

PROJET : FORENSIQUE MEMOIRE AVEC VOLATILITY 2



La forensique de la mémoire est un sous-domaine crucial de la forensique numérique, qui implique l'acquisition et l'analyse de la mémoire volatile d'un ordinateur ou, en d'autres termes, de la RAM de l'ordinateur. Les informations stockées dans la RAM d'un ordinateur peuvent fournir des informations précieuses sur l'état du système au moment de l'acquisition.

La mémoire acquise est normalement appelée dump de mémoire et peut être particulièrement utile pour identifier les processus en cours, les informations d'identification des utilisateurs, les connexions réseau, les clés de registre, les clés de chiffrement, l'historique du navigateur, le contenu du presse-papiers et d'autres informations précieuses.

Dans ce projet nous analyserons la mémoire d'un ordinateur infectée par le malware cridex avec VOLATILITY2. Nous essayerons de récupérer des informations pertinentes durant cette investigation.

Le malware Cridex, est un type de cheval de Troie bancaire qui a été actif pendant plusieurs années.

Son principal objectif est de cibler les systèmes Windows afin de s'emparer d'informations sensibles, principalement des données financières telles que les identifiants de connexion bancaire, les informations de cartes de crédit, les données de comptes en ligne, ainsi que d'autres informations personnelles et confidentielles.

1. Détermination du profil à utiliser

Le plugin **imageinfo** permet de déterminer le profil de la machine utilisée afin de continuer dans les investigations.

Le profil est « WinXPSP2x86 ».

```
mdiaw@mdiaw: ~/Volatility
mdiaw@mdiaw:~/Volatility$ volatility -f cridex01.vmem imageinfo
Volatility Foundation Volatility Framework 2.6
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 (/home/mdiaw/Volatility/cridex01.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
mdiaw@mdiaw:~/Volatility$
```

2. Liste des processus

La liste des processus peut être affichée avec le plugin **pslist** comme le montre la capture suivante. Il permet également d'afficher les PID (Processus ID) et les PPID (Parent Processus ID).

Dans la capture ci-dessous un exécutable nommé **reader_sl.exe** avec le **PID 1640** attire notre attention mais nous nous pencherons dessus plus tard.

Nous pouvons également voir que l'exécutable « explorer.exe (PID 1484) », a ensuite exécuté le « **reader_sl.exe (1640)** ».

```
mdiaw@mdiaw:~/Volatility$ volatility -f cridex01.vmem --profile WinXPSP2x86 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V) Name PID PPID Thds Hnds Sess Wow64 Start
-----
x823c89c8 System 4 0 53 240 ----- 0
x822f1020 smss.exe 368 4 3 19 ----- 0 2012-07-22 02:42:31 UTC+0000
x822a0598 csrss.exe 584 368 9 326 0 0 2012-07-22 02:42:32 UTC+0000
x82298700 winlogon.exe 608 368 23 519 0 0 2012-07-22 02:42:32 UTC+0000
x81e2ab28 services.exe 652 608 16 243 0 0 2012-07-22 02:42:32 UTC+0000
x81e2a3b8 lsass.exe 664 608 24 330 0 0 2012-07-22 02:42:32 UTC+0000
x82311360 svchost.exe 824 652 20 194 0 0 2012-07-22 02:42:33 UTC+0000
x81e29ab8 svchost.exe 908 652 9 226 0 0 2012-07-22 02:42:33 UTC+0000
x823001d0 svchost.exe 1004 652 64 1118 0 0 2012-07-22 02:42:33 UTC+0000
x821dfda0 svchost.exe 1056 652 5 60 0 0 2012-07-22 02:42:33 UTC+0000
x82295650 svchost.exe 1220 652 15 197 0 0 2012-07-22 02:42:35 UTC+0000
x821dea70 explorer.exe 1484 1464 17 415 0 0 2012-07-22 02:42:36 UTC+0000
x81eb17b8 spoolsv.exe 1512 652 14 113 0 0 2012-07-22 02:42:36 UTC+0000
x81e7bda0 reader_sl.exe 1640 1484 5 39 0 0 2012-07-22 02:42:36 UTC+0000
x820e8da0 alg.exe 788 652 7 104 0 0 2012-07-22 02:43:01 UTC+0000
x821fcda0 wuauclt.exe 1136 1004 8 173 0 0 2012-07-22 02:43:46 UTC+0000
x8205bda0 wuauclt.exe 1588 1004 5 132 0 0 2012-07-22 02:44:01 UTC+0000
```

