Cette procédure a permis de générer plusieurs images disque, dont une contenant le malware.



disk_image_after_virus.E01	21/01/2026 16:13	Fichier E01	1 535 867 Ko
disk_image_after_virus.E01.txt	21/01/2026 18:17	Document texte	3 Ko
disk_image_after_virus.E02	21/01/2026 16:14	Fichier E02	1 535 858 Ko
disk_image_after_virus.E03	21/01/2026 16:15	Fichier E03	1 535 813 Ko
disk_image_after_virus.E04	21/01/2026 16:16	Fichier E04	1 535 907 Ko
disk_image_after_virus.E05	21/01/2026 16:17	Fichier E05	1 535 926 Ko
disk_image_after_virus.E06	21/01/2026 16:18	Fichier E06	1 535 832 Ko
disk_image_after_virus.E07	21/01/2026 16:19	Fichier E07	1 535 914 Ko
disk_image_after_virus.E08	21/01/2026 16:19	Fichier E08	1 535 869 Ko
disk_image_after_virus.E09	21/01/2026 16:20	Fichier E09	1 535 917 Ko
disk_image_after_virus.E10	21/01/2026 16:22	Fichier E10	1 535 958 Ko
disk_image_after_virus.E11	21/01/2026 16:22	Fichier E11	1 535 818 Ko
disk_image_after_virus.E12	21/01/2026 16:24	Fichier E12	1 535 909 Ko
disk_image_after_virus.E13	21/01/2026 16:25	Fichier E13	1 535 838 Ko
disk_image_after_virus.E14	21/01/2026 16:40	Fichier E14	1 535 877 Ko
disk_image_after_virus.E15	21/01/2026 16:42	Fichier E15	1 535 891 Ko

2. Analyse forensique

L'image disque contenant le malware a ensuite été analysée avec **Autopsy**. Lors de l'analyse, nous avons consulté le panneau de gauche, dans la rubrique **Analysis Results → Encryption Suspected**.

Un fichier suspect y a été identifié avec les caractéristiques suivantes :

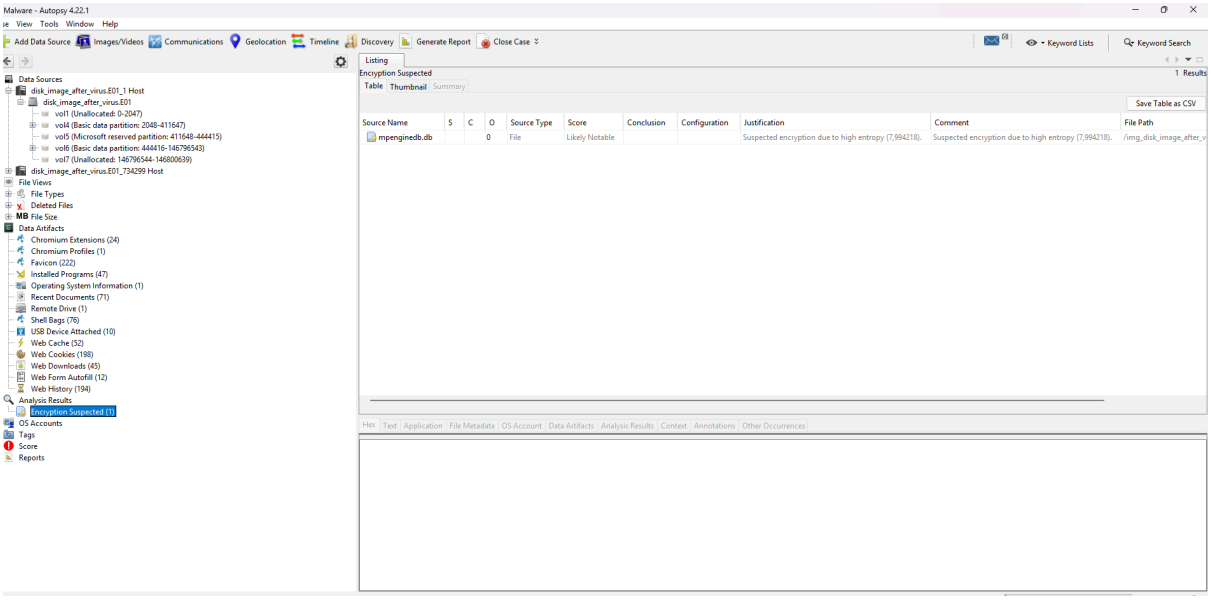
- Source type : *File*
- Score : *Likely notable*
- Justification : *Suspected encryption due to high entropy (7.994218)*
- Commentaire : *Suspected encryption due to high entropy (7.994218)*

Cette entrée indique la présence d'un fichier présentant une entropie très élevée, caractéristique d'un contenu potentiellement chiffré ou dangereux.

