Rapport cyber

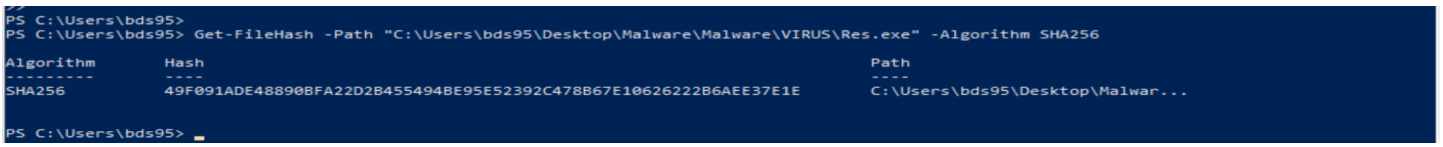
Partie 1:

Storie 1:

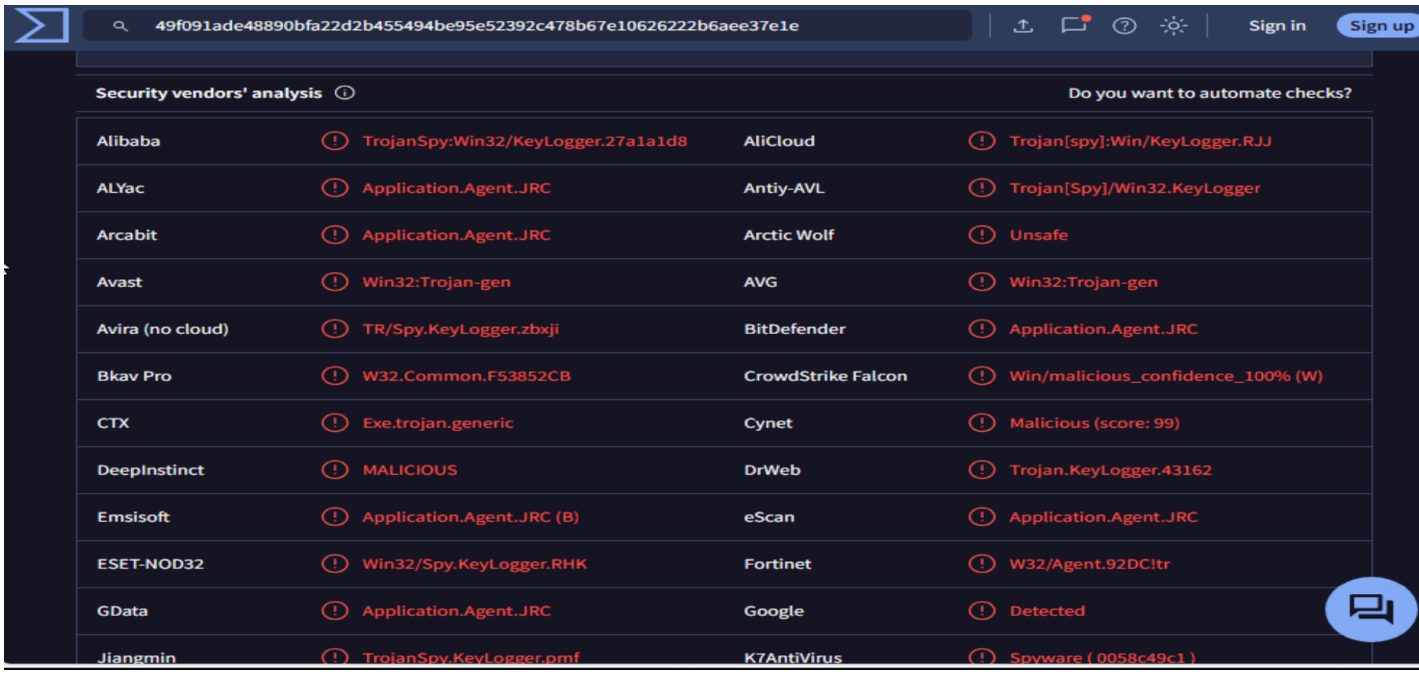
- Installer le malware
- dézipper le malware (attention : vérifier si on est bien en type Nat)
- double clique sur res pour le lancer
- gestionnaire des tâche, se met en arrière plan

Storie 2 :

- Pour récupérer l'empreinte unique du fichier suspect, on tape la commande : “ `Get-FileHash -Path “C:\User\bds95\Desktop\Malware\Malware\VIRUS\Res.exe” -Algorithm SHA256`”
- on copie le hash



- on le met dans VirusTotal.com et on le compare avec les bases existante


49f091ade48890bfa22d2b455494be95e52392c478b67e10626222b6aee37e1e
Sign in
Sign up
Security vendors' analysis
Do you want to automate checks?
Alibaba
TrojanSpy:Win32/KeyLogger.27a1a1d8
AliCloud
Trojan[spy]:Win/KeyLogger.RJJ
ALYac
Application.Agent.JRC
Antiy-AVL
Trojan[Spy]/Win32.KeyLogger
Arcabit
Application.Agent.JRC
Arctic Wolf
Unsafe
Avast
Win32:Trojan-gen
AVG
Win32:Trojan-gen
Avira (no cloud)
TR/Spy.KeyLogger.zbxji
BitDefender
Application.Agent.JRC
Bkav Pro
W32.Common.F53852CB
CrowdStrike Falcon
Win/malicious_confidence_100% (W)
CTX
Exe.trojan.generic
Cynet
Malicious (score: 99)
DeepInstinct
MALICIOUS
DrWeb
Trojan.KeyLogger.43162
Emsisoft
Application.Agent.JRC (B)
eScan
Application.Agent.JRC
ESET-NOD32
Win32/Spy.KeyLogger.RHK
Fortinet
W32/Agent.92DC!tr
GData
Application.Agent.JRC
Google
Detected
Jiangmin
TrojanSpy.KeyLogger.pmf
K7AntiVirus
Spyware (0058c49c1)

File *Res.exe*

Summary

Download | Resubmit sample

Size	24.5KB
Type	PE32 executable (console) Intel 80386 (stripped to external PDB), for MS Windows
MD5	d872a3086fbb82ed08a8322c028692dc
SHA1	af1d820e374ed50757dcde26bda069fa86b9b771
SHA256	49f091ade48890bfa22d2b455494be95e52392c478b67e10626222b6aee37e1e
SHA512	Show SHA512
CRC32	424B937B
ssdeep	None
Yara	• keylogger - Run a keylogger

Score

This file is **very suspicious**, with a score of **10 out of 10!**

Please notice: The scoring system is currently still in development and should be considered an ***alpha*** feature.