3.Arborescence des processus

Avec **pstree** nous pouvons voir l'arborescence des processus en cours. Cela permet de mettre en exergue les relations entre les PID et les PPID et de détecter des processus spécifiques.

```
mdiaw@mdiaw:~/Volatility$ volatility -f cridex01.vmem --profile WinXPSP2x86 pstree
Volatility Foundation Volatility Framework 2.6
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
... 0x81e2ab28:services.exe         652     608      16     243    2012-07-22 02:42:32 UTC+0000
.... 0x821dfa0:svchost.exe           1056     652        5       60    2012-07-22 02:42:33 UTC+0000
.... 0x81eb17b8:spoolsv.exe           1512     652      14     113    2012-07-22 02:42:36 UTC+0000
.... 0x81e29ab8:svchost.exe           908      652        9     226    2012-07-22 02:42:33 UTC+0000
.... 0x823001d0:svchost.exe           1004     652      64    1118    2012-07-22 02:42:33 UTC+0000
..... 0x8205bda0:wuauclt.exe           1588    1004        5     132    2012-07-22 02:44:01 UTC+0000
..... 0x821fcd0: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
. 0x821dea70:explorer.exe            1484    1464      17     415    2012-07-22 02:42:36 UTC+0000
. 0x81e7bda0:reader_sl.exe           1640    1484        5       39    2012-07-22 02:42:36 UTC+0000
```

4.Dissimulation de processus

Lors de l'affichage des processus, certains processus malveillants tentent de se cacher. Avec le plugin **psview** si les colonnes **pslist** et **pscan** affichent simultanément (ou l'une des deux) « **false** », cela témoigne d'un processus qui veut se cacher. Dans notre cas aucun processus essaie de se cacher.

```
mdiaw@mdiaw: ~/Volatility
mdiaw@mdiaw:~/Volatility$ volatility -f cridex01.vmem --profile WinXPSP2x86 psxview
Volatility Foundation Volatility Framework 2.6
Offset(P)  Name                               PID  pslist  pscan  thrddproc  pspcid  csrss  session  deskthrd  ExitTime
-----
0x02498700 winlogon.exe                       608  True    True    True       True    True  True     True     True
0x02511360 svchost.exe                         824  True    True    True       True    True  True     True     True
0x022e8da0 alg.exe                     788  True    True    True       True    True  True     True     True
0x020b17b8 spoolsv.exe                 1512 True    True    True       True    True  True     True     True
0x0202ab28 services.exe               652  True    True    True       True    True  True     True     True
0x02495650 svchost.exe               1220 True    True    True       True    True  True     True     True
0x0207bda0 reader_sl.exe             1640 True    True    True       True    True  True     True     True
0x025001d0 svchost.exe               1004 True    True    True       True    True  True     True     True
0x02029ab8 svchost.exe               908  True    True    True       True    True  True     True     True
0x023fcd0 wuauclt.exe                 1136 True    True    True       True    True  True     True     True
0x0225bda0 wuauclt.exe                 1588 True    True    True       True    True  True     True     True
0x0202a3b8 lsass.exe                  664  True    True    True       True    True  True     True     True
0x023dea70 explorer.exe               1484 True    True    True       True    True  True     True     True
0x023dfd0 svchost.exe               1056 True    True    True       True    True  True     True     True
0x024f1020 smss.exe                  368  True    True    True       True    False False    False
0x025c89c8 System                     4    True    True    True       True    False False    False
0x024a0598 csrss.exe                  584  True    True    True       True    False True     True
```

5. Les connexion réseaux

Pour voir les connexions réseaux nous faisons appel au plugin « **connscan** ». Nous pouvons constater que l'adresse IP local **172.16.112.128** a noué des connexions avec 2 adresses IPs à distance que sont **41.168.5.140** et **125.19.103.198** au niveau du port 8080.

```
mdiaw@mdiaw:~/Volatility$ volatility -f cridex01.vmem --profile WinXPSP2x86 connscan
Volatility Foundation Volatility Framework 2.6
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
```

Faisons une petite analyse avec Virus Total pour savoir si ces 2 adresses IPs sont malveillantes ou pas.

