User Story 1 :

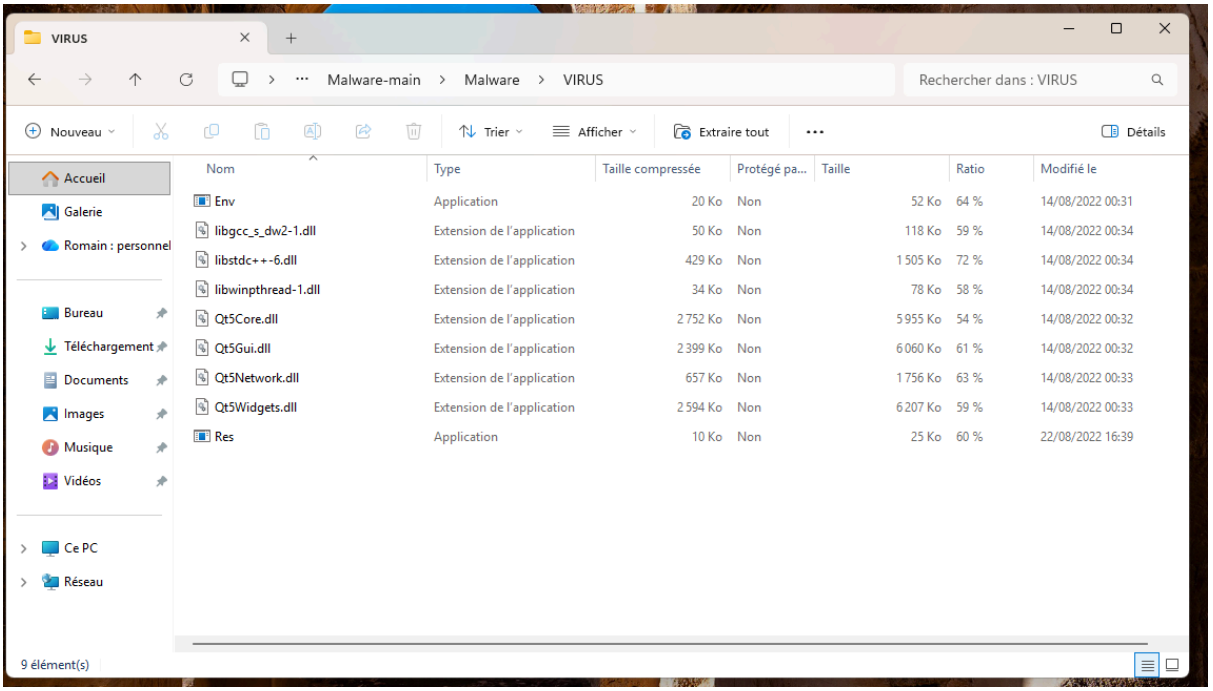
Nous avons créé une machine virtuelle grâce à Virtual Box avec Windows10 puis nous sommes allé sur le repo pour télécharger le Malware.

Nous l'avons installé sur la machine et tout a crash donc nous avons tout réinstallé en ajoutant plus de RAM.

Nous avons contasté que le virus consomme beaucoup de puissance sur la machine.

Nous allons procédé à une analyse sur le Malware dans les prochaines story.

Nom du Malware : Res.exe



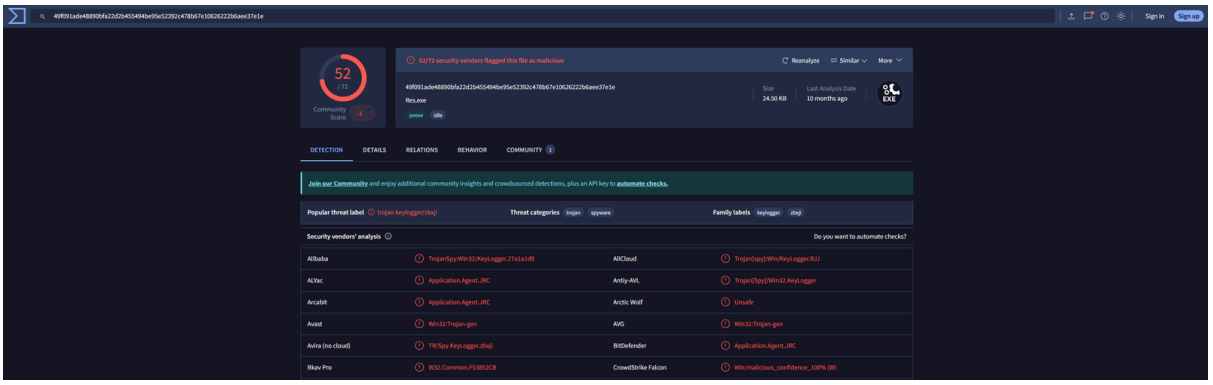
User Story 2 :

Après avoir lancer le Malware, nous voulions savoir si ce dernier était deja connu sur le web.