Feedback

Expecting different results? Send us this analysis and we will inspect it. Click here

HYBRID ANALYSIS

Request Info

Submission name:	Res.exe
Size:	25KiB
Type:	peexe executable
Mime:	application/x-dosexec
SHA256:	49f091ade48890bfa22d2b455494be95e52392c478b67e10626222b6aee37e1e
Submitted At:	2020-08-14 05:53:35 (UTC)
Last Anti-Virus Scan:	2026-01-15 15:04:32 (UTC)
Last Sandbox Report:	2024-03-05 14:47:58 (UTC)

malicious

Threat Score: 100/100
AV Detection: 63%
Labeled As: Win/malicious_confidence_100

Post | Link | E-Mail

0 Community Score 0

Anti-Virus Results

Updated 5 days ago - Click to Refresh

CrowdStrike Falcon
Static Analysis and ML
Malicious
(100%)
No Additional Data

MetaDefender
Multi Scan Analysis
Malicious
(7/26)
More Details

Storie 3 :

Étape 1 : Les Imports (Ce que le malware *sait* faire)

- **Installer pesStudio**
- **glisser/déposer le malware**
- **On va dans l'onglet "imports".**

- **Ce qu'on voit:**
  - `GetAsyncKeyState` et `GetKeyState` (marqués d'une croix rouge).
  - `VirtualProtect` et `VirtualQuery`.
  - `ZN10QArray`.
- **Ce que ça fait:**
  - `GetAsyncKeyState` : enregistre les touches du clavier pour voler des mots de passe.
  - `VirtualProtect` indique qu'il manipule la mémoire

Étape 2 : Indicateurs de compromission extraits

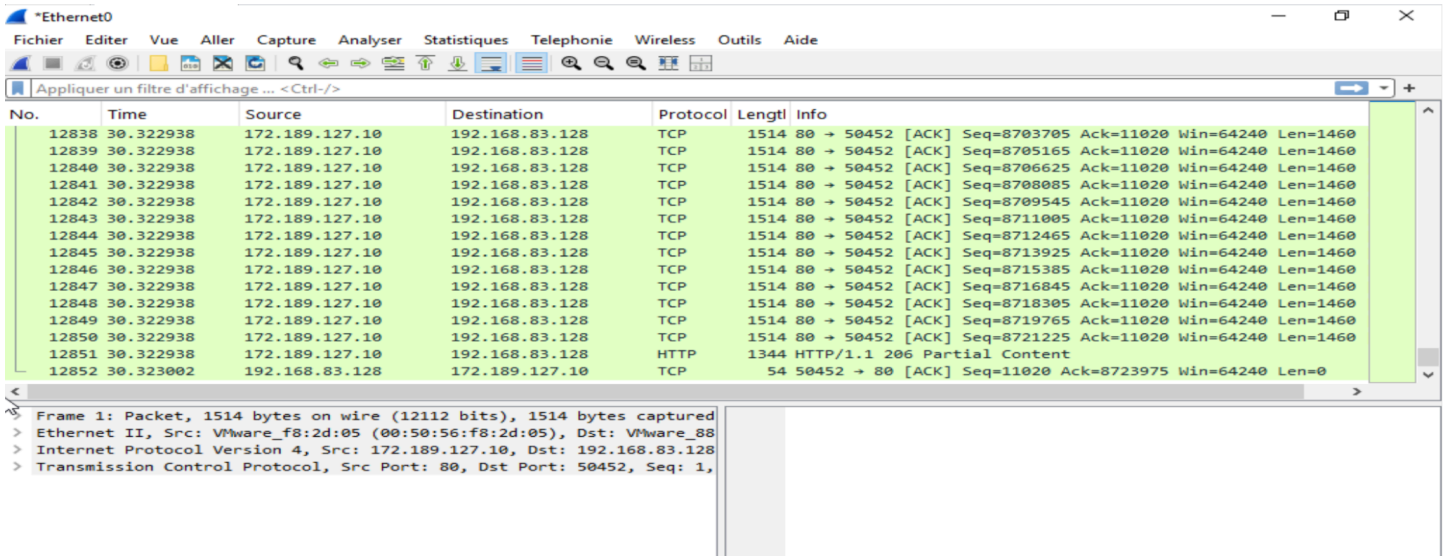
- **Ce qu'on voit :**
  - Le chemin complet : `c:\users\bds95\desktop\malware\malware\virus\res.exe`.
  - Type : `executable, 32-bit, console`.
  - Le nom du fichier est `res.exe`.
  - **VirusTotal > score : 52/72**.
  - **Entropy : 5.788**.

imports (100)	flag (7)	type	ordinal
DeleteCriticalSection	-	implicit	-
EnterCriticalSection	-	implicit	-
FreeLibrary	-	implicit	-
GetAsyncKeyState	x	implicit	-
GetConsoleWindow	-	implicit	-
GetCurrentProcess	x	implicit	-
GetCurrentProcessId	x	implicit	-
GetCurrentThreadId	x	implicit	-
GetKeyState	x	implicit	-
GetLastError	-	implicit	-
GetModuleHandleA	-	implicit	-
GetProcAddress	-	implicit	-
GetStartupInfoA	-	implicit	-
GetSystemTimeAsFileTime	-	implicit	-
GetTickCount	-	implicit	-
InitializeCriticalSection	-	implicit	-
LeaveCriticalSection	-	implicit	-
LoadLibraryA	-	implicit	-
QueryPerformanceCounter	-	implicit	-
SetUnhandledExceptionFilter	-	implicit	-
ShowWindow	-	implicit	-
Sleep	-	implicit	-
TerminateProcess	-	implicit	-
TlsGetValue	-	implicit	-
UnhandledExceptionFilter	-	implicit	-
VirtualProtect	x	implicit	-
VirtualQuery	x	implicit	-
_Unwind_Resume	-	implicit	-
_ZN10QArrayData10deallocateEPS_jj	-	implicit	-
_ZN16QCoreApplication4execEv	-	implicit	-
_ZN16QCoreApplicationC1ERiPPci	-	implicit	-

indicator (18)	detail
file > name	c:\users\bds95\desktop\malware\malware\virus\res.exe
file > signature	Microsoft Linker 2.25
file > sha256	49F091ADE48890BFA22D2B455494BE95E52392C478B67E10626222B6AEE3...
file > info	size: 25088 bytes, entropy: 5.788
file > type	executable, 32-bit, console
virustotal > permalink	https://www.virustotal.com/gui/file/49f091ade48890bfa22d2b455494be...
virustotal > scan-date	2025-03-19 10:45:50
virustotal > score	52/72
stamp > compiler	Fri Dec 22 12:02:53 2017
resource	n/a
thread-local-storage > callback	0x00002400 | 0x00002450
section > virtualized	name: .bss
entry-point > location	0x000014E0 (section: .text)
certificate	n/a
imports > flag	GetAsyncKeyState | GetCurrentProcess | GetCurrentProcessId | GetCurre...
imphash > md5	CF56E47F3329229BC9AD3C8DCA0D39F7
exports	n/a
overlay	n/a

Storie 4 :

- Installation de Wireshark, Process Monitor
- lancement de wireshark clique sur ethernet 0



- lancement de processus monitor > Filtrer  > dans les deux listes déroulantes on met “Process Name” et “Contains” et dans la 3ème (avant le then) on écrit re > Puis on appuie sur ok
- et on obtient ceci :

Il se cache (Dissimulation) : Dès l'exécution, il masque immédiatement sa fenêtre de console (écran noir) pour devenir invisible à l'utilisateur.

