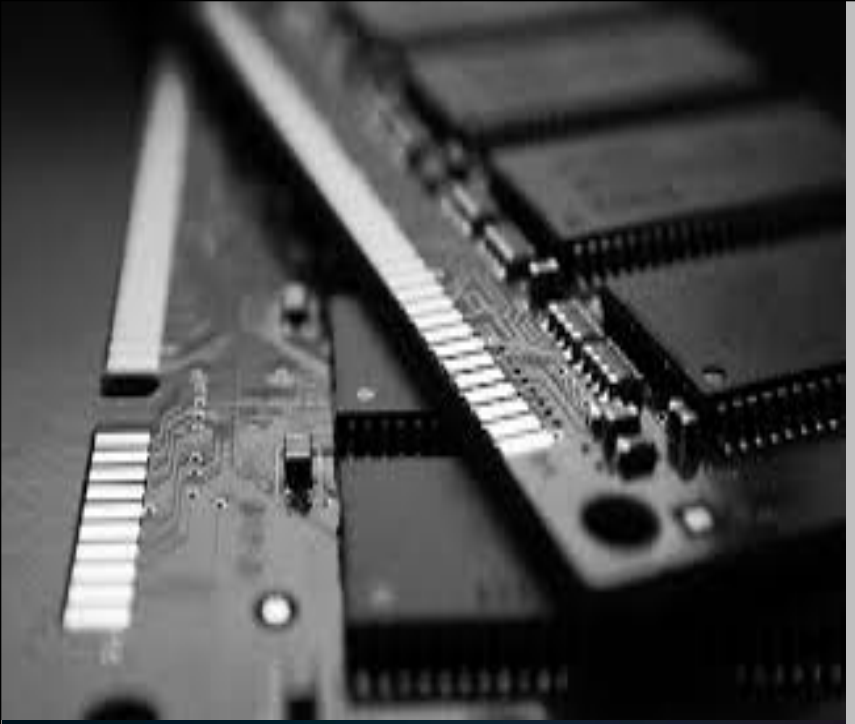


volatility

MEMORY FORENSICS

BY:MESHAL NASSER

What is Volatility?

Volatility is a command line memory analysis and forensics tool for extracting artifacts from memory dumps.

is an open-source memory forensics framework for incident response and malware analysis.

Cridex Malware

In this presentation, I will do analysis against Cridex malware.

Image Information.

Before we start the analysis we need to know the profile of the image by running the command bellow:

```
┌──(root💀 kali)-[~/Desktop/Volimages]
└─# volatility -f /root/Desktop/Volimages/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 (/root/Desktop/Volimages/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
```

>its clear now , we can see the profile of the image.

Pslist command.

Now let run the pslist command.

Pslist command is : Print all runnig processes by following the EPROCESS lists.

```
┌──(root㉿kali)-[~/Desktop/Volimages]
└─# volatility -f /root/Desktop/Volimages/cridex.vmem --profile=WinXPSP2x86 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
0x821dfda0 svchost.exe            1056    652      5       60      0      0 2012-07-22 02:42:33 UTC+0000
0x82295650 svchost.exe            1220    652     15      197      0      0 2012-07-22 02:42:35 UTC+0000
0x821dea70 explorer.exe           1484   1464     17      415      0      0 2012-07-22 02:42:36 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
```

Pslist command.

According to the screenshot in the previous slide we can tell that :

reader_sl.exe looks suspicious and need further analysis.

>explorer.exe has run reader_sl.exe

Active connections.

Lets run the command bellow to check for open connections.

Connections command is :Print list of open connections.

Now its clear , there is an active connections holding PID : 1484.

```
┌──(root💀 kali)-[~/Desktop/Volimages]
└─# volatility -f /root/Desktop/Volimages/cridex.vmem --profile=WinXPSP2x86 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
```

Active connections.

When we take the IP that we found it in previous slide and run it on virustotal we found it suspicious.

Finding malware.

Now , we going to use malfind command.

malfind command is : Find hidden and injected code.

Again the command found those process as a suspicious.

```
Process: reader_sl.exe Pid: 1640 Address: 0x3d0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 33, MemCommit: 1, PrivateMemory: 1, Protection: 6
```

```
Process: explorer.exe Pid: 1484 Address: 0x1460000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 33, MemCommit: 1, PrivateMemory: 1, Protection: 6
```