Alors, nous avons procédé à l'écriture de ces commandes afin de récuperer le Hash du Malware.

Commandes pour récuperer le Hash : Get-FileHash -Algorithm SHA256 "C:\Users\theol\Desktop\VIRUS\Res.exe"
Résultat :
49F091ADE48890BFA22D2B455494BE95E52392C478B67E10626222B6AEE37E1E

Par la suite, nous sommes allé sur VirusTotal puis nous avons renseigné le Hash et nous avons obtenu le resultat suivant :

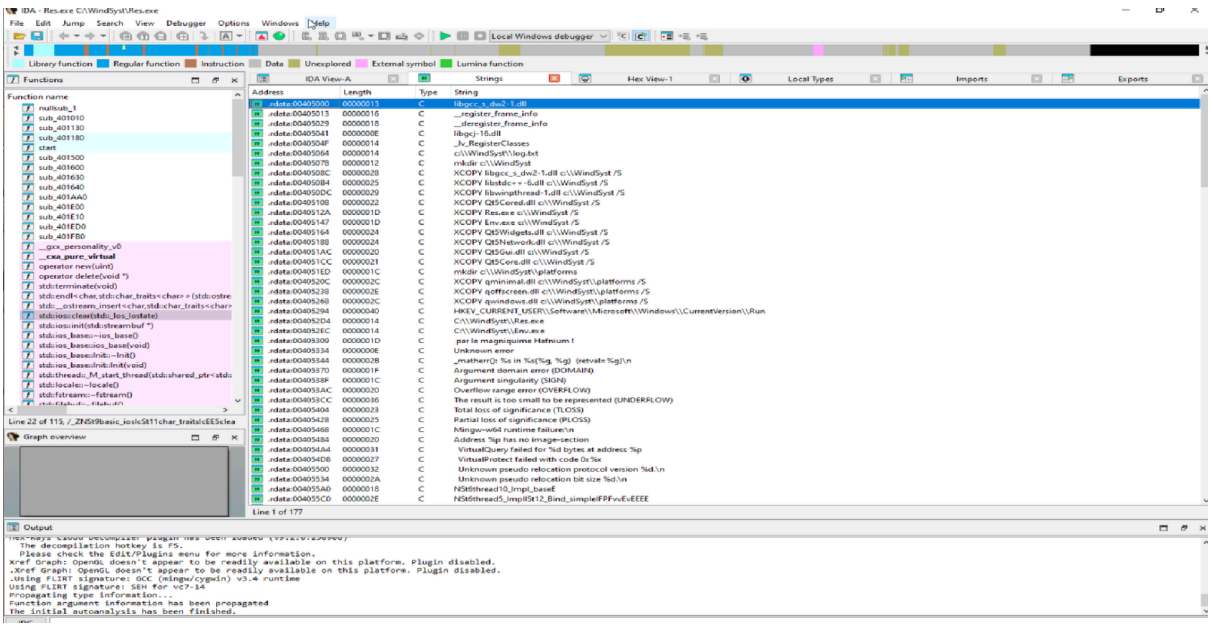


User Story 3 :

Nous avons par la suite analysé ce Malware :

