Lab Assignment 2

Volatility Memory Forensics

Darisi Priyatham

Roll No: 2021BCY0016

Cridex.vmem file

- `volatility -f cridex . vmem imageinfo` – To get the information about this image file

```
D:\cyber\volatility_2.6>volatility -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 (D:\cyber\volatility_2.6\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
```

- `volatility -f cridex . vmem pslist` – This command give us list of all processes running (it doesnot include all the hidden processes and to get hidden processes use *psxview*)
- From the pid and ppid we can tell if a cretain process is parent / child.

```
D:\cyber\volatility_2.6>volatility -f cridex.vmem pslist
Volatility Foundation Volatility Framework 2.6
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
0x81e2ab28 services.exe            652    608     16      243      0      0 2012-07-22 02:42:32 UTC+0000
0x81e2a3b8 lsass.exe               664    608     24      330      0      0 2012-07-22 02:42:32 UTC+0000
0x82311360 svchost.exe             824    652     20      194      0      0 2012-07-22 02:42:33 UTC+0000
0x81e29ab8 svchost.exe             908    652      9      226      0      0 2012-07-22 02:42:33 UTC+0000
0x823001d0 svchost.exe            1004    652     64     1118      0      0 2012-07-22 02:42:33 UTC+0000
```

- `volatility -f cridex.vmem pstree`
- Observation :
  - reader_sl.exe is the child of explorer process so it should have formed after 2:42:36
  - So they shouldn't have initiated at same time so this is a suspicious file .
  - we can get this observation from pslist as well but pstree gives better understanding of the parent child relationship

```
D:\cyber\volatility_2.6>volatility -f cridex.vmem 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
.... 0x821dfda0: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
..... 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
 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
```

- `volatility -f cridex.vmem cmdline -p 1640` – to get the path of this reader_sl.exe file
- Observation :
  - It shows that it is coming from adobe

```
D:\cyber\volatility_2.6>volatility -f cridex.vmem cmdline -p 1640
Volatility Foundation Volatility Framework 2.6
**************************************************************************
reader_sl.exe pid:   1640
Command line : "C:\Program Files\Adobe\Reader 9.0\Reader\Reader_sl.exe"
```

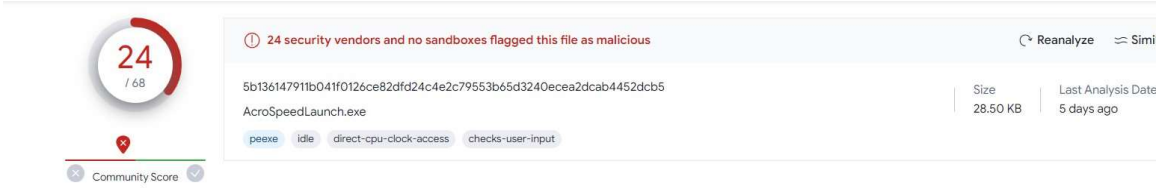
- `volatility -f cridex.vmem connscan` – To know with what all external ip addresses this file is making connections

```
D:\cyber\volatility_2.6>volatility -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
```

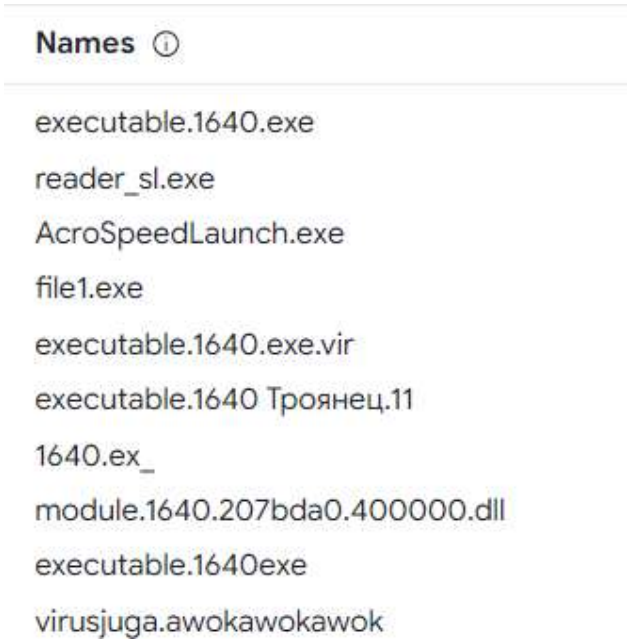
- `volatility -f cridex.vmem procdump –p 1640 --dump-dir.` – This command creates a procedure dump of the reader_sl.exe

- ```
  D:\cyber\volatility_2.6>volatility -f cridex.vmem procdump -p 1640 --dump-dir .
  Volatility Foundation Volatility Framework 2.6
  Process(V) ImageBase  Name                 Result
  ---------- ---------- -------------------- ------
  0x81e7bda0 0x00400000 reader_sl.exe        OK: executable.1640.exe
  ```

  Using virustotal we can check the percentage of virus in this procdump file



  - Here in details we can see what other file names this same



  virus has been seen

- `volatility -f cridex.vmem malfind -p 1640 -D.` – finds the code that malfind assumes as corrupted and now this is being dumped in a directory D We can upload this on virustotal to check.

