

Sommaire

[1. Analyse d’un DUMP mémoire 1](#_Toc131147393)

# 1. Analyse d’un DUMP mémoire

Pour analyser un DUMP de mémoire il est important de savoir quel outil utiliser.

Ici nous utiliserons volatility

**/ ! \ Attention : Avant d’utiliser volatility il est important de savoir sur quel type de mémoire on va travailler**

**En fonction de l’OS le mémoire diffère (Windows, Linux, Mac, Android…)**

La liste des images et des plugins possibles de passer en commande sont listés sur le GitHub de Volatility :

<https://github.com/volatilityfoundation/volatility>

Nous pouvons maintenant lancer volatility avec la commande suivante :

PS D:\tmp\vm\volatility\_2.6\_win64\_standalone> .\volatility\_2.6\_win64\_standalone.exe -f "D:\tmp\vm\ram\_suspecte - Copie.raw" --profile=Win2016x64\_14393 imageinfo

Syntaxe :

-f : Permet de spécifier le fichier sur lequel on va travailler

--profile : Permet de spécifier sur quel type de mémoire on va travailler

Imageinfo : Permet de définir les informations que l’on souhaite retrouver dans la mémoire

Résultat de la commande :

Volatility Foundation Volatility Framework 2.6

INFO : volatility.debug : Determining profile based on KDBG search...

Suggested Profile(s) : Win2016x64\_14393

AS Layer1 : Win10AMD64PagedMemory (Kernel AS)

AS Layer2 : FileAddressSpace (D:\tmp\vm\ram\_suspecte - Copie.raw)

PAE type : No PAE

DTB : 0x1aa000L

KDBG : 0xf80239782500L

Number of Processors : 1

Image Type (Service Pack) : 0

KPCR for CPU 0 : 0xfffff802397d4000L

KUSER\_SHARED\_DATA : 0xfffff78000000000L

Image date and time : 2023-03-30 08:27:07 UTC+0000

Image local date and time : 2023-03-30 10:27:07 +0200

Voici d’autres exemples de commandes qui permettent de récupérer d’autres informations :

PS D:\tmp\vm\volatility\_2.6\_win64\_standalone> .\volatility\_2.6\_win64\_standalone.exe -f "D:\tmp\vm\ram\_suspecte - Copie.raw" --profile=Win2016x64\_14393 pslist

Permet de lister les processus qui ont été exécuté

Résultat de la commande :

Volatility Foundation Volatility Framework 2.6

Offset(V) Name PID PPID Thds Hnds Sess Wow64 Start Exit

------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------

0xffffd5853722e040 System 4 0 92 0 ------ 0 2023-03-30 07:55:27 UTC+0000

0xffffd585379fc840 smss.exe 264 4 2 0 ------ 0 2023-03-30 07:55:27 UTC+0000

0xffffd585379f0080 csrss.exe 348 340 10 0 0 0 2023-03-30 07:55:28 UTC+0000

0xffffd58538fc3080 smss.exe 408 264 0 -------- 1 0 2023-03-30 07:55:29 UTC+0000 2023-03-30 07:55:29 UTC+0000

0xffffd58538fc0080 csrss.exe 416 408 11 0 1 0 2023-03-30 07:55:29 UTC+0000

... ... ... ...

PS D:\tmp\vm\volatility\_2.6\_win64\_standalone> .\volatility\_2.6\_win64\_standalone.exe -f "D:\tmp\vm\ram\_suspecte - Copie.raw" --profile=Win2016x64\_14393 cmdline

Permet de lister les commande qui ont été exécuté

Retour de la commande :

Volatility Foundation Volatility Framework 2.6

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

System pid: 4

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

smss.exe pid: 264

Command line : \SystemRoot\System32\smss.exe

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

csrss.exe pid: 348

Command line : %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16

... ... ... ... ...

Ici nous pouvons voir les différentes commandes qui sont exécutés sur la machine infectée

Pour vérifier que les services lancés sont bien légitimes nous pouvons ouvrir le gestionnaire de tâches sur une machine propre et vérifier dans l’onglet « services » que le service est bien présent

Nous pourrons donc considérer que le service n’est pas suspect (exemple avec le service DcomLaunch) :



Il existe bien sur une machine non infectée donc le service n’est pas suspect

Si un service ou une commande nous parait suspect et qu’on ne retrouve pas d’infos dans le gestionnaire de tâches nous pouvons effectuer des recherches sur internet (exemple avec le processus MsMpEng.exe) :

Une image contenant texte

Description générée automatiquement

Après quelques recherches sur internet nous ne trouvons **aucune documentation officielle de Microsoft**. Nous avons **seulement des forums** donc nous pouvons en déduire que le **processus est suspect**

PS D:\tmp\vm\volatility\_2.6\_win64\_standalone> .\volatility\_2.6\_win64\_standalone.exe -f "D:\tmp\vm\ram\_suspecte - Copie.raw" --profile=Win2016x64\_14393 pstree

Permet de voir l’arborescence des processus exécutés et de savoir qui sont les processus parents qui ont exécuté d’autres processus

Résultat de commande :

Name Pid PPid Thds Hnds Time

-------------------------------------------------- ------ ------ ------ ------ ----

0xffffd5853722e040:System 4 0 92 0 2023-03-30 07:55:27 UTC+0000

. 0xffffd585379fc840:smss.exe 264 4 2 0 2023-03-30 07:55:27 UTC+0000

.. 0xffffd58538fc3080:smss.exe 408 264 0 ------ 2023-03-30 07:55:29 UTC+0000

... 0xffffd58538fc0080:csrss.exe 416 408 11 0 2023-03-30 07:55:29 UTC+0000

... ... ... ...