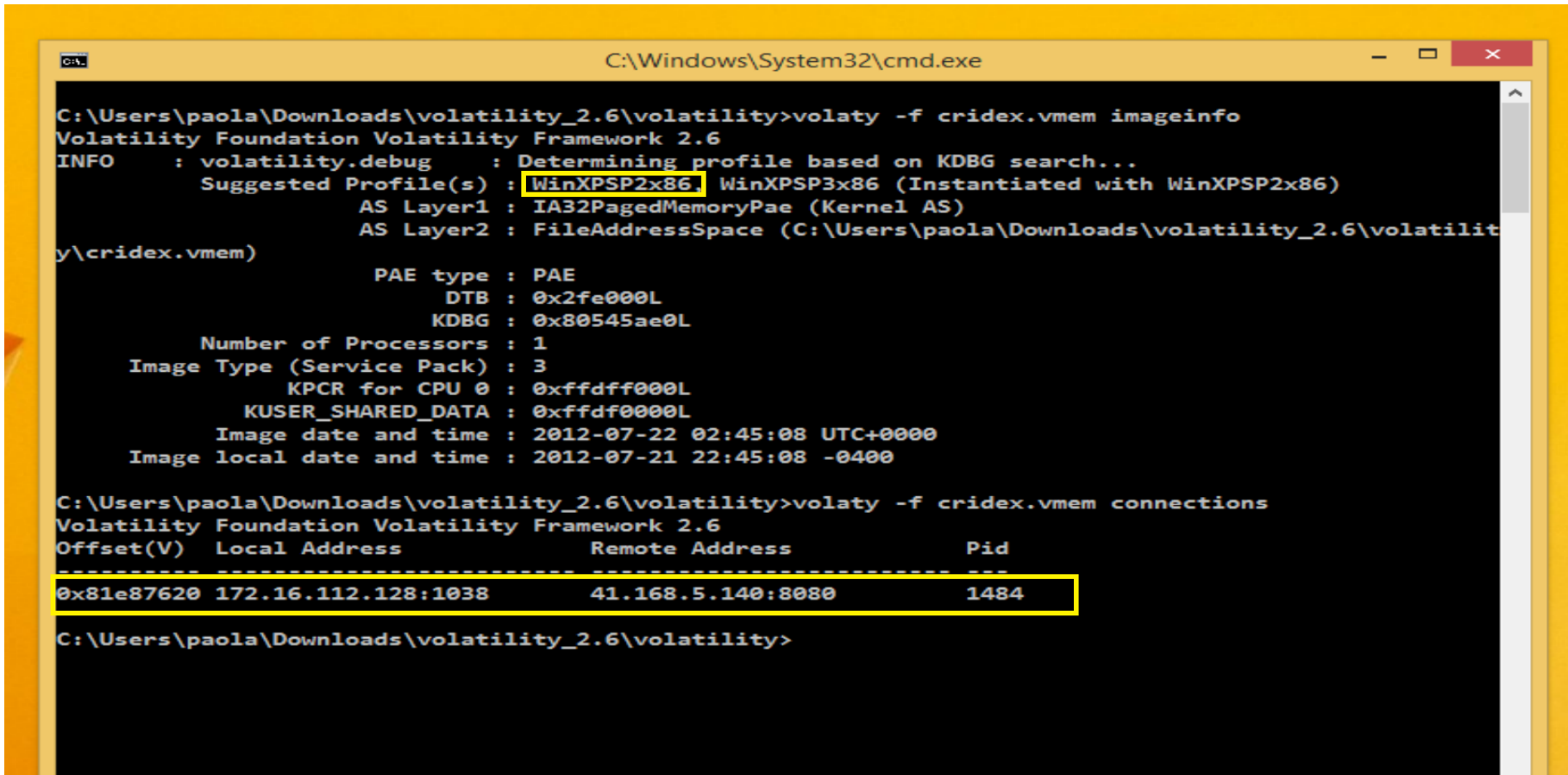


Programa usado: Volatility para la extraccion de informacion en arcrivo cridex.vmem



```
C:\Users\paola\Downloads\volatility_2.6\volatility>volatyl -f cridex.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 (C:\Users\paola\Downloads\volatility_2.6\volatilit
y\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

C:\Users\paola\Downloads\volatility_2.6\volatility>volatyl -f cridex.vmem connections
Volatility Foundation Volatility Framework 2.6
Offset(V)  Local Address          Remote Address          Pid
-----
0x81e87620 172.16.112.128:1038          41.168.5.140:8080          1484

C:\Users\paola\Downloads\volatility_2.6\volatility>
```