- `volatility -f cridex.vmem memdump –p 1640 --dump-dir.` – This
  ```

generates memory dump of the file

- `strings 1640. dmp > 1640. txt` – this creates a txt file with all the strings in text format

```
D:\cyber\volatility_2.6>volatility -f cridex.vmem memdump -p 1640 --dump-dir .
Volatility Foundation Volatility Framework 2.6
************************************************************************
Writing reader_sl.exe [  1640] to 1640.dmp

D:\cyber\volatility_2.6>strings 1640.dmp > 1640.txt

Strings v2.54 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2021 Mark Russinovich
Sysinternals - www.sysinternals.com
```

- `strings 1640. dmp I grep –i "41.168.5.140:8080"` – Checks if the ip we got from connscan is present in this mem dump file.

```
D:\cyber\volatility_2.6>strings 1640.dmp | grep -i "41.168.5.140:8080"
http://41.168.5.140:8080/zb/v_01_a/in/
Host: 41.168.5.140:8080
```

  - Run this ip on http://passivedns.mnemonic.no

- Conclusion
  - In the above process we got to know that the Cridex.vmem file has virus in reader_sl.exe file and we also found to which ip it is making connection with.

Stage 2 :The malware can persist on both ram and hard disk

Checking for persistence

- `volatility -f cridex.vmem hivelist` – to check if this virus is trying to persisit

```
D:\cyber\volatility_2.6>volatility -f cridex.vmem hivelist
Volatility Foundation Volatility Framework 2.6
Virtual    Physical   Name
---------- ---------- ----
0xe18e5b60 0x093f8b60 \Device\HarddiskVolume1\Documents and Settings\Robert\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1a19b60 0x0a5a9b60 \Device\HarddiskVolume1\Documents and Settings\Robert\NTUSER.DAT
0xe18398d0 0x08a838d0 \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe18614d0 0x08e624d0 \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.DAT
0xe183bb60 0x08e2db60 \Device\HarddiskVolume1\Documents and Settings\NetworkService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe17f2b60 0x08519b60 \Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSER.DAT
0xe1570510 0x07669510 \Device\HarddiskVolume1\WINDOWS\system32\config\software
0xe1571008 0x0777f008 \Device\HarddiskVolume1\WINDOWS\system32\config\default
0xe15709b8 0x076699b8 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
0xe15719e8 0x0777f9e8 \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
0xe13ba008 0x02e4b008 [no name]
0xe1035b60 0x02ac3b60 \Device\HarddiskVolume1\WINDOWS\system32\config\system
0xe102e008 0x02a7d008 [no name]
```

  This is showing registery info

- `volatility -f cridex.vmem printkey -K "Software\Microsoft\Windows\CurrentVersion\Run"` - this cmd to get key

```
----------------------------
Registry: \Device\HarddiskVolume1\Documents and Settings\Robert\NTUSER.DAT
Key name: Run (S)
Last updated: 2012-07-22 02:31:51 UTC+0000

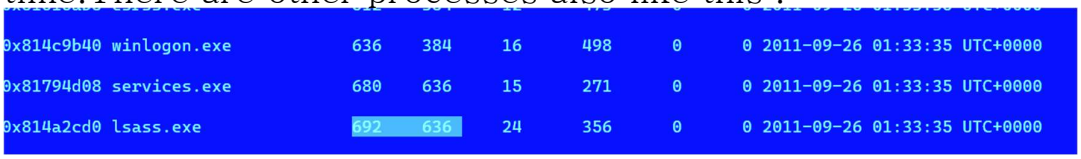
Subkeys:

Values:
REG_SZ        KB00207877.exe  : (S) "C:\Documents and Settings\Robert\Application Data\KB00207877.exe"
----------------------------
```

  - This is suspicious bec it comes from documents from user Robert • This was the file that was brought into hardisk which persisted the malware.

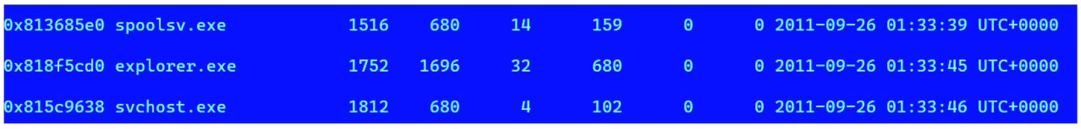
shylock.vmem file

- `pslist` :
- Observation :
  - here we can see that parent and child are created at same time.There are other processes also like this .