Ce que nous avons obtenu

L’acquisition disque bit-à-bit a été réalisée avec succès, en garantissant l’intégrité des données grâce aux hash MD5 et SHA-256. L’analyse forensique de l’image disque a permis d’identifier un fichier suspect signalé comme Encryption Suspected, avec une entropie proche de 8.

Cet élément constitue une preuve tangible de l’activité malveillante sur le disque et confirme la présence de fichiers liés à l’attaque, potentiellement utilisés pour la dissimulation ou la persistance du malware.



Validation des critères d’acceptation

- **Image disque bit-à-bit réalisée** : Validé
- **Intégrité de l’image vérifiée (MD5 / SHA-256)** : Validé

- **Fichiers suspects identifiés via analyse forensique** : Validé

US 8:Analyse croisée RAM / disque
EN TANT QUE analyste SOC,
JE VEUX corréler les données mémoire et disque,
AFIN DE reconstruire un scénario d'attaque cohérent.

Critères d'acceptation :

- Correspondance entre processus mémoire et fichiers disque
- Détection d'éventuelle persistance

Réflexion

L'analyse mémoire et l'analyse disque, prises séparément, fournissent des informations partielles. Leur corrélation permet en revanche de reconstruire un scénario temporel et fonctionnel de l'attaque.

Ce que nous avons fait

Nous avons comparé les résultats de l'analyse disque (Autopsy) et de l'analyse mémoire (DumpIt + Volatility).

- Le fichier suspect identifié sur le disque, présentant une entropie élevée, était présent sur le système avant et pendant l'acquisition mémoire.

- Le dump RAM ayant été réalisé après l'infection, ce fichier faisait partie de l'environnement du système au moment de l'acquisition.

Cependant, la cohérence entre :

- la présence du fichier suspect sur le disque,

- l'état actif du système lors de l'acquisition mémoire,

- et les artefacts forensiques observés,

permet d'établir que ce fichier était susceptible d'être chargé ou exécuté en mémoire.

Ce que nous avons obtenu

L'analyse croisée RAM / disque a permis de reconstruire un scénario d'attaque cohérent, malgré les limitations techniques liées aux outils. Les éléments collectés indiquent que :

- le fichier suspect identifié sur le disque était présent et potentiellement actif en mémoire;
- l’infection était active ou récente au moment de l’acquisition ;
- un mécanisme de persistance est plausible, renforçant la gravité de la compromission.

Il y a donc une activit malveillante constante sur le système.

Validation des critères d’acceptation

- Corrélation entre artefacts disque et mémoire réalisée : Validé
- Reconstruction d’un scénario d’attaque cohérent : Validé
- Identification d’un potentiel mécanisme de persistance : Validé

US 9 :Identification de la clé USB utilisée
EN TANT QUE analyste forensic,
JE VEUX identifier l'UID / numéro de série de la clé USB utilisée sur le poste compromis,
AFIN DE relier le périphérique à un collaborateur ou à un événement précis de fuite de données.

Critères d'acceptation :

- Le numéro de série unique (USB Serial / UID) est extrait

Ce que nous avons fait

Nous avons utilisé l'outil Registry Explorer pour analyser la ruche SYSTEM du système compromis.

Les étapes réalisées sont les suivantes :

- Installation de Registry Explorer
- Chargement de la ruche SYSTEM via l'option *Load Hive*
- Navigation dans le registre au chemin suivant :
  `SYSTEM\ControlSet001\Enum\USBSTOR`

Cette analyse a permis d'identifier un périphérique de stockage USB précédemment connecté à la machine.