- appelle `GetConsoleWindow` et `ShowWindow` avec le paramètre `0` (SW_HIDE) pour **masquer la fenêtre de la console**

Il s'installe (Déploiement) : Il crée un dossier spécifique C:\WindSyst et y copie ses fichiers exécutables (Res.exe, Env.exe) ainsi que les bibliothèques nécessaires pour fonctionner.

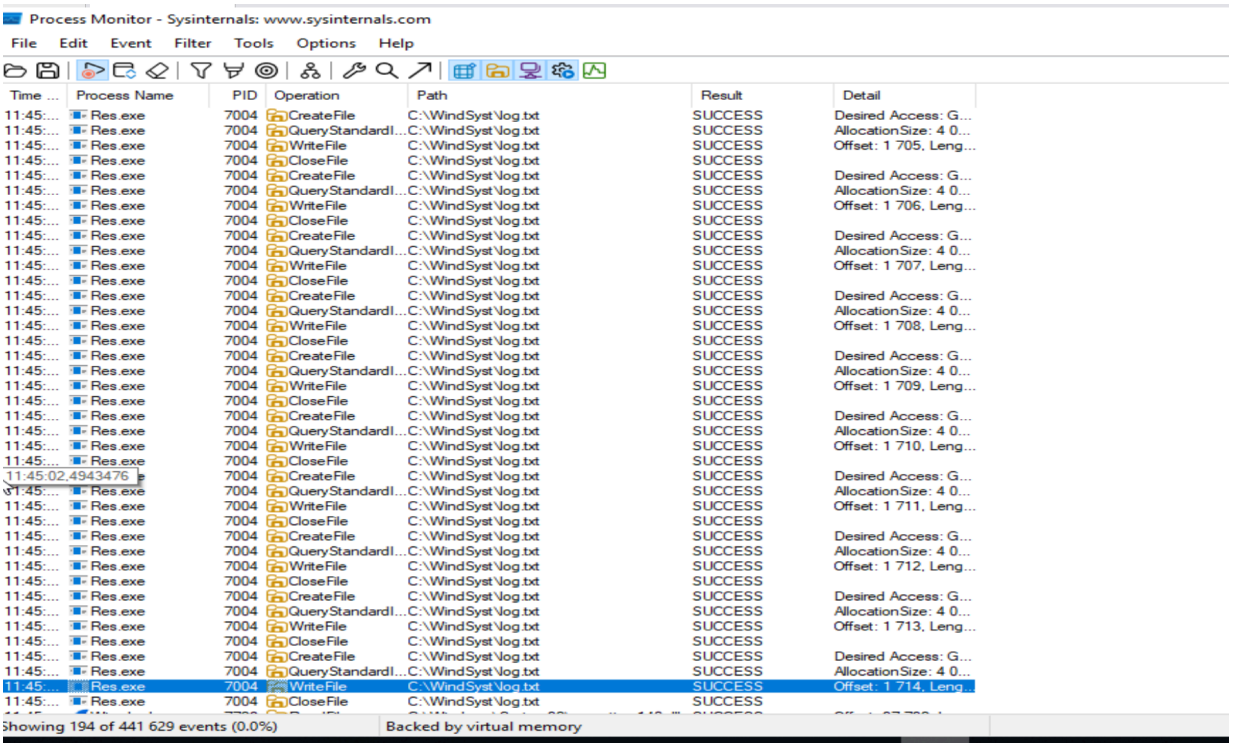
- **Création d'un répertoire caché :** `mkdir c:\\WindSyst`. Le malware crée un dossier à la racine du disque pour y stocker ses composants.

Il s'incruste (Persistance) : Il modifie le Registre Windows (Run) pour forcer le système à relancer le virus automatiquement à chaque démarrage de l'ordinateur.

- `HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Run (Cible)`. Il injecte deux valeurs nommées **"Res"** et **"Env"** pointant vers `C:\\WindSyst\\Res.exe` et `C:\\WindSyst\\Env.exe (Action)`. Le code utilise les classes du framework **Qt** (`QSettings`) pour modifier le Registre Windows.

Il espionne (Vol de données) : Il enregistre en continu toutes les touches frappées au clavier et sauvegarde le texte volé dans le fichier C:\WindSyst\log.txt.

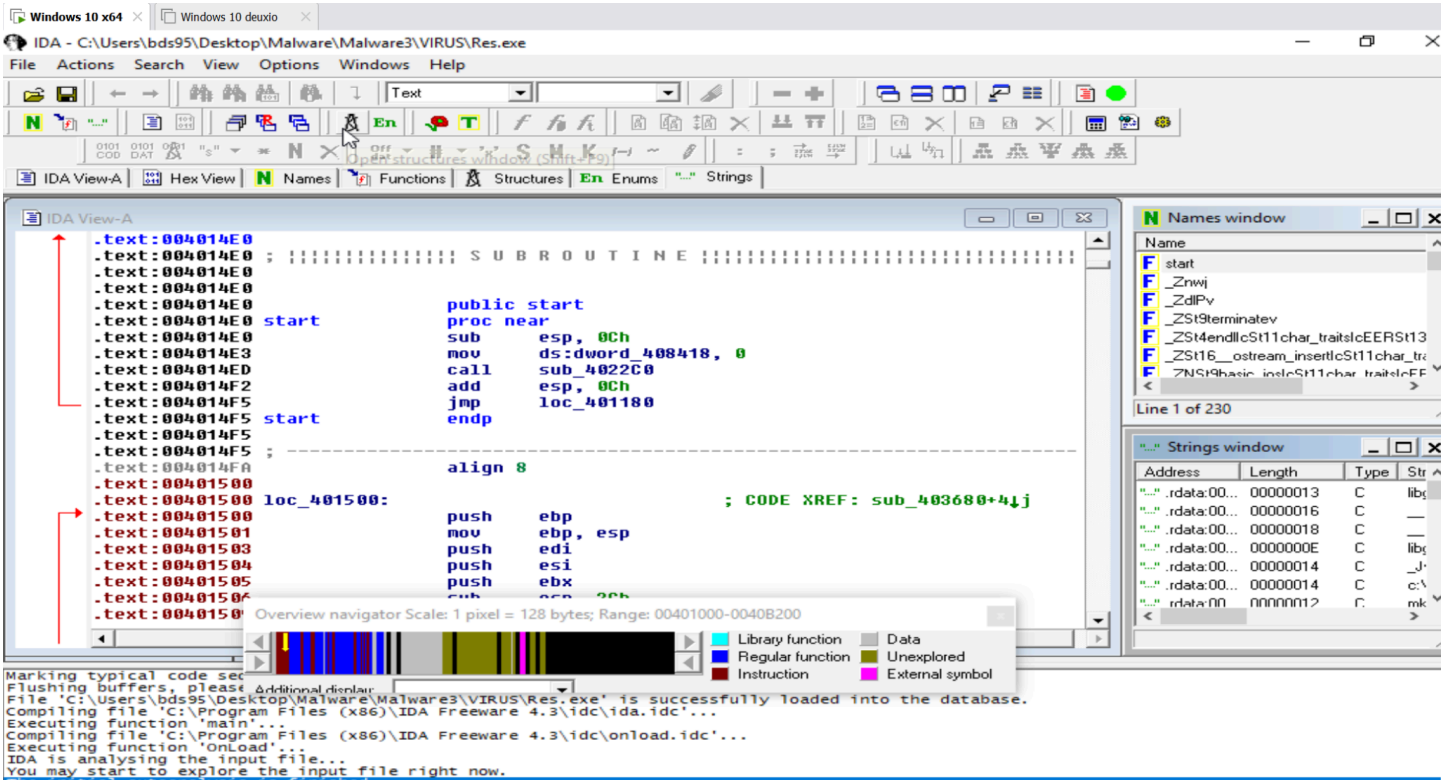
- **Capture :** Il utilise la fonction `GetAsyncKeyState` dans une boucle pour surveiller en temps réel chaque touche pressée sur le clavier.
- **Enregistrement :** Les données capturées sont écrites dans un fichier local nommé `c:\\WindSyst\\log.txt`.