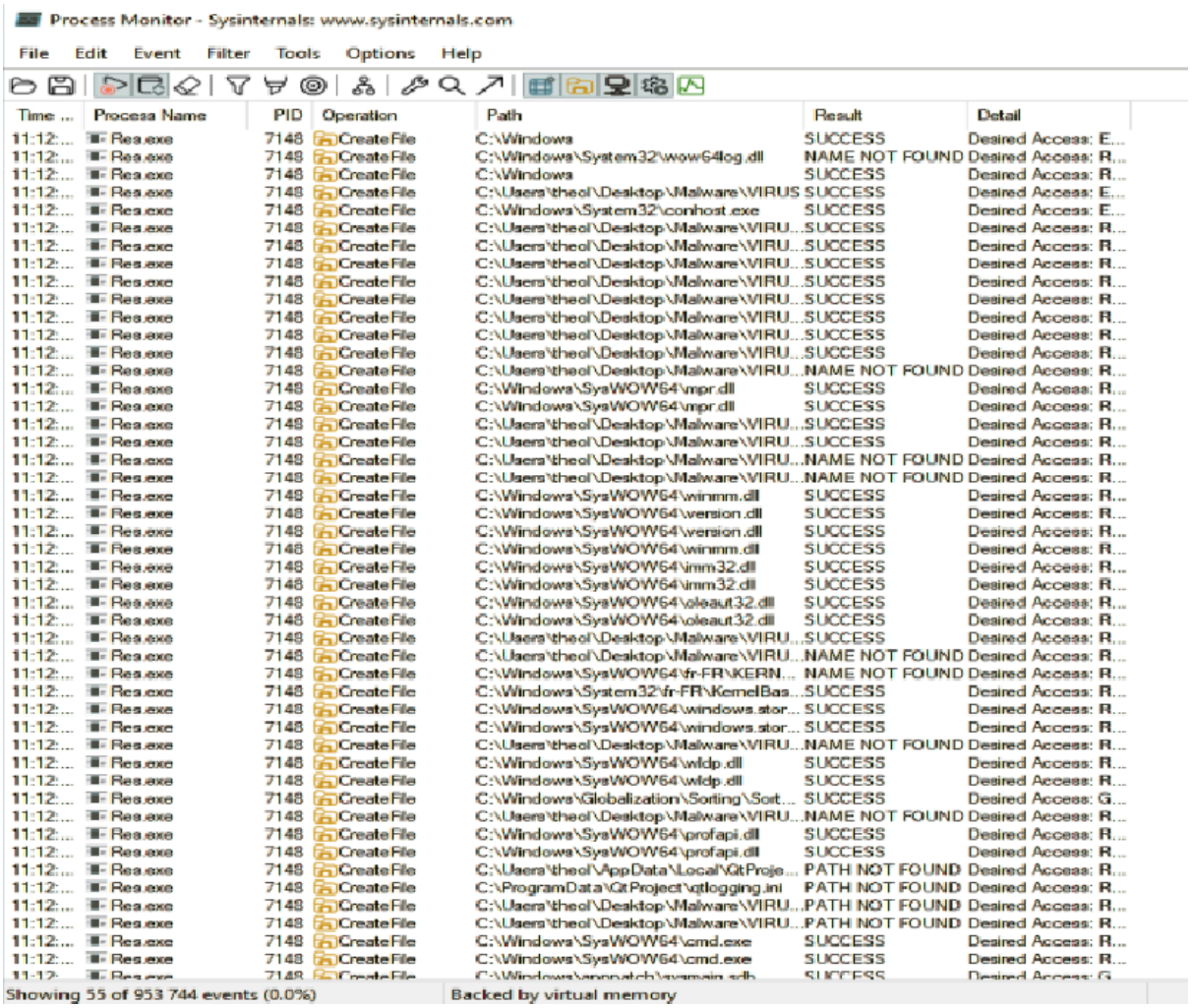
Etape 1 : Installer PeStudio
Etape 2 : Ouvrir Res.exe (Malware) avec PeStudio
Etape 3 : Constater les différents problèmes rencontrés

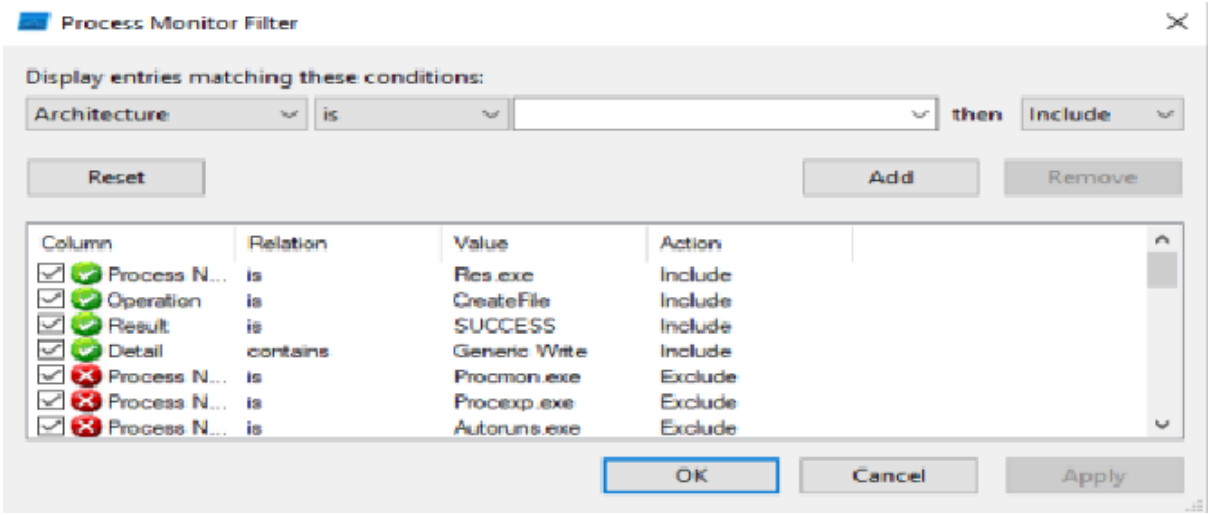
Nous avons pu constater les dégats sur la machine :
- Forte augmentation de la consommation de la RAM
- Score de 52/72 (ex : spyWare / keyLogger / trojan)
- imports (get current process, virtualprotect, getcurrentprocessId, getcurrentThread, virtualQuery, getAsyncKeyState, getKeyState)