La imagen pudo haber sido sacada desde una windows XP Service pack 2 el 21-22 de julio de 2012

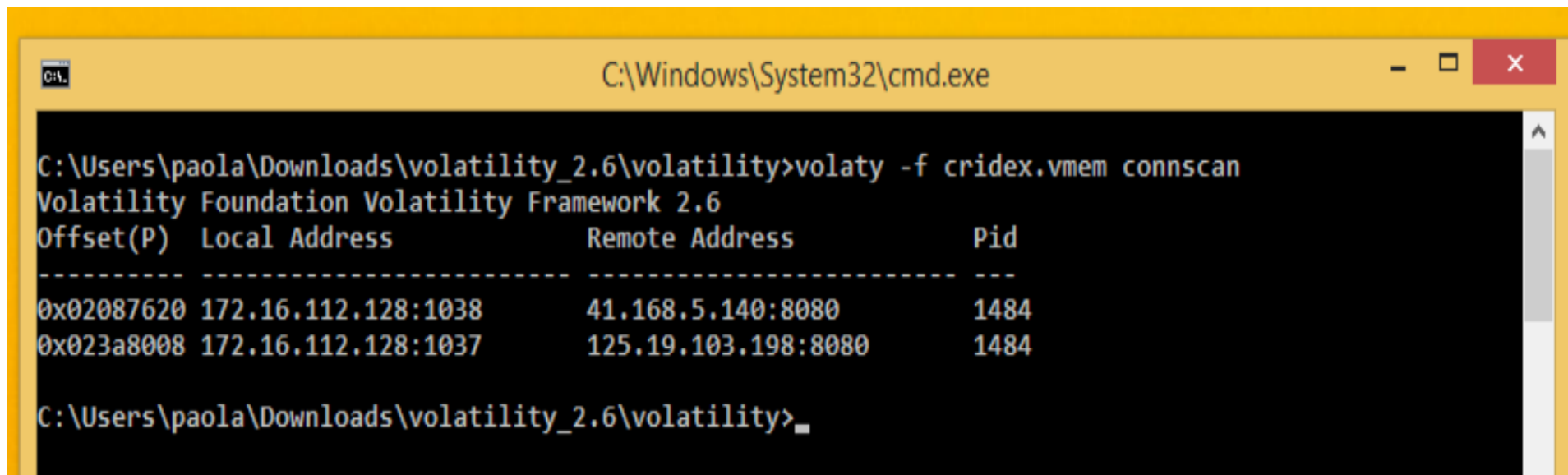
La IP de la maquina de la que se obtuvo la Imagen es 172.16.112.128 con una coneccion remota a 41.168.5.140 con Process ID 1484

C:\Windows\System32\cmd.exe									
Offset(V) Exit	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	
0x823c89c8	System	4	0	53	240	-----	0		
0x822f1020 0000	smss.exe	368	4	3	19	-----	0	2012-07-22 02:42:31	UTC+
0x822a0598 0000	csrss.exe	584	368	9	326	0	0	2012-07-22 02:42:32	UTC+
0x82298700 0000	winlogon.exe	608	368	23	519	0	0	2012-07-22 02:42:32	UTC+
0x81e2ab28 0000	services.exe	652	608	16	243	0	0	2012-07-22 02:42:32	UTC+
0x81e2a3b8 0000	lsass.exe	664	608	24	330	0	0	2012-07-22 02:42:32	UTC+
0x82311360 0000	svchost.exe	824	652	20	194	0	0	2012-07-22 02:42:33	UTC+
0x81e29ab8 0000	svchost.exe	908	652	9	226	0	0	2012-07-22 02:42:33	UTC+
0x823001d0 0000	svchost.exe	1004	652	64	1118	0	0	2012-07-22 02:42:33	UTC+
0x821dfda0 0000	svchost.exe	1056	652	5	60	0	0	2012-07-22 02:42:33	UTC+
0x82295650 0000	svchost.exe	1220	652	15	197	0	0	2012-07-22 02:42:35	UTC+
0x821dea70 0000	explorer.exe	1484	1464	17	415	0	0	2012-07-22 02:42:36	UTC+
0x81eb17b8 0000	spoolsv.exe	1512	652	14	113	0	0	2012-07-22 02:42:36	UTC+
0x81e7bda0 0000	reader_sl.exe	1640	1484	5	39	0	0	2012-07-22 02:42:36	UTC+
0x820e8da0 0000	alg.exe	788	652	7	104	0	0	2012-07-22 02:43:01	UTC+
0x821fcda0 0000	wuauclt.exe	1136	1004	8	173	0	0	2012-07-22 02:43:46	UTC+
0x8205bda0 0000	wuauclt.exe	1588	1004	5	132	0	0	2012-07-22 02:44:01	UTC+