Ce que nous avons obtenu

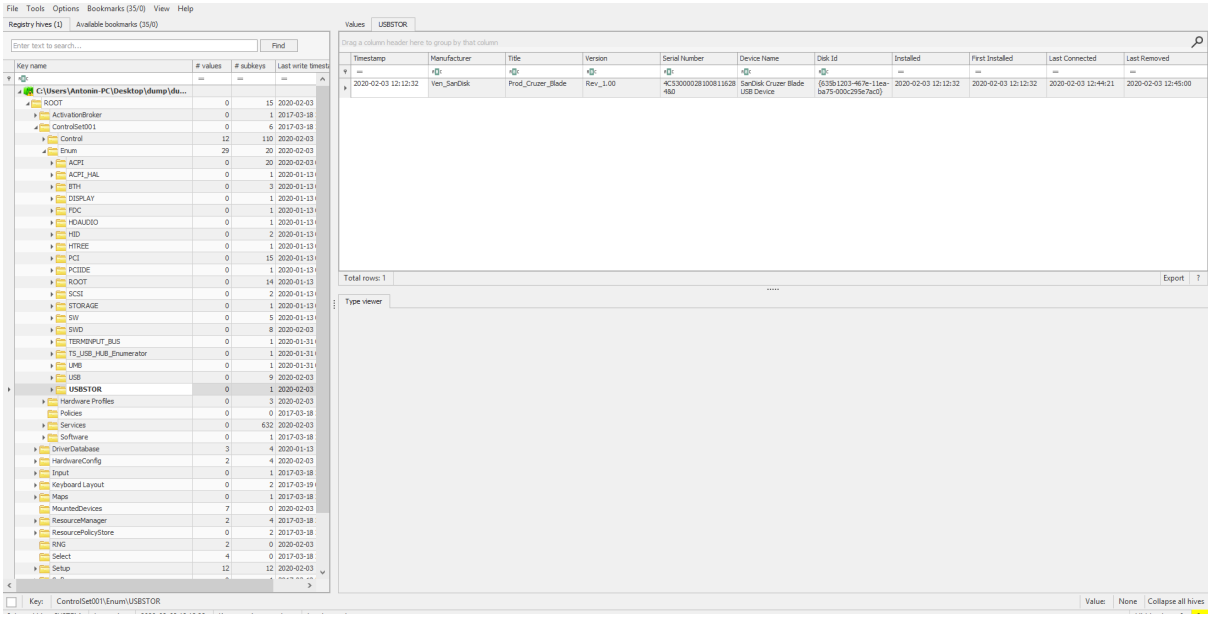
L'analyse du registre a permis d'identifier une clé USB de type SanDisk Cruzer Blade.
Le numéro de série unique (USB Serial / UID) extrait est le suivant :

4C530000281008116284

Cet identifiant permet de relier de façon fiable cette clé USB à l'incident de fuite de données.

Validation des critères d'acceptation

- Numéro de série USB extrait : Validé


File Tools Options Bookmarks (35/0) View Help
Registry hives (1) Available bookmarks (35/0)
Enter text to search...
Find
Key name # values # subkeys Last write timestamp
C:\Users\Antonin-PC\Desktop\dump\dump
ROOT 0 15 2020-02-03
ActivationBroker 0 1 2017-03-18
ControlSet001 0 6 2017-03-18
Control 12 110 2020-02-03
Enum 29 20 2020-02-03
ACPI 0 20 2020-02-03
ACPI_HAL 0 1 2020-01-13
BTH 0 3 2020-01-13
DISPLAY 0 1 2020-01-13
FDC 0 1 2020-01-13
HDAUDIO 0 1 2020-01-13
HID 0 2 2020-01-13
HTREE 0 1 2020-01-13
PCI 0 15 2020-01-13
PCIIDE 0 1 2020-01-13
ROOT 0 14 2020-01-13
SCSI 0 2 2020-01-13
STORAGE 0 1 2020-01-13
SW 0 5 2020-01-13
SWD 0 8 2020-02-03
TERMINPUT_BUS 0 1 2020-01-31
TS_USB_HUB_Enumerator 0 1 2020-01-31
UMB 0 1 2020-01-31
USB 0 9 2020-02-03
USBSTOR 0 1 2020-02-03
Hardware Profiles 0 3 2020-02-03
Policies 0 0 2017-03-18
Services 0 632 2020-02-03
Software 0 1 2017-03-18
DriverDatabase 3 4 2020-01-13
HardwareConfig 2 4 2020-02-03
Input 0 1 2017-03-18
Keyboard Layout 0 2 2017-03-19
Maps 0 1 2017-03-18
MountedDevices 7 0 2020-02-03
ResourceManager 2 4 2017-03-18
ResourcePolicyStore 0 2 2017-03-18
RNG 2 0 2020-02-03
Select 4 0 2017-03-18
Setup 12 12 2020-02-03
Values USBSTOR
Drag a column header here to group by that column
Timestamp Manufacturer Title Version Serial Number Device Name Disk Id Installed First Installed Last Connected Last Removed
2020-02-03 12:12:32 Ven_SanDisk Prod_Cruzer_Blade Rev_1.00 4C530000281008116284 80 SanDisk Cruzer Blade USB Device {635b1203-467e-11ea-ba75-000c295e7ac0} 2020-02-03 12:12:32 2020-02-03 12:12:32 2020-02-03 12:44:21 2020-02-03 12:45:00
Total rows: 1 Export ?
Type viewer
Key: ControlSet001\Enum\USBSTOR Value: None Collapse all hives