User Story 4 :

Nous avons remarqué que le Malware crée un fichier.
Pour trouver ce fichier, nous avons utiliser ProcessHacker et ProcessExplorer pour identifier le processus infecté.





User Story 5 :

Description clair des impacts :
Il existe un nouveau fichier nommé "xcopy.exe"

Il crée un dossier `C:\WindSyst`
- Chaîne trouvée : `mkdir C:\WindSyst`
- Il copie ensuite plusieurs DLLs et exécutables dans ce dossier :
  - `libgcc_s_dw2-1.dll`, `libstdc++-6.dll`, `Qt5Core.dll`, `Qt5Gui.dll`, etc.
  - `Res.exe` et `Env.exe`

- Possible accès au micro ou interaction avec des fichiers audio

User Story 6 :

Pour faire le dump de la mémoire vive, nous avons :

  - Nous avons tout d'abord installer DumpIt
  - Puis on est aller dans le Powershell jusqu'a DumpIt.exe :
C:\Users\theol\Desktop\Comae-Toolkit-v20230117\x64
  - On a lancé dumpIt.exe avec la commande \DumpIt.exe
  - On a eu le dump et la destination du fichier
  - Nous avons installé PIP, puis installer volatility avec pip.
  - Une fois que nous avons vérifier que tout était installé avec "vol -h", nous avons pu faire l'analyse avec la commande : vol -f "nom du dump" windows.pslist
  - Nous avons donc pu avoir les resultat

```
All rights reserved.

Thanks for using DumpIt! Always use Microsoft crash dumps!

  Destination path:           \??\C:\Users\theol\Desktop\Comae-Toolkit-v20230117\x64\DESKTOP-4I2P9JF-20260122-084701.dmp

  Computer name:              DESKTOP-4I2P9JF

  --> Proceed with the acquisition ? [y/n] y

  [+] Information:
  Dump Type:                   Microsoft Crash Dump


  [+] Machine Information:
  Windows version:            10.0.19045
  MachineId:                  0AF6F08F-AFDC-48D5-842B-08D1615F7C83
  TimeStamp:                  134135452257879731
  Cr3:                        0x1aa000
  KdCopyDataBlock:            0xfffff80646310c08
  KdDebuggerData:             0xfffff80646a00b20
  KdpDataBlockEncoded:        0xfffff80646a50b40

  Current date/time:          [2026-01-22 (YYYY-MM-DD) 8:47:05 (UTC)]
  + Processing... Done.

  Acquisition finished at:    [2026-01-22 (YYYY-MM-DD) 8:48:18 (UTC)]
  Time elapsed:               1:12 minutes:seconds (72 secs)

  Created file size:           17179406336 bytes (16383 MB)
  Total physical memory size:  16383 MB

  NtStatus (troubleshooting):   0x80000000
  Total of written pages:       4194189
  Total of inacessible pages:          0
  Total of accessible pages:    4194189

  SHA-256: F4820959DD84A188FE43511C2ADB0F143FBBE835B9497B007A8BA8E46EF05BA4

  JSON path:                  C:\Users\theol\Desktop\Comae-Toolkit-v20230117\x64\DESKTOP-4I2P9JF-20260122-084701.json

PS C:\Users\theol\Desktop\Comae-Toolkit-v20230117\x64> _
```