proceso 1484 .140:8080 Explorer.exe (1464) 02:42:36

proceso 1640(reader\_sl) anidado a proceso 1484(explorer.exe) 02:42:36

al parecer el reader\_sl se ejecuta una vez se abre el explorer

A screenshot of a Windows command prompt window. The title bar is yellow and contains the text 'C:\Windows\System32\cmd.exe'. The command prompt shows the execution of 'volatyl -f cridex.vmem connscan' in the directory 'C:\Users\paola\Downloads\volatility\_2.6\volatility'. The output displays two network connections from process 1484. The first connection is to 41.168.5.140:8080 at local address 172.16.112.128:1038. The second connection is to 125.19.103.198:8080 at local address 172.16.112.128:1037. The prompt ends with a cursor on a new line.

```
C:\Users\paola\Downloads\volatility_2.6\volatility>volatyl -f cridex.vmem 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
C:\Users\paola\Downloads\volatility_2.6\volatility>
```

al capturar esta memoria habia 2 conecciones usando el proceso 1484(explorer.exe)

1° a la IP 41.168.5.140

2° a la IP 125.19.103.198

```
C:\Windows\System32\cmd.exe

C:\Users\paola\Downloads\volatility_2.6\volatility>volatyl -f cridex.vmem cmdline
Volatility Foundation Volatility Framework 2.6
*****
System pid:      4
*****
smss.exe pid:    368
Command line :  \SystemRoot\System32\smss.exe
*****
csrss.exe pid:   584
Command line :  C:\WINDOWS\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,30
ServerDll=baserv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConSer
ff MaxRequestThreads=16
*****
winlogon.exe pid: 608
Command line :  winlogon.exe
*****
services.exe pid: 652
Command line :  C:\WINDOWS\system32\services.exe
*****
lsass.exe pid:   664
Command line :  C:\WINDOWS\system32\lsass.exe
*****
svchost.exe pid: 824
Command line :  C:\WINDOWS\system32\svchost -k DcomLaunch
*****
svchost.exe pid: 908
Command line :  C:\WINDOWS\system32\svchost -k rpcss
*****
svchost.exe pid: 1004
Command line :  C:\WINDOWS\System32\svchost.exe -k netsvcs
*****
svchost.exe pid: 1056
Command line :  C:\WINDOWS\system32\svchost.exe -k NetworkService
*****
svchost.exe pid: 1220
Command line :  C:\WINDOWS\system32\svchost.exe -k LocalService
*****
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"
*****
```

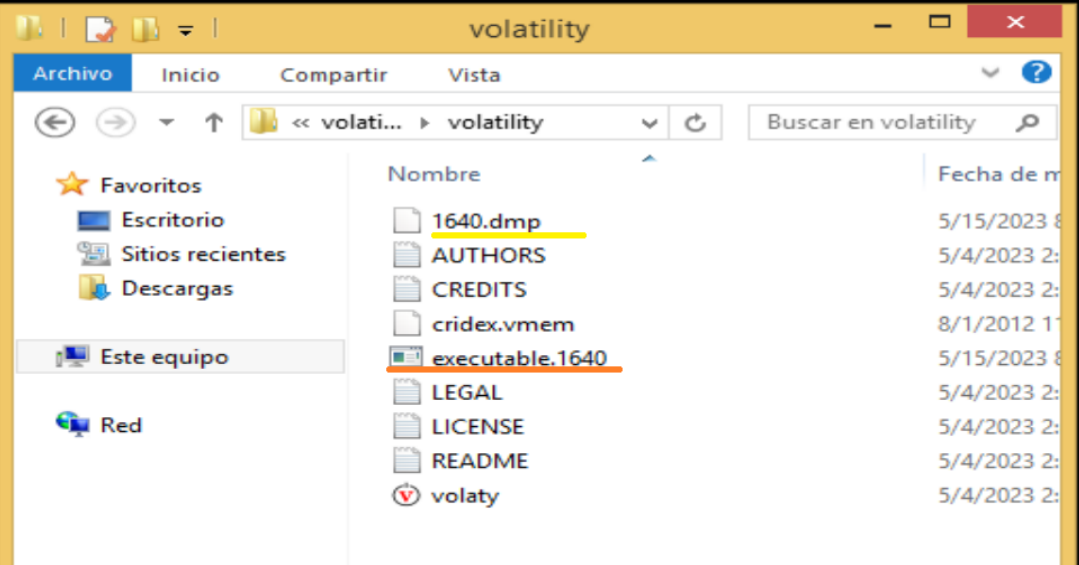
el proceso 1640 ubicado en C:\Program Files\Adobe\Reader 9.0\ Reader\Reader\_sl.exe