Le malware est un keyLogger qui va créer un fichier log.txt dans le dossier WindSyst qui avec toutes les entrées clavier utilisé par l'utilisateur.

- installer IDA pro
- glisser le fichier res.exe

On obtient le code en assembleur du malware



Story 5:

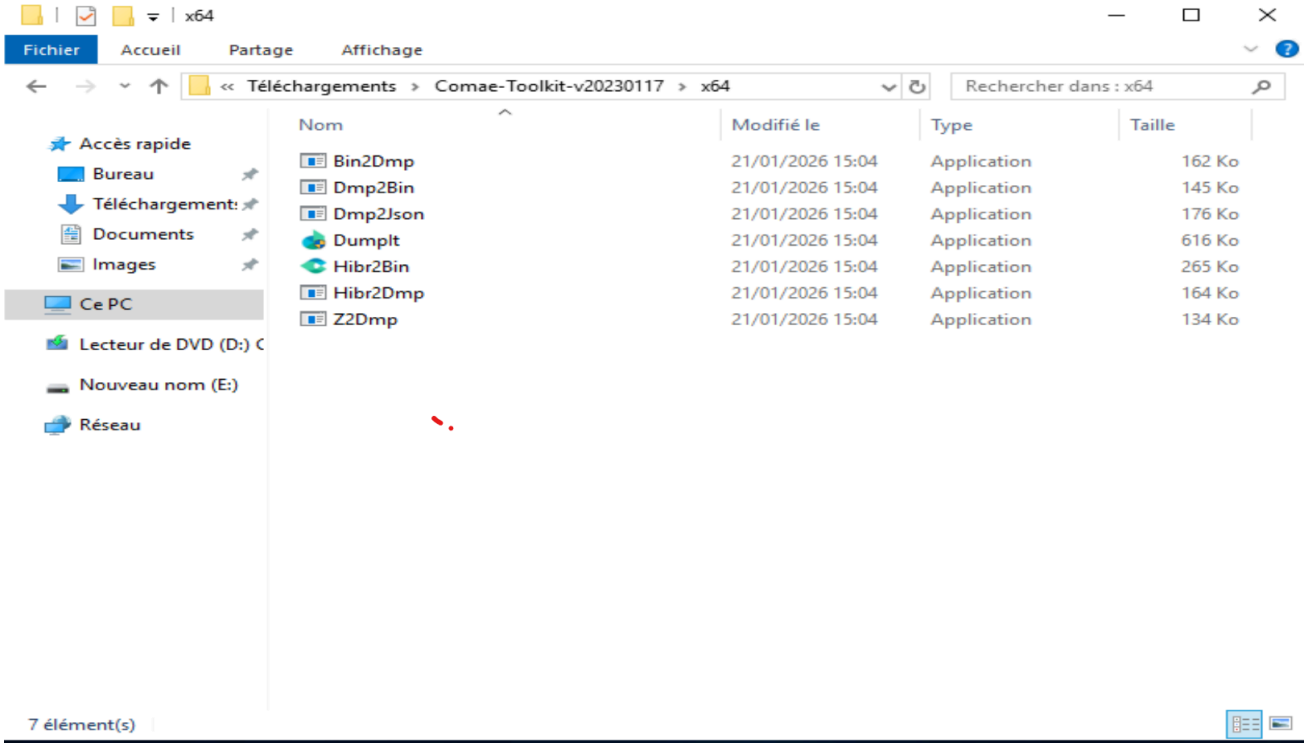
C'est un logiciel espion qui enregistre tout ce qui est tapé au clavier. Les conséquences sont le vol des mots de passe et des données bancaires.

Niveau de risque : malicieux (détecté par la majorité des antivirus).
Recommandations : Isoler la machine du réseau, réinstaller le système complètement et changer tous les mots de passe depuis un autre ordinateur."

