[1. Analyse d’un DUMP mémoire 1](#_Toc131153742)

[2. Résumé de l’attaque 7](#_Toc131153743)

# 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\cridex.vmem" --profile=WinXPSP2x86 imageinfo

**Syntaxe :**

-f : Permet de spécifier le fichier sur lequel on va travailler (ici cridex.vmem)

--profile : Permet de spécifier sur quel type de mémoire on va travailler (ici WinXPSP2x86)

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

**Retour de commande :**

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

Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)

AS Layer1 : IA32PagedMemoryPae (Kernel AS)

AS Layer2 : FileAddressSpace (D:\tmp\vm\cridex.vmem)

PAE type : PAE

DTB : 0x2fe000L

KDBG : 0x80545ae0L

Number of Processors : 1

Image Type (Service Pack) : 3

KPCR for CPU 0 : 0xffdff000L

KUSER\_SHARED\_DATA : 0xffdf0000L

Image date and time : 2012-07-22 02:45:08 UTC+0000

Image local date and time : 2012-07-21 22:45:08 -0400

//////////////////////////////////////////////////////////////////////////////////////////////////////////

**Commande pour vérifier la liste des commandes qui ont été exécutées :**

PS D:\tmp\vm\volatility\_2.6\_win64\_standalone> .\volatility\_2.6\_win64\_standalone.exe -f "D:\tmp\vm\cridex.vmem" --profile=WinXPSP2x86 cmdline

**Retour de la commande :**

spoolsv.exe pid: 1512

Command line : C:\WINDOWS\system32\spoolsv.exe

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

reader\_sl.exe pid: 1640

Command line : "C:\Program Files\Adobe\Reader 9.0\Reader\Reader\_sl.exe"

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

alg.exe pid: 788

Command line : C:\WINDOWS\System32\alg.exe

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

wuauclt.exe pid: 1136

Command line : "C:\WINDOWS\system32\wuauclt.exe" /RunStoreAsComServer Local\[3ec]SUSDSb81eb56fa3105543beb3109274ef8ec1

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

wuauclt.exe pid: 1588

Command line : "C:\WINDOWS\system32\wuauclt.exe"

Ici nous pouvons voir qu’un fichier a été ouvert avec Adobe Reader

Par la suite nous pouvons voir que le Pare-Feu s’est activé et a envoyé une notification

Avec cette commande :

volatility\_2.6\_win64\_standalone.exe -f cridex.vmem --profile=WinXPSP2x86 psxview –R

On peut vérifier s'il y a des processus cachés s'il y a False.

Ici tout est semble bon

**Retour de la commande :**

Offset(P) Name PID pslist psscan thrdproc pspcid csrss session deskthrd ExitTime

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

0x02498700 winlogon.exe 608 True True True True True True True

0x02511360 svchost.exe 824 True True True True True True True

0x022e8da0 alg.exe 788 True True True True True True True

0x020b17b8 spoolsv.exe 1512 True True True True True True True

0x0202ab28 services.exe 652 True True True True True True True

0x02495650 svchost.exe 1220 True True True True True True True

0x0207bda0 reader\_sl.exe 1640 True True True True True True True

0x025001d0 svchost.exe 1004 True True True True True True True

0x02029ab8 svchost.exe 908 True True True True True True True

0x023fcda0 wuauclt.exe 1136 True True True True True True True

0x0225bda0 wuauclt.exe 1588 True True True True True True True

0x0202a3b8 lsass.exe 664 True True True True True True True

0x023dea70 explorer.exe 1484 True True True True True True True

0x023dfda0 svchost.exe 1056 True True True True True True True

0x024f1020 smss.exe 368 True True True True Okay Okay Okay

0x025c89c8 System 4 True True True True Okay Okay Okay

0x024a0598 csrss.exe 584 True True True True Okay True True

//////////////////////////////////////////////////////////////////////////////////////////////////////////