L'analyse sur VT montrent que ces IPs sont malveillantes comme le prouve les 2 captures ci-dessous.

The image shows two screenshots of the VirusTotal interface. The top screenshot is for IP address 125.19.103.198 (125.19.0.0/16), AS 9498 (BHARTI Airtel Ltd.). It shows a Community Score of 4/94 and 4/94 security vendors flagged this IP address as malicious. The bottom screenshot is for IP address 41.168.5.140 (41.168.0.0/15), AS 36937 (Neotel). It shows a Community Score of 5/94 and 5/94 security vendors flagged this IP address as malicious. Both screenshots show a table of security vendors' analysis results.

Security vendors' analysis	125.19.103.198 (125.19.0.0/16)	41.168.5.140 (41.168.0.0/15)
alphaMountain.ai	Malicious	Malicious
Dr.Web	Malicious	Malicious
MalwareURL	Malware	Malware
Webroot	Malicious	Malicious
CyRadar		Malicious
Dr.Web		Malicious
MalwareURL		Malware

6. Lignes de commandes et analyse d'exécutable malveillant

Le plugin « **cmdline** » nous permet d'afficher les commandes de voir les commandes récemment exécutées. Nous faisons un focus sur les PID 1640 et PID 1484.

```
mdiaw@mdiaw:~/Volatility$ volatility -f cridex01.vmem --profile WinXPSP2x86 cmdline
Volatility Foundation Volatility Framework 2.6
*****

explorer.exe pid: 1484
Command line : C:\WINDOWS\Explorer.EXE
*****
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"
*****
```

Nous allons extraire l'exécutable du PID 1640 et l'analysons sur virus total avec procdump.

```
mdiaw@mdiaw:~/Volatility$ volatility -f cridex01.vmem --profile WinXPSP2x86 procdump -p 1640 -D .
Volatility Foundation Volatility Framework 2.6
Process(V) ImageBase Name Result
-----
0x81e7bda0 0x00400000 reader_sl.exe OK: executable.1640.exe
mdiaw@mdiaw:~/Volatility$
```

Une fois chargé sur VIRUS TOTAL, nous constatons que l'exécutable du PID 1640 est classé comme malicieux comme le montre la capture ci-dessous.

5b136147911b041f0126ce82dfd24c4e2c79553b65d3240ecea2dcab4452dcb5

AcroSpeedLaunch.exe

Size: 28.50 KB | Last Analysis Date: 1 month ago

Community Score: 26 / 71

26/71 security vendors flagged this file as malicious

peexe | idle | direct-cpu-clock-access | checks-user-input

Popular threat label: trojan.multiop/r002c0djh24

Threat categories: trojan, pua

Family labels: multiop, r002c0djh24

Security vendors' analysis:

Vendor	Detection
Alibaba	Trojan:Win32/Multiop.788dce0e
CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cylance	Unsafe
AliCloud	Trojan:Win/Multiop.Gen
CTX	Exe.trojan.multiop
DeepInstinct	MALICIOUS