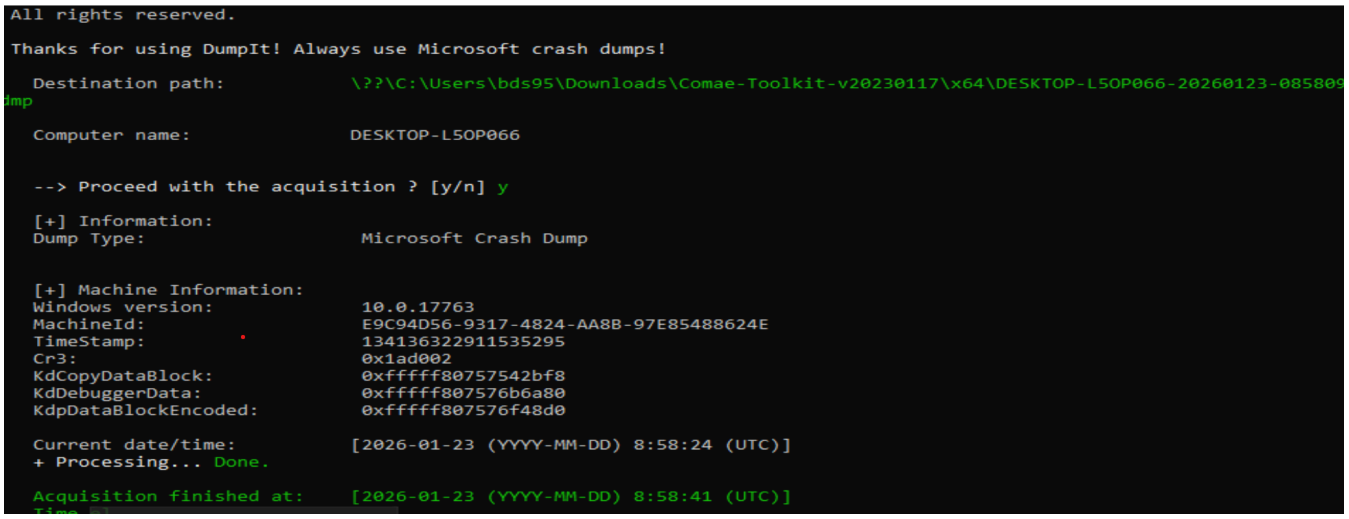
Partie 2

Story 6

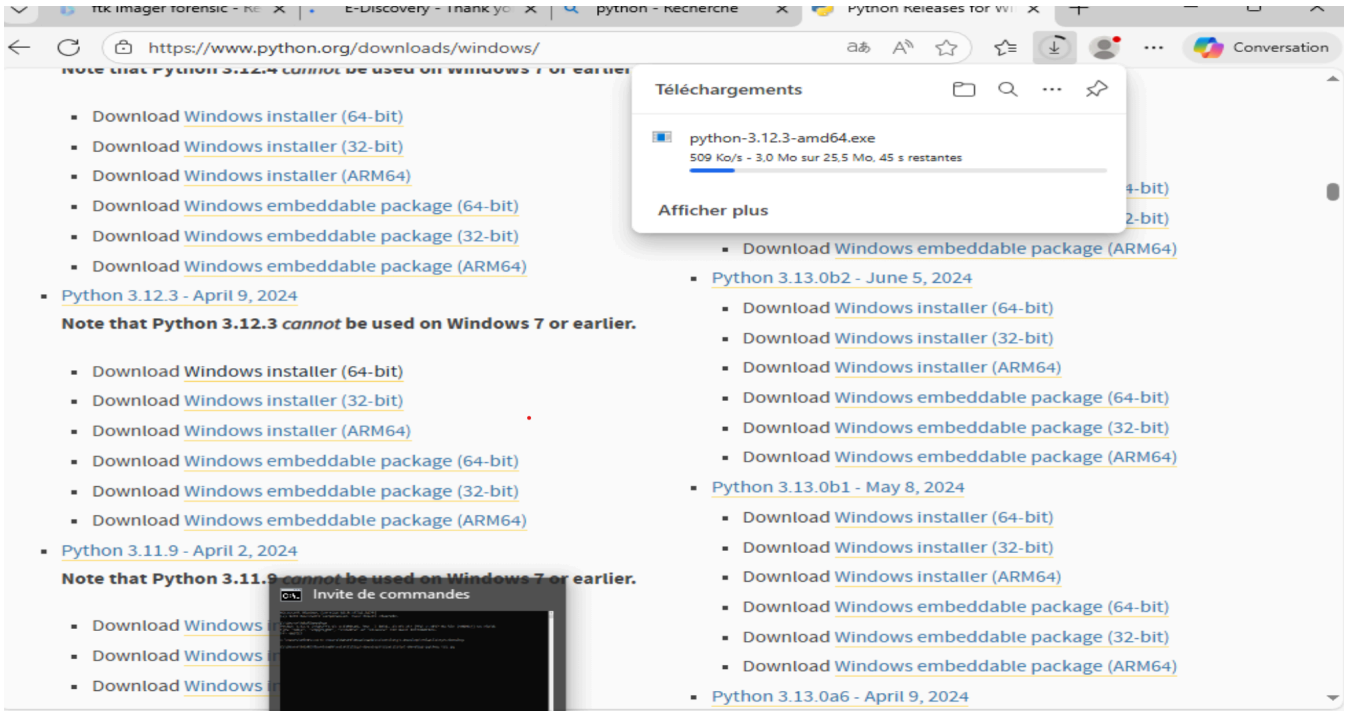
- Installer magnet dumplt



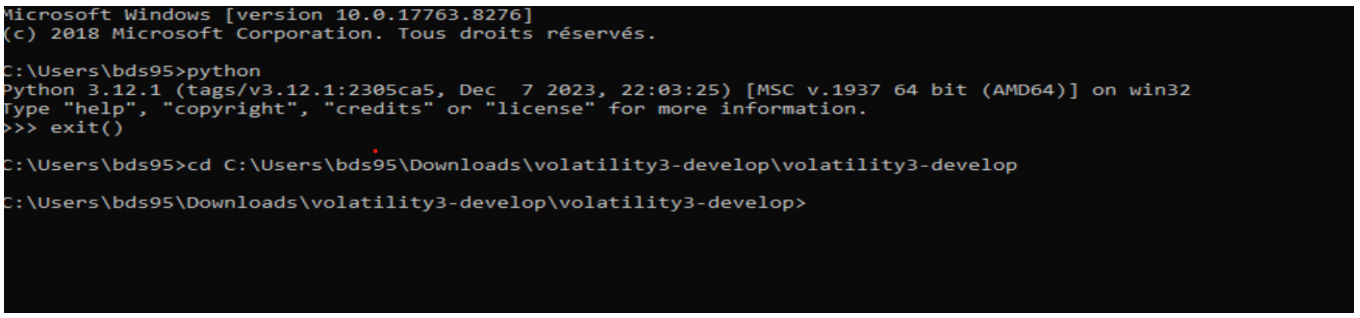
- Exécuter dumplt.exe qui réalise un dump de la mémoire vive du système



- Installer python 3.1.2 pour volatility



- Installer volatility : git clone https://github.com/volatilityfoundation/volatility3.git
- Dans le cmd se placer à l'endroit où volatility est installer