**Commande pour lister les processus ouverts dans une arborescence :**

PS D:\tmp\vm\volatility\_2.6\_win64\_standalone> .\volatility\_2.6\_win64\_standalone.exe -f "D:\tmp\vm\cridex.vmem" --profile=WinXPSP2x86 pstree

**Retour de la commande :**

Name Pid PPid Thds Hnds Time

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

0x823c89c8:System 4 0 53 240 1970-01-01 00:00:00 UTC+0000

. 0x822f1020:smss.exe 368 4 3 19 2012-07-22 02:42:31 UTC+0000

.. 0x82298700:winlogon.exe 608 368 23 519 2012-07-22 02:42:32 UTC+0000

..... 0x8205bda0:wuauclt.exe 1588 1004 5 132 2012-07-22 02:44:01 UTC+0000

..... 0x821fcda0:wuauclt.exe 1136 1004 8 173 2012-07-22 02:43:46 UTC+0000

.... 0x82311360:svchost.exe 824 652 20 194 2012-07-22 02:42:33 UTC+0000

.... 0x820e8da0:alg.exe 788 652 7 104 2012-07-22 02:43:01 UTC+0000

.... 0x82295650:svchost.exe 1220 652 15 197 2012-07-22 02:42:35 UTC+0000

... 0x81e2a3b8:lsass.exe 664 608 24 330 2012-07-22 02:42:32 UTC+0000

.. 0x822a0598:csrss.exe 584 368 9 326 2012-07-22 02:42:32 UTC+0000

. 0x81e7bda0:reader\_sl.exe 1640 1484 5 39 2012-07-22 02:42:36 UTC+0000

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

//////////////////////////////////////////////////////////////////////////////////////////////////////////

**Commande pour voir tous les ports qui ont été utilisés :**

PS D:\tmp\vm\volatility\_2.6\_win64\_standalone> .\volatility\_2.6\_win64\_standalone.exe -f "D:\tmp\vm\cridex.vmem" --profile=WinXPSP2x86 connscan

**Retour de la commande :**

Offset(P) Local Address Remote Address Pid

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

0x02087620 172.16.112.128:1038 41.168.5.140:8080 1484

0x023a8008 172.16.112.128:1037 125.19.103.198:8080 1484

Ici nous pouvons voir que la victime porte l’IP 172.16.112.128

Après quelques recherches sur internet nous avons trouvé que les ports 1037 et 1038 sont des ports contenant des failles

//////////////////////////////////////////////////////////////////////////////////////////////////////////

**Commande pour lister tous les processus qui ont été ouverts :**

PS D:\tmp\vm\volatility\_2.6\_win64\_standalone> .\volatility\_2.6\_win64\_standalone.exe -f "D:\tmp\vm\cridex.vmem" --profile=WinXPSP2x86 pslist

**Retour de la commande :**

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

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

0x823c89c8 System 4 0 53 240 ------ 0

0x822f1020 smss.exe 368 4 3 19 ------ 0 2012-07-22 02:42:31 UTC+0000

0x822a0598 csrss.exe 584 368 9 326 0 0 2012-07-22 02:42:32 UTC+0000

0x82298700 winlogon.exe 608 368 23 519 0 0 2012-07-22 02:42:32 UTC+0000

0x81eb17b8 spoolsv.exe 1512 652 14 113 0 0 2012-07-22 02:42:36 UTC+0000

0x81e7bda0 reader\_sl.exe 1640 1484 5 39 0 0 2012-07-22 02:42:36 UTC+0000

0x820e8da0 alg.exe 788 652 7 104 0 0 2012-07-22 02:43:01 UTC+0000

0x821fcda0 wuauclt.exe 1136 1004 8 173 0 0 2012-07-22 02:43:46 UTC+0000

0x8205bda0 wuauclt.exe 1588 1004 5 132 0 0 2012-07-22 02:44:01 UTC+0000

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

//////////////////////////////////////////////////////////////////////////////////////////////////////////

**Commandes pour voir toutes les connexions :**

volatility\_2.6\_win64\_standalone.exe -f cridex.vmem --profile=WinXPSP2x86 sockets