US 10:Chronologie de la fuite
EN TANT QUE responsable sécurité,
JE VEUX déterminer quand la clé USB a été utilisée,
AFIN DE vérifier la concordance avec les dates supposées de fuite de données.

Critères d'acceptation :

- Horodatages exploitables (last connected, first install)
- Chronologie claire des événements

Timestamp	Manufacturer	Title	Version	Serial Number	Device Name	Disk Id	Installed	First Installed	Last Connected	Last Removed
=	abc	abc	abc	abc	abc	abc	=	=	=	=
2020-02-03 12:12:32	Ven_SanDisk	Prod_Cruzer_Blade	Rev_1.00	4C530000281008116284&0	SanDisk Cruzer Blade USB Device	{635b1203-467e-11ea-ba75-000c295e7ac0}	2020-02-03 12:12:32	2020-02-03 12:12:32	2020-02-03 12:44:21	2020-02-03 12:45:00

Réflexion

Windows conserve des métadonnées temporelles liées aux périphériques USB dans la ruche SYSTEM. L'exploitation des champs *First Installed* et *Last Connected* permet de reconstruire une chronologie fiable.

Ce que nous avons fait

Nous avons réalisé la même manipulation que pour l'US 9 à l'aide de Registry Explorer :

- Chargement de la ruche SYSTEM via *Load Hive*
- Navigation dans le registre au chemin suivant :
  `SYSTEM\ControlSet001\Enum\USBSTOR`
-

Nous avons ensuite analysé les colonnes temporelles associées à la clé USB identifiée, notamment :

- **First Installed**
- **Last Connected**

Ces informations ont été extraites et interprétées afin de reconstituer une chronologie des événements.

Ce que nous avons obtenu

Les horodatages collectés permettent d'établir la chronologie suivante :

Date / Heure	Événement
2020-02-03 12:12:32	Première installation de la clé USB
2020-02-03 12:44:21	Connexion de la clé USB
2020-02-03 12:45:00	Retrait de la clé USB

Cette chronologie est claire et exploitable. Elle permet de vérifier la concordance entre l'utilisation de la clé USB et les dates supposées de la fuite de données.

Validation des critères d'acceptation

- **Horodatages exploitables identifiés (First Install / Last Connected)** : Validé
- **Chronologie claire des événements établie** : Validé

	Timestamp	Manufacturer	Title	Version	Serial Number	Device Name	Disk Id	Installed	First Installed	Last Connected	Last Removed
	=	r□c	r□c	r□c	r□c	r□c	r□c	=	=	=	=
▸	2020-02-03 12:12:32	Ven_SanDisk	Prod_Cruzer_Blade	Rev_1.00	4C530000281008116284&0	SanDisk Cruzer Blade USB Device	{635b1203-467e-11ea-ba75-000c295e7ac0}	2020-02-03 12:12:32	2020-02-03 12:12:32	2020-02-03 12:44:21	2020-02-03 12:45:00