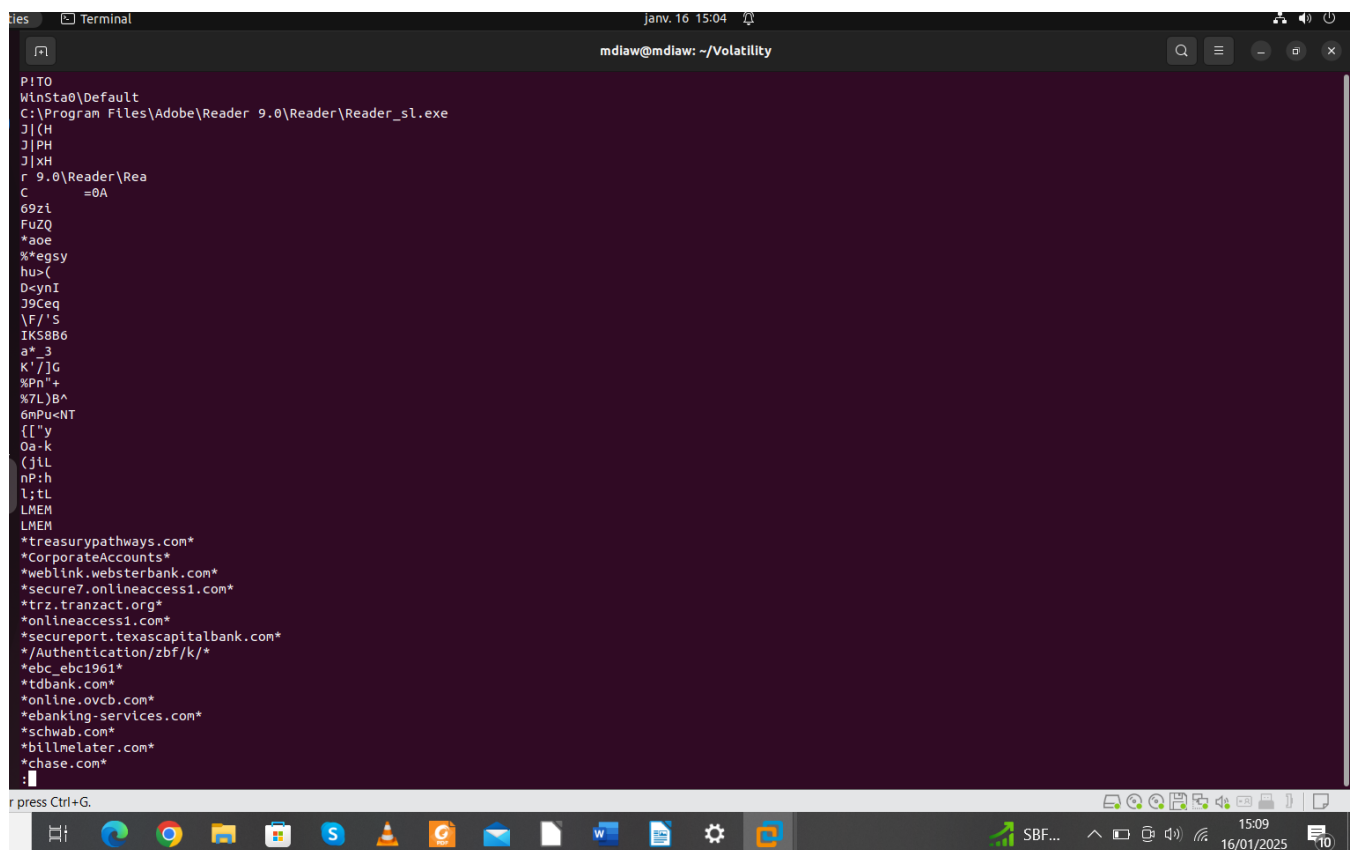
We use cookies and related technologies to remember user preferences, for security, to analyse our traffic, and to enable website functionality. Learn more about cookies in our [Privacy Notice](#).

Analysons le dump de la mémoire de l'exécutable du PID 1640 pour trouver plus de preuve.

```
mdiaw@mdiaw:~/Volatility$ volatility -f cridex01.vmem --profile WinXPSP2x86 memdump -p 1640 -D .
Volatility Foundation Volatility Framework 2.6
*****
Writing reader_sl.exe [ 1640] to 1640.dmp
```

L'analyse du dump mémoire d'avec le plugin strings nous permet de voir les chaînes de caractères brutes traduites de la mémoire. Plusieurs caractères pouvant correspondre à des organismes bancaires peuvent être identifiés dans la capture ci-dessous.

```
mdiaw@mdiaw:~/Volatility$ strings 1640.dmp | less
```



```
P!TO
WinSta0\Default
C:\Program Files\Adobe\Reader 9.0\Reader\Reader_sl.exe
J!(H
J!PH
J!xH
r 9.0\Reader\Rea
C
=0A
69zi
FUZQ
*aoe
%*egsy
hu>(
D<synI
J9Ceq
\F/'S
IKS8B6
a*_3
K/'jG
%Pn'+
%7L)B^
6mPu<NT
{['y
0a-k
(jiL
nP:h
l;tL
LMEM
LMEM
*treasurypathways.com*
*CorporateAccounts*
*weblink.websterbank.com*
*secure7.onlineaccess1.com*
*trrz.tranzact.org*
*onlineaccess1.com*
*secureport.texascapitalbank.com*
*/Authentication/zbf/k/*
*ebc_ebc1961*
*tdbank.com*
*online.ovcb.com*
*ebanking-services.com*
*schwab.com*
*billmelater.com*
*chase.com*
:
```