```
0x814c9b40 winlogon.exe           636    384     16      498      0      0 2011-09-26 01:33:35 UTC+0000
0x81794d08 services.exe           680    636     15      271      0      0 2011-09-26 01:33:35 UTC+0000
0x814a2cd0 lsass.exe              692    636     24      356      0      0 2011-09-26 01:33:35 UTC+0000
```

  - here explorer doesn't have a parent. Now this is going to be our first priority to check rather than all above proccesses.



```
0x813685e0 spoolsv.exe           1516    680     14      159      0      0 2011-09-26 01:33:39 UTC+0000
0x818f5cd0 explorer.exe          1752   1696     32      680      0      0 2011-09-26 01:33:45 UTC+0000
0x815c9638 svchost.exe           1812    680      4      102      0      0 2011-09-26 01:33:46 UTC+0000
```

- `cmdline` :
  - We got the pid and its path

```
**************************************************
explorer.exe pid:   1752
Command line : C:\WINDOWS\Explorer.EXE
**************************************************
```

- `connscan` :
- Observation :

- All outside ips this explorer is contacting

```
D:\cyber\volatility_2.6>volatility -f shylock.vmem connscan
Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------ ------------------------- ---
0x014f6ab0 10.0.0.109:1072          209.190.4.84:443          1752
0x01507380 10.0.0.109:1073          209.190.4.84:443          1752
0x016c2b00 10.0.0.109:1065          184.173.252.227:443       1752
0x017028a0 10.0.0.109:1067          184.173.252.227:443       1752
0x01858cb0 10.0.0.109:1068          209.190.4.84:443          1752
```

handles in whole memdump but I gave the explorer id `dlllist -p 1752`

to get its dump

- Observation :
  - we can see it is running some cryptographic processes which explorer is not supposed to do.

```
0x77120000    0x8b000     0xffff C:\WINDOWS\system32\OLEAUT32.dll
0x7e290000   0x173000     0xffff C:\WINDOWS\system32\SHDOCVW.dll
0x77a80000    0x95000     0xffff C:\WINDOWS\system32\CRYPT32.dll
0x77b20000    0x12000     0xffff C:\WINDOWS\system32\MSASN1.dll
0x754d0000    0x80000     0xffff C:\WINDOWS\system32\CRYPTUI.dll
0x5b860000    0x55000     0xffff C:\WINDOWS\system32\NETAPI32.dll
```

- `malfind` :
  - it gave all the processes which have mlaware

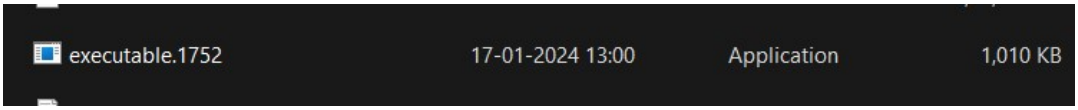
```
D:\cyber\volatility_2.6>volatility -f shylock.vmem malfind
Volatility Foundation Volatility Framework 2.6
Process: csrss.exe Pid: 612 Address: 0x7f6f0000
Vad Tag: Vad  Protection: PAGE_EXECUTE_READWRITE
Flags: Protection: 6

0x7f6f0000  c8 00 00 00 5c 01 00 00 ff ee ff ee 08 70 00 00   ....\........
0x7f6f0010  08 00 00 00 00 fe 00 00 00 00 10 00 00 20 00 00   ............
0x7f6f0020  00 02 00 00 00 20 00 00 8d 01 00 00 ff ef fd 7f   ............
0x7f6f0030  03 00 08 06 00 00 00 00 00 00 00 00 00 00 00 00   ............