**Retour de la commande :**

Offset(V) PID Port Proto Protocol Address Create Time

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

0x81ddb780 664 500 17 UDP 0.0.0.0 2012-07-22 02:42:53 UTC+0000

0x82240d08 1484 1038 6 TCP 0.0.0.0 2012-07-22 02:44:45 UTC+0000

0x81dd7618 1220 1900 17 UDP 172.16.112.128 2012-07-22 02:43:01 UTC+0000

0x82125610 788 1028 6 TCP 127.0.0.1 2012-07-22 02:43:01 UTC+0000

0x8219cc08 4 445 6 TCP 0.0.0.0 2012-07-22 02:42:31 UTC+0000

0x81ec23b0 908 135 6 TCP 0.0.0.0 2012-07-22 02:42:33 UTC+0000

0x82276878 4 139 6 TCP 172.16.112.128 2012-07-22 02:42:38 UTC+0000

0x82277460 4 137 17 UDP 172.16.112.128 2012-07-22 02:42:38 UTC+0000

0x81e76620 1004 123 17 UDP 127.0.0.1 2012-07-22 02:43:01 UTC+0000

0x82172808 664 0 255 Reserved 0.0.0.0 2012-07-22 02:42:53 UTC+0000

0x81e3f460 4 138 17 UDP 172.16.112.128 2012-07-22 02:42:38 UTC+0000

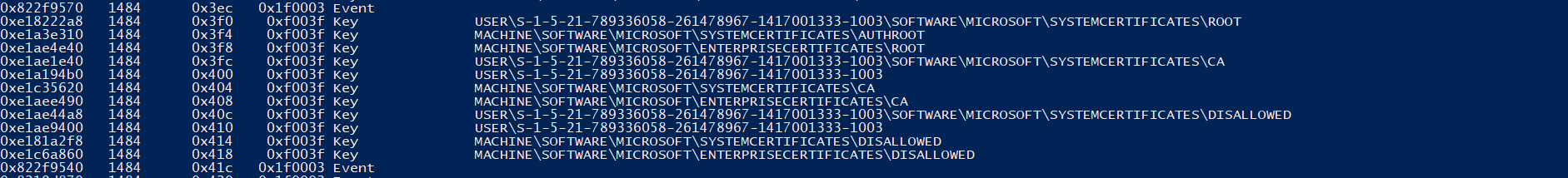
0x821f0630 1004 123 17 UDP 172.16.112.128 2012-07-22 02:43:01 UTC+0000

0x822cd2b0 1220 1900 17 UDP 127.0.0.1 2012-07-22 02:43:01 UTC+0000

0x82172c50 664 4500 17 UDP 0.0.0.0 2012-07-22 02:42:53 UTC+0000

0x821f0d00 4 445 17 UDP 0.0.0.0 2012-07-22 02:42:31 UTC+0000

//////////////////////////////////////////////////////////////////////////////////////////////////////////



Sur cette image nous pouvons qu’un utilisateur supprimé sur cette machine possédait des certificats sur le profil

# 2. Résumé de l’attaque

Pour résumer un **utilisateur** a dû ouvrir un fichier dans un **Adobe Reader DC** depuis un **lecteur amovible**

Par la suite un **Malware** s’est activé sur l’IP **41.168.5.140** (adresse Sud-Africaine) et **125.19.103.198** et a infecté le pc de l’utilisateur sur l’IP **172.16.112.128**

L’adresse Sud-Africaine a été trouvé grâce au site suivant : <https://ipinfo.io/41.168.5.140>

Un Malware portant le nom de « **cridex** » qui est de type « **Trojan** » est une forme de malware qui se spécialise dans le **vol d'informations d'identification bancaires** via un système qui utilise des macros de Microsoft Word.

Le site <https://www.malwareurl.com/ns_listing.php?ip=41.168.5.140> référence les IP malicieuse (ici nous pouvons voir que l’IP 41.168.5.140 y est référencé)

De plus sur le poste nous pouvons voir qu’un utilisateur a été supprimé