Se puede apreciar que el ejecutable Reader\_sl.exe se podria haber disfrazado dentro el programa Adobe Reader

```
C:\Users\paola\Downloads\volatility_2.6\volatility>volatyl -f cridex.vmem -p 1640 memdump -D c:/Users/paola/Downloads/volatility_2.6/volatility
Volatility Foundation Volatility Framework 2.6
Writing reader_sl.exe [ 1640] to 1640.dmp

C:\Users\paola\Downloads\volatility_2.6\volatility>volatyl -f cridex.vmem -p 1640 procdump -D c:/Users/paola/Downloads/volatility_2.6/volatility
Volatility Foundation Volatility Framework 2.6
Process(V) ImageBase Name Result
0x81e7bda0 0x00400000 reader_sl.exe OK: executable.1640.exe

C:\Users\paola\Downloads\volatility_2.6\volatility>
```



Se extrajo el archivo Reader\_sl.exe usando 2 metodos:  
memdump del cual se obtuvo el archivo 1640.dmp  
procdump del caul se obtuvo el ejecutable executable.1640

WINDOWS8.1 [Corriendo] - Oracle VM VirtualBox

VirusTotal - File - a18fa7d736daad7e5453a3ee6f96dd3d73677d461640.dmp

https://www.virustotal.com/gui/file/a18fa7d736daad7e5453a3ee6f96dd3d73677d461640.dmp 67%

a18fa7d736daad7e5453a3ee6f96dd3d73677d461640.dmp

1 / 59

1 security vendor and no sandboxes flagged this file as malicious

a18fa7d736daad7e5453a3ee6f96dd3d73677d461640.dmp 73.63 MB 2023-04-23 19:29:39 UTC 21 days ago

Community Score

DETECTION DETAILS COMMUNITY

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

Security vendors' analysis ⓘ Do you want to automate checks?

Ikarus	Phishing.JS.Agent	Acronis (Static ML)	Undetected
AhnLab-V3	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	AVG	Undetected

Analisis con virus total del archivo obtenido a traves de memdump

VirusTotal - File - 5b136147911b041f0126ce82dfd24c4e2c79553b0ecea2dcab4452dob5

https://www.virustotal.com/gui/file/5b136147911b041f0126ce82dfd24c4e2c79553b0ecea2dcab4452dob5 67%

5b136147911b041f0126ce82dfd24c4e2c79553b0ecea2dcab4452dob5

35 / 70

35 security vendors and no sandboxes flagged this file as malicious

5b136147911b041f0126ce82dfd24c4e2c79553b0ecea2dcab4452dob5  
AcroSpeedLaunch.exe  
28.50 KB  
Size  
2023-05-10 10:51:38 UTC  
5 days ago  
EXE

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

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

Popular threat label **trojan.multip/r002c0ddo21** Threat categories trojan pus Family labels multip r002c0ddo21

Security vendors' analysis Do you want to automate checks?

Alibaba	Trojan:Win32/Multip.788dce0e	ALYac	Trojan.GenericKD.41512677
Arcabit	Trojan.Generic.D2796EE5	BitDefender	Trojan.GenericKD.41512677
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cybereason	Malicious.3f5a91
Cylance	Unsafe	DeepInstinct	MALICIOUS
Emsisoft	Trojan.GenericKD.41512677 (B)	eScan	Trojan.GenericKD.41512677
Fortinet	PossibleThreat	GData	Trojan.GenericKD.41512677
Google	Detected	Ikarus	Trojan.Win32.Patched
K7AntiVirus	Riskware ( 0040eff71 )	K7GW	Riskware ( 0040eff71 )
Lionio	Trojan.Win32.Generic.41c	Malwarebytes	Generic.Malware/Suspicious
MAX	Malware (ai Score=99)	MaxSecure	Trojan.Malware.1728101.susgen

Analisis con virus total del archivo obtenido a traves de procdump