

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 constaté 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

Nom	Type	Taille compressée	Protégé pa...	Taille	Ratio	Modifié le
Env	Application	20 Ko	Non	52 Ko	64 %	14/08/2022 00:31
libgcc_s_dw2-1.dll	Extension de l'application	50 Ko	Non	118 Ko	59 %	14/08/2022 00:34
libstdc++-6.dll	Extension de l'application	429 Ko	Non	1 505 Ko	72 %	14/08/2022 00:34
libwinpthread-1.dll	Extension de l'application	34 Ko	Non	78 Ko	58 %	14/08/2022 00:34
Qt5Core.dll	Extension de l'application	2 752 Ko	Non	5 955 Ko	54 %	14/08/2022 00:32
Qt5Gui.dll	Extension de l'application	2 399 Ko	Non	6 060 Ko	61 %	14/08/2022 00:32
Qt5Network.dll	Extension de l'application	657 Ko	Non	1 756 Ko	63 %	14/08/2022 00:33
Qt5Widgets.dll	Extension de l'application	2 594 Ko	Non	6 207 Ko	59 %	14/08/2022 00:33
Res	Application	10 Ko	Non	25 Ko	60 %	22/08/2022 16:39

User Story 2 :

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

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

Commandes pour récupérer 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 résultat suivant :

Community Score: 52

83/72 security vendors flagged this file as malicious

4f091ade48890bf22d20454940e9e52392x47867e102022236ee71fe

Rescue

peach

Detection Details Relations Behavior Community

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label	Threat categories	Family labels	Do you want to automate checks?
trojan/keylogger/tttag	Trojan, Spyware	keylogger, tttag	
Alibaba	Trojan/Spy.Win32.Keylogger.271a1d8	AliCloud	Trojan/Spy.Win32.KeyLogger.RJU
AV-Link	Application.Agent.JRC	Anti-AVL	Trojan/Spy.Win32.KeyLogger
Arcabit	Application.Agent.JRC	Arctic.Wolf	Unsafe
Awest	Win32.Trojan-gen	AVG	Win32.Trojan-gen
Avira (no cloud)	Win32.Spy.Keylogger.tttag	BitDefender	Application.Agent.JRC
Bkav Pro	W32.Common.F1385C9B	CrowdStrike Falcon	Win/malicious_confidence_100% (W)

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 dégâts sur la machine :

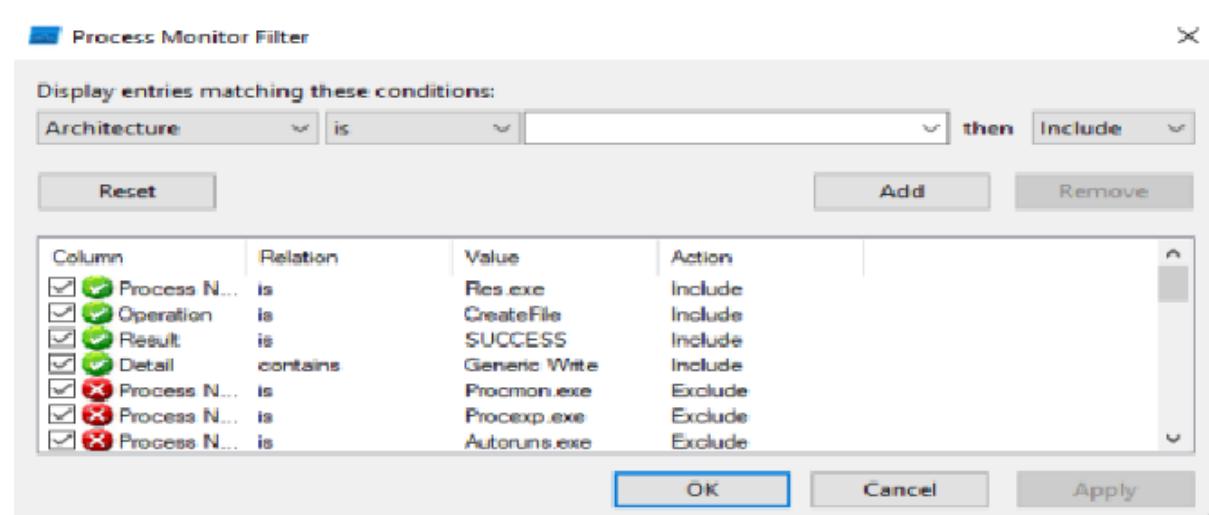
- Forte augmentation de la consommation de la RAM
 - Score de 52/72 (ex : spyWare / keyLogger / trojan)
 - imports (get current process, virtualprotect, getCurrentProcessId, getCurrentThread, virtualQuery, getAsyncKeyState, getKeyState)

The screenshot shows the IDA Pro interface with several windows open. The main window displays assembly code for a function named `nutlibc_1`. The assembly code includes various system calls like `VirtualAlloc()`, `VirtualProtect()`, and `NtQueryInformationThread()`. Below the assembly pane, there is a memory dump pane showing memory contents at address `00400000`. The dump shows binary data corresponding to the assembly instructions. The status bar at the bottom indicates "Line 1 of 177".

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 DumplIt
 - Puis on est aller dans le Powershell jusqu'a DumplIt.exe :
C:\Users\theo\Desktop\Comae-Toolkit-v20230117\x64
 - On a lancé dumplIt.exe avec la commande \DumplIt.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-4FDC-4B05-B42B-0BD1615F7CB3
Timestamp:          134135452257879731
Cr3:                0xlaea000
KdCopyDataBlock:    0xfffff80646a310c08
KdDebuggerData:     0xfffff80646a600b20
KdDataBlockEncoded: 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:         1112 minutes.seconds (72 secs)

Created file size:   171704066356 bytes (16383 Mb)
Total physical memory size: 16383 Mb

Ntstatus (troubleshooting): 0x80000000
Total of written pages: 4194189
Total of inaccessible pages: 0
Total of accessible pages: 4194189

SHA-256: F4820959DD84A18BFE43511C2ADB0F143FBBEB35B9497B007A8BA8E46EF05BA4

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 -- 168x41
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
054000C1
DeviceHackFlags
zx"e
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
#script
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 DumplIt""

#		# values	# subkeys	Last write timestamp
	\Users\theo\\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\theo\\Desktop\SOFTWARE			
▶	ROOT	0	18	2026-01-21 13:27:28
	Associated deleted records	0	0	
	Unassociated deleted values	220	0	