Dumping Processes & Memory

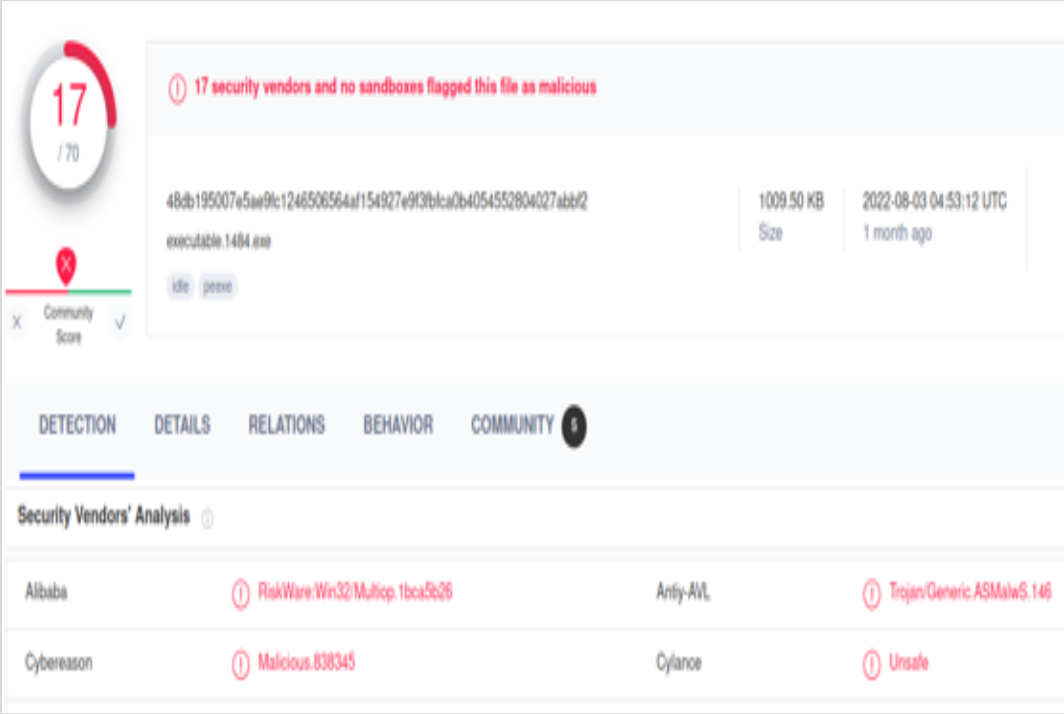
Now we are going to dump the processes and run it in virustotal or any threat intelligence tool.

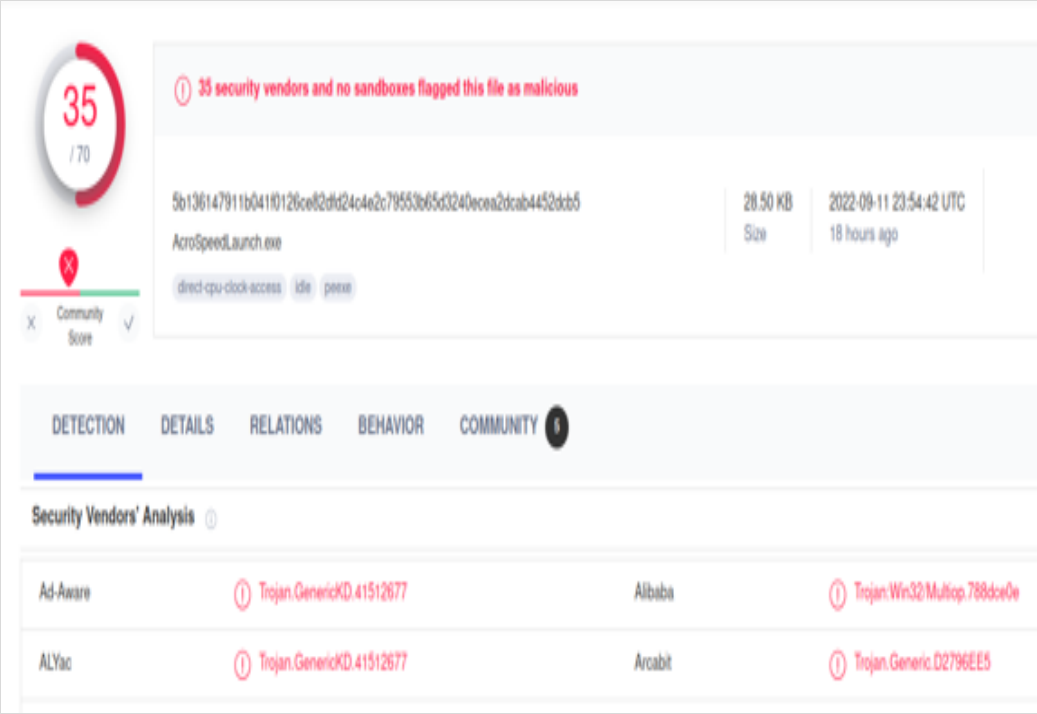
```
┌──(root💀 kali)-[~/Desktop/Volimages]
└─# volatility -f /root/Desktop/Volimages/cridex.vmem --profile=WinXPSP2x86 procdump -p 1640 -D /root/Desktop/Volimag
es
Volatility Foundation Volatility Framework 2.6
Process(V) ImageBase  Name             Result
────────── ───────── ──────────────── ──────
0x81e7bda0 0x00400000 reader_sl.exe      OK: executable.1640.exe

┌──(root💀 kali)-[~/Desktop/Volimages]
└─# volatility -f /root/Desktop/Volimages/cridex.vmem --profile=WinXPSP2x86 memdump -p 1640 -D /root/Desktop/Volimage
s
Volatility Foundation Volatility Framework 2.6
************************************************************************
Writing reader_sl.exe [  1640] to 1640.dmp
```

```
┌──(root💀 kali)-[~/Desktop/Volimages]
└─# volatility -f /root/Desktop/Volimages/cridex.vmem --profile=WinXPSP2x86 procdump -p 1484 -D /root/Desktop/Volimag
es
Volatility Foundation Volatility Framework 2.6
Process(V) ImageBase  Name             Result
────────── ───────── ──────────────── ──────
0x821dea70 0x01000000 explorer.exe       OK: executable.1484.exe

┌──(root💀 kali)-[~/Desktop/Volimages]
└─# volatility -f /root/Desktop/Volimages/cridex.vmem --profile=WinXPSP2x86 memdump -p 1484 -D /root/Desktop/Volimage
s
Volatility Foundation Volatility Framework 2.6
************************************************************************
Writing explorer.exe [  1484] to 1484.dmp
```

Virustotal.

Finally, we took the dump process .exe and run it on Virustotal.





References:

https://www.computerhope.com/jargon/c/cridex-malware.htm

https://www.volatilityfoundation.org/

Thank You