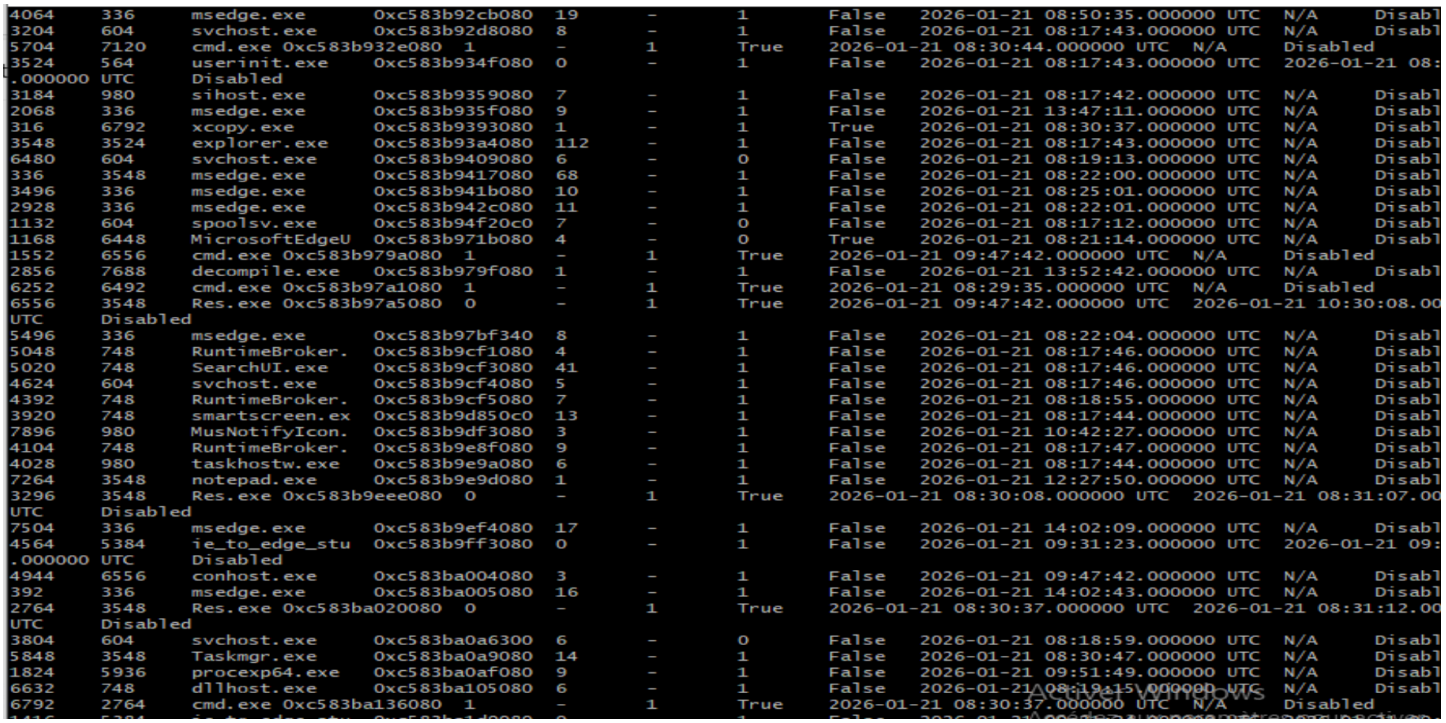


- Dans le cmd entrer la commande *pip install —user -e" .[full]"* - pour installer les dépendences

```
C:\Users\bds95\Downloads\volatility3-develop\volatility3-develop>pip install --user -e".[full]"
Obtaining file:///C:/Users/bds95/Downloads/volatility3-develop/volatility3-develop
  Installing build dependencies ... done
  Checking if build backend supports build_editable ... done
  Getting requirements to build editable ... done
  Preparing editable metadata (pyproject.toml) ... done
Requirement already satisfied: pefile>=2024.8.26 in c:\users\bds95\appdata\roaming\python\python312\site-packages (from
volatility3==2.28.0) (2024.8.26)
Requirement already satisfied: yara-python<5,>=4.5.1 in c:\users\bds95\appdata\roaming\python\python312\site-packages (f
rom volatility3==2.28.0) (4.5.4)
Requirement already satisfied: capstone<6,>=5.0.3 in c:\users\bds95\appdata\roaming\python\python312\site-packages (from
 volatility3==2.28.0) (5.0.6)
Requirement already satisfied: pycryptodome<4,>=3.21.0 in c:\users\bds95\appdata\roaming\python\python312\site-packages
(from volatility3==2.28.0) (3.23.0)
Requirement already satisfied: leechcorepyc<3,>=2.19.2 in c:\users\bds95\appdata\roaming\python\python312\site-packages
(from volatility3==2.28.0) (2.22.6)
Requirement already satisfied: pillow<11.0.0,>=10.0.0 in c:\users\bds95\appdata\roaming\python\python312\site-packages (
from volatility3==2.28.0) (10.4.0)
Building wheels for collected packages: volatility3
  Building editable for volatility3 (pyproject.toml) ... done
  Created wheel for volatility3: filename=volatility3-2.28.0-0.editable-py3-none-any.whl size=7733 sha256=e8850804e6bbc4
974c76462af042fac130b279d6472cd6b338ee5f7704023807
  Stored in directory: C:\Users\bds95\AppData\Local\Temp\pip-ephem-wheel-cache-p1gvabc0\wheels\f3\61\52\9d3f7864cd3db8a6
9138102212e938e11c18f925393448c852
Successfully built volatility3
Installing collected packages: volatility3
  Attempting uninstall: volatility3
    Found existing installation: volatility3 2.28.0
    Uninstalling volatility3-2.28.0:
      Successfully uninstalled volatility3-2.28.0
  WARNING: The scripts vol.exe and volshell.exe are installed in 'C:\Users\bds95\AppData\Roaming\Python\Python312\Script
s' which is not on PATH.
  Consider adding this directory to PATH or, if you prefer to suppress this warning, use --no-warn-script-location.
Successfully installed volatility3-2.28.0

[notice] A new release of pip is available: 23.2.1 -> 25.3
[notice] To update, run: python.exe -m pip install --upgrade pip

C:\Users\bds95\Downloads\volatility3-develop\volatility3-develop>
```

- Puis python vol.py -f *“path/DESKTOP-L50P066-20260121.dmp windows.netscan* - analyse du réseau
- Puis python vol.py -f *“path/DESKTOP-L50P066-20260121.dmp windows.pslist* - récupère les fichier actif
- puis python vol.py *-f “path/DESKTOP-L50P066-20260121.dmp windows.psscan* - récupère les fichier cacher

```
C:\Users\bds95\Downloads\volatility3-develop\volatility3-develop>python vol.py -f DESKTOP-L5OP066-20260121-140455.dmp wi
ndows.psscan
Volatility 3 Framework 2.28.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime
        File output

5660    336     msedge.exe      0x9680000d7500  17      -       1       False   2026-01-21 08:39:46.000000 UTC  N/A
        Disabled
4320    3548    SecurityHealth  0x9680000dd3c0  1       -       1       False   2026-01-21 08:19:03.000000 UTC  N/A
        Disabled
6164    604     SecurityHealth  0x9680000df080  9       -       0       False   2026-01-21 08:19:03.000000 UTC  N/A
        Disabled
4888    748     ApplicationFra  0x9680001c72c0  5       -       1       False   2026-01-21 08:21:51.000000 UTC  N/A
        Disabled
3728    2436    conhost.exe     0x9680001ee080  3       -       1       False   2026-01-21 08:30:07.000000 UTC  N/A
        Disabled
3732    3548    pestudio.exe    0x9680001f7240  9       -       1       False   2026-01-21 09:06:47.000000 UTC  N/A
        Disabled
4       0       System  0xc583b3c6b040  110     -       N/A     False   2026-01-21 08:17:04.000000 UTC  N/A     Disabled

1008    604     svchost.exe     0xc583b3c760c0  15      -       0       False   2026-01-21 08:17:09.000000 UTC  N/A
        Disabled
88      4       Registry        0xc583b3c81080  4       -       N/A     False   2026-01-21 08:16:59.000000 UTC  N/A
        Disabled
4532    4612    iexplore.exe    0xc583b3cce580  19      -       1       True    2026-01-21 08:20:31.000000 UTC  N/A
        Disabled
5388    5704    xcopy.exe       0xc583b3cd8080  1       -       1       True    2026-01-21 08:30:44.000000 UTC  N/A
        Disabled
1268    604     svchost.exe     0xc583b3d14080  16      -       0       False   2026-01-21 08:17:11.000000 UTC  N/A
        Disabled
1204    604     svchost.exe     0xc583b3d49300  19      -       0       False   2026-01-21 08:17:11.000000 UTC  N/A
        Disabled
7736    7004    conhost.exe     0xc583b3d69080  3       -       1       False   2026-01-21 10:30:46.000000 UTC  N/A
        Disabled
1420    336     msedge.exe      0xc583b3d71080  17      -       1       False   2026-01-21 12:47:06.000000 UTC  N/A
        Disabled
1116    604     svchost.exe     0xc583b3d86080  4       -       0       False   2026-01-21 08:17:09.000000 UTC  N/A
        Disabled
1052    604     svchost.exe     0xc583b3da4080  12      -       0       False   2026-01-21 08:17:09.000000 UTC  N/A
        Disabled
288     4       smss.exe        0xc583b43890c0  2       -       N/A     False   2026-01-21 08:17:04.000000 UTC  N/A
        Disabled
```