User Story 9 :

Ouvrir un terminal depuis le dossier du dump

Faire cette commande : strings SYSTEM | grep -i usbstor -A 5

Dans le résultat, on trouve :

USBSTOR\Disk&Ven_SanDisk&Prod_Cruzer_Blade&Rev_1.00\4C530000281008116284&0 37HardwareID

```
dump — -zsh — 168×41
Last login: Fri Jan 23 08:57:29 on console
samuel@Mac-CF-23-002 dump % strings SYSTEM | grep -i usbstor -A 5
USBSTOR
ImagePath
Type
Start
ErrorControl
DisplayName
--
usbstor.inf
Active
Configurations@
usbxhci.inf
Active
Configurations
--
usbstor
054C00C1
DeviceHackFlags
zx"c
058F6362
DeviceHackFlags
--
USBSTOR
DiskSony____MSC-U01N________
Configuration
Manufacturer
Description
DiskSony____MSC-U01_________
--
USBSTOR\Disk&Ven_SanDisk&Prod_Cruzer_Blade&Rev_1.00\4C530000281008116284&0
37HardwareID
igur
CompatibleIDs
{540b947e-8b40-45bc-a8a2-6a0b894cbda2}
0004R
--
##?#USBSTOR#Disk&Ven_SanDisk&Prod_Cruzer_Blade&Rev_1.00#4C530000281008116284&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
LC16
#escript
DeviceInstance&
```

User Story 10 :

Outils utilisés :

FTK Imager : pour extraire les fichiers du registre Windows (SYSTEM, SOFTWARE)

Artefacts extraits :

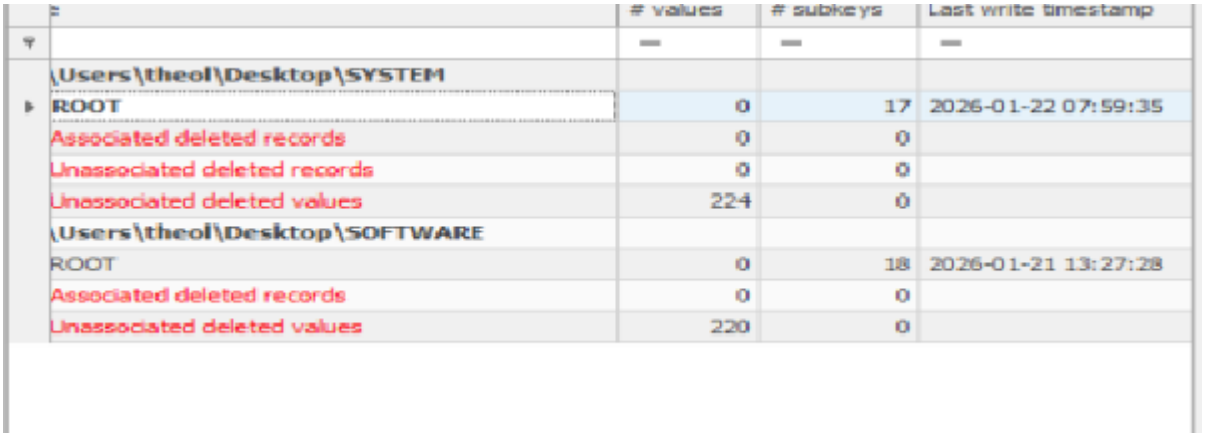
SYSTEM : contient les clés USBSTOR, USB, MountedDevices
SOFTWARE : utilisé pour corrélation utilisateur

Analyse des artefacts USB :

Première installation : 2026-01-21 13:27
Dernière connexion : 2026-01-22 07:59

""Chronologie des événements

2026-01-20 14:32 — Installation initiale de la clé USB (USBSTOR + setupapi.dev.log)
2026-01-21 — Activité utilisateur sur le poste (NTUSER.DAT)
2026-01-22 09:15 — Dernière connexion de la clé USB (USB)
2026-01-22 — Dump mémoire réalisé avec DumpIt""



	# values	# subkeys	Last write timestamp
\Users\theol\Desktop\SYSTEM			
ROOT	0	17	2026-01-22 07:59:35
Associated deleted records	0	0	
Unassociated deleted records	0	0	
Unassociated deleted values	224	0	
\Users\theol\Desktop\SOFTWARE			
ROOT	0	18	2026-01-21 13:27:28
Associated deleted records	0	0	
Unassociated deleted values	220	0	