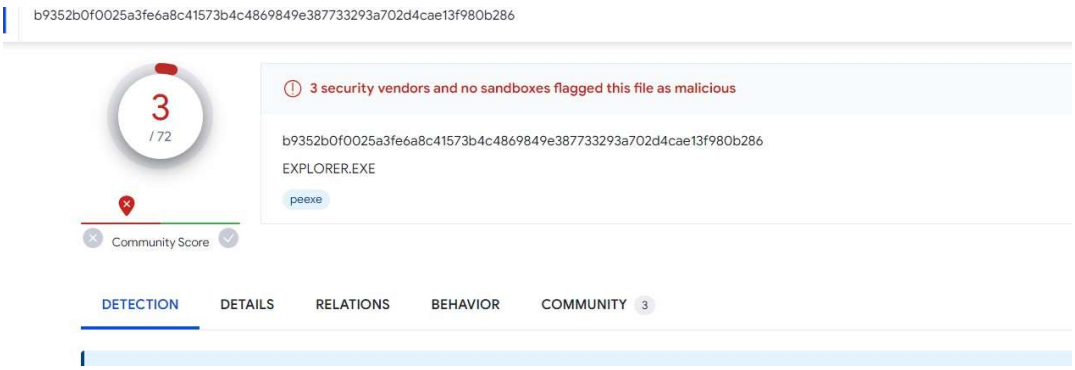
0x7f6f0000 c8000000          ENTER 0x0, 0x0
0x7f6f0004 5c                POP ESP
0x7f6f0005 0100              ADD [EAX], EAX
0x7f6f0007 00ff              ADD BH, BH
0x7f6f0009 ee                OUT DX, AL
0x7f6f000a ff                DB 0xff
0x7f6f000b ee                OUT DX, AL
0x7f6f000c 087000            OR [EAX+0x0], DH
0x7f6f000f 0008              ADD [EAX], CL
0x7f6f0011 0000              ADD [EAX], AL
0x7f6f0013 0000              ADD [EAX], AL
0x7f6f0015 fe00              INC BYTE [EAX]
```

- `malfind -p 1752` – for this explorer process
- Observation :
  - Result on virustotal clearly shows this file has virus

- `procdump -p 1752` :
  - dump – excecutable file is created



- Observation :
  - Putting this excecutable on virustotal shows us less amount where as the malfind file which we uploaded showed more bec that one has all the code files which are malicious and this has everythingdumped inside.



`memdump ans strings` : changes the dump file to txt file

```
D:\cyber\volatility_2.6>volatility -f shylock.vmem memdump -p 1752 --dump-dir .
Volatility Foundation Volatility Framework 2.6
************************************************************************
Writing explorer.exe [  1752] to 1752.dmp

D:\cyber\volatility_2.6>strings 1752.dmp>1752.txt
```

- Checking for persistence

`volatility -f shylock.vmem hivelist` – to check if this virus is trying to persist

-

```
D:\cyber\volatility_2.6>volatility -f shylock.vmem hivelist
Volatility Foundation Volatility Framework 2.6
Virtual    Physical   Name
---------- ---------- ----
0xe19d9a48 0x0e97ca48 \Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSER.DAT
0xe1610008 0x0c7d0008 \Device\HarddiskVolume1\WINDOWS\system32\config\software
0xe160e4c0 0x0c8424c0 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
0xe1610b60 0x0c7d0b60 \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
0xe1618008 0x0c7da008 \Device\HarddiskVolume1\WINDOWS\system32\config\default
0xe13c4570 0x0246f570 [no name]
0xe1018388 0x02200388 \Device\HarddiskVolume1\WINDOWS\system32\config\system
0xe1008b60 0x020c4b60 [no name]
0xe17cf008 0x045e1008 \Device\HarddiskVolume1\Documents and Settings\Administrator\Local Settings\Application Data\
soft\Windows\UsrClass.dat
0xe17a1520 0x04572520 \Device\HarddiskVolume1\Documents and Settings\Administrator\NTUSER.DAT
0xe1e292a0 0x007d52a0 \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Application Data\
oft\Windows\UsrClass.dat
0xe1e25b60 0x007d1b60 \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.DAT
0xe19e0008 0x0e90a008 \Device\HarddiskVolume1\Documents and Settings\NetworkService\Local Settings\Application Dat
osoft\Windows\UsrClass.dat
```

- This is showing registery info
- `volatility -f cridex.vmem printkey -K "Software\Microsoft\Windows\CurrentVersion\Run"` this cmd to get key

```
D:\cyber\volatility_2.6>volatility -f shylock.vmem printkey -K "Software\Microsoft\Windows\CurrentVersion\Run"
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSER.DAT
Key name: Run (S)
Last updated: 2009-12-27 01:38:21 UTC+0000

Subkeys:

Values:
----------------------------
Registry: \Device\HarddiskVolume1\Documents and Settings\Administrator\NTUSER.DAT
Key name: Run (S)
Last updated: 2011-09-30 00:25:35 UTC+0000

Subkeys:

Values:
REG_SZ        ctfmon.exe      : (S) C:\WINDOWS\system32\ctfmon.exe
REG_SZ        {919863BF-D426-AA00-979B-DF55477F92A7} : (S) C:\Documents and Settings\Administrator\Application Data\Intuit\Quicken\Log\rdshost.exe
----------------------------
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\default
Key name: Run (S)
Last updated: 2009-12-26 20:26:10 UTC+0000

Subkeys:

Values:
----------------------------
Registry: \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.DAT
Key name: Run (S)
Last updated: 2009-12-27 01:38:24 UTC+0000

Subkeys:

Values:
```

- Conclusion :
  - We concluded explore file is corrupted
  - Then checked in virustotal
  - Found the persistance as well