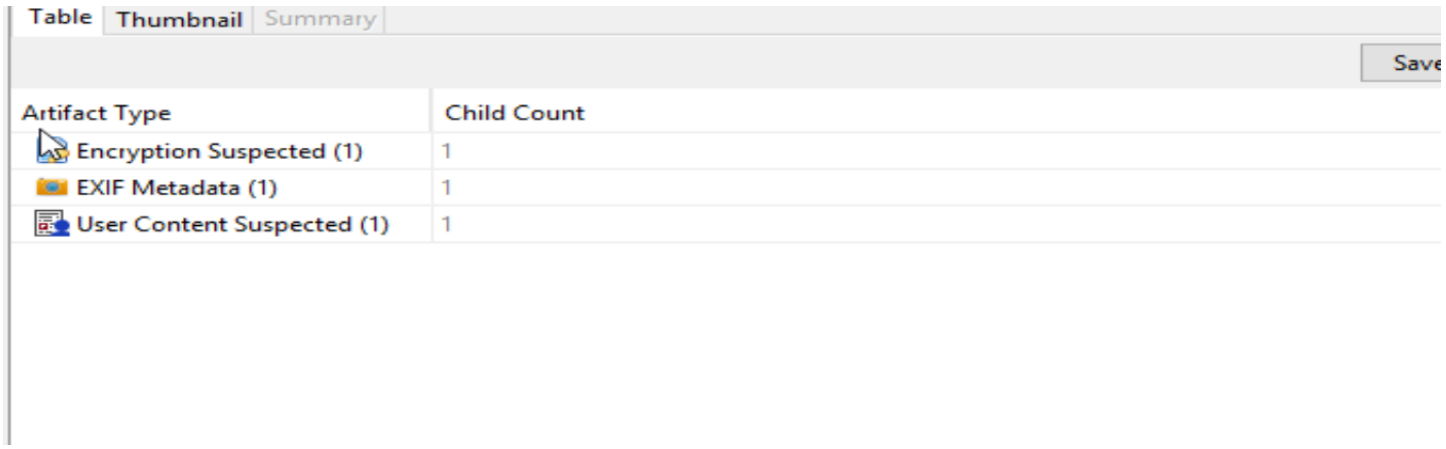
```
4064    336     msedge.exe      0xc583b92cb080  19      -       1       False   2026-01-21 08:50:35.000000 UTC  N/A     Disabl
3204    604     svchost.exe     0xc583b92d8080  8       -       1       False   2026-01-21 08:17:43.000000 UTC  N/A     Disabl
5704    7120    cmd.exe 0xc583b932e080  1       -       1       True    2026-01-21 08:30:44.000000 UTC  N/A     Disabled
3524    564     userinit.exe    0xc583b934f080  0       -       1       False   2026-01-21 08:17:43.000000 UTC  2026-01-21 08:
.000000 UTC     Disabled
3184    980     sihost.exe      0xc583b9359080  7       -       1       False   2026-01-21 08:17:42.000000 UTC  N/A     Disabl
2068    336     msedge.exe      0xc583b935f080  9       -       1       False   2026-01-21 13:47:11.000000 UTC  N/A     Disabl
316     6792    xcopy.exe       0xc583b9393080  1       -       1       True    2026-01-21 08:30:37.000000 UTC  N/A     Disabl
3548    3524    explorer.exe    0xc583b93a4080  112     -       1       False   2026-01-21 08:17:43.000000 UTC  N/A     Disabl
6480    604     svchost.exe     0xc583b9409080  6       -       0       False   2026-01-21 08:19:13.000000 UTC  N/A     Disabl
336     3548    msedge.exe      0xc583b9417080  68      -       1       False   2026-01-21 08:22:00.000000 UTC  N/A     Disabl
3496    336     msedge.exe      0xc583b941b080  10      -       1       False   2026-01-21 08:25:01.000000 UTC  N/A     Disabl
2928    336     msedge.exe      0xc583b942c080  11      -       1       False   2026-01-21 08:22:01.000000 UTC  N/A     Disabl
1132    604     spoolsv.exe     0xc583b94f20c0  7       -       0       False   2026-01-21 08:17:12.000000 UTC  N/A     Disabl
1168    6448    MicrosoftEdgeU  0xc583b971b080  4       -       0       True    2026-01-21 08:21:14.000000 UTC  N/A     Disabl
1552    6556    cmd.exe 0xc583b979a080  1       -       1       True    2026-01-21 09:47:42.000000 UTC  N/A     Disabled
2856    7688    decompile.exe   0xc583b979f080  1       -       1       False   2026-01-21 13:52:42.000000 UTC  N/A     Disabl
6252    6492    cmd.exe 0xc583b97a1080  1       -       1       True    2026-01-21 08:29:35.000000 UTC  N/A     Disabled
6556    3548    Res.exe 0xc583b97a5080  0       -       1       True    2026-01-21 09:47:42.000000 UTC  2026-01-21 10:30:08.00
UTC     Disabled
5496    336     msedge.exe      0xc583b97bf340  8       -       1       False   2026-01-21 08:22:04.000000 UTC  N/A     Disabl
5048    748     RuntimeBroker.  0xc583b9cf1080  4       -       1       False   2026-01-21 08:17:46.000000 UTC  N/A     Disabl
5020    748     SearchUI.exe    0xc583b9cf3080  41      -       1       False   2026-01-21 08:17:46.000000 UTC  N/A     Disabl
4624    604     svchost.exe     0xc583b9cf4080  5       -       1       False   2026-01-21 08:17:46.000000 UTC  N/A     Disabl
4392    748     RuntimeBroker.  0xc583b9cf5080  7       -       1       False   2026-01-21 08:18:55.000000 UTC  N/A     Disabl
3920    748     smartscreen.ex  0xc583b9d850c0  13      -       1       False   2026-01-21 08:17:44.000000 UTC  N/A     Disabl
7896    980     MusNotifyIcon.  0xc583b9df3080  3       -       1       False   2026-01-21 10:42:27.000000 UTC  N/A     Disabl
4104    748     RuntimeBroker.  0xc583b9e8f080  9       -       1       False   2026-01-21 08:17:47.000000 UTC  N/A     Disabl
4028    980     taskhostw.exe   0xc583b9e9a080  6       -       1       False   2026-01-21 08:17:44.000000 UTC  N/A     Disabl
7264    3548    notepad.exe     0xc583b9e9d080  1       -       1       False   2026-01-21 12:27:50.000000 UTC  N/A     Disabl
3296    3548    Res.exe 0xc583b9eee080  0       -       1       True    2026-01-21 08:30:08.000000 UTC  2026-01-21 08:31:07.00
UTC     Disabled
7504    336     msedge.exe      0xc583b9ef4080  17      -       1       False   2026-01-21 14:02:09.000000 UTC  N/A     Disabl
4564    5384    ie_to_edge_stu  0xc583b9ff3080  0       -       1       False   2026-01-21 09:31:23.000000 UTC  2026-01-21 09:
.000000 UTC     Disabled
4944    6556    conhost.exe     0xc583ba004080  3       -       1       False   2026-01-21 09:47:42.000000 UTC  N/A     Disabl
392     336     msedge.exe      0xc583ba005080  16      -       1       False   2026-01-21 14:02:43.000000 UTC  N/A     Disabl
2764    3548    Res.exe 0xc583ba020080  0       -       1       True    2026-01-21 08:30:37.000000 UTC  2026-01-21 08:31:12.00
UTC     Disabled
3804    604     svchost.exe     0xc583ba0a6300  6       -       0       False   2026-01-21 08:18:59.000000 UTC  N/A     Disabl
5848    3548    Taskmgr.exe     0xc583ba0a9080  14      -       1       False   2026-01-21 08:30:47.000000 UTC  N/A     Disabl
1824    5936    procexp64.exe   0xc583ba0af080  9       -       1       False   2026-01-21 09:51:49.000000 UTC  N/A     Disabl
6632    748     dllhost.exe     0xc583ba105080  6       -       1       False   2026-01-21 08:19:15.000000 UTC  N/A     Disabl
6792    2764    cmd.exe 0xc583ba136080  1       -       1       True    2026-01-21 08:30:37.000000 UTC  N/A     Disabled
```

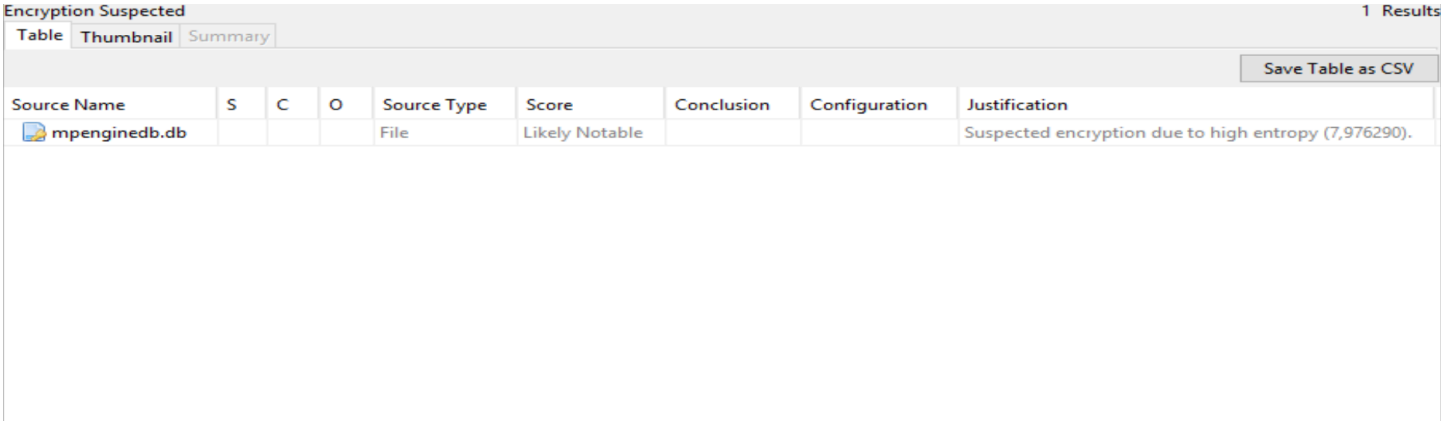
le malware est bien trouvé dans la mémoire

Story 7

- installer FTK Imager
- aller dans file puis create disk Image
- on sélectionne Physical Drive
- choisir drive 0 puis E01
- on choisit le dossier de destination (dans un autre disque que celui utilisé) puis et le nom de fichier
- on clique sur finish

- installer autopsy
- créer une case avec un nom avec base directory le dossier du malware puis next puis finish
- puis on choisit l'image du disque créé précédemment avec FTK Image
- une fois l'analyse finie aller dans analysis schedule et on observe ceci :





Story 8:

Correspondance Processus Mémoire / Fichiers Disque

- **Processus en Mémoire (RAM) :** L'analyse Volatility (mentionnée en Story 6) confirme l'exécution du processus malveillant.
- **Fichier sur Disque :** Ce processus correspond à l'exécutable **`Res.exe`**.
- **Chemin identifié :** Le fichier est localisé dans un répertoire caché créé par le malware : **`C:\WindSyst\Res.exe`**.

2. Détection de la Persistance L'analyse confirme que le malware assure sa survie au redémarrage via une modification du Registre Windows :

- **Mécanisme :** Ajout de valeurs dans la clé de registre `Run`.
- **Emplacement :** `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run`.

- **Cible :** Les valeurs créées pointent directement vers les fichiers `C:\WindSyst\Res.exe` et `C:\WindSyst\Env.exe`, forçant leur lancement à chaque ouverture de session.

Partie 3:

Story 9:

1) Installer Registry Explorer
2) Aller dans File puis load hive puis sélectionner le fichier SYSTEM dans le dossier dump extrait
3) Sélectionnez “yes” dans la popup puis “ok” puis “annuler” puis yes
4) Puis sélectionner le dossier root de la clé puis controlset001 puis USBSTOR puis Disk&Ven puis on retrouve le numéro de série et les autres donnée dans le tableau values

marque: SanDisk Cruzer Blade USB Device
numéro de série: 4C530000281008116284&0

Story 10:
First Installed: 2020-02-03 12:12:32
Installed : 2020-02-03 12:12:32
Last Connected : 2020-02-03 12:44:21

Last Removed: 2020-02-03 12:45:00