

# 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 below:

```
(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 : 0xfffff000L
      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 running processes by following the EPROCESS lists.

```
(root@kali) [~/Desktop/Volimages]
# volatility -f /root/Desktop/Volimages/cridex.vmem --profile=WinXPSP2-x86 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     0     2012-07-22 02:42:31 UTC+0000
0x822f1020 smss.exe              368  4     3    19    0     0     2012-07-22 02:42:32 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
0x821fcd00 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.

```
(rootkali)-[~/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.

**4** / 94  
Community Score

**4** security vendors flagged this IP address as malicious

41.168.5.140 (41.168.0.0/15)  
AS 36937 (Necotel)

DETECTION    DETAILS    **RELATIONS**    COMMUNITY 5

**Passive DNS Replication (1)**

Date resolved	Detections	Resolver	Domain
2013-04-01	0 / 93	VirusTotal	support.tray-international.com

**Communicating Files (32)**

Scanned	Detections	Type	Name
2012-12-04	24 / 46	Win32 EXE	25c854592fd30b954d3208ec672bf1d1
2020-09-23	54 / 71	Win32 EXE	mmcshevt.dll
2021-11-30	58 / 67	Win32 EXE	KB00656625.exe
2021-11-11	55 / 66	Win32 EXE	1032-eee3908d5a285d01ba1fdcc2d02237aeb13569e2
2022-03-04	53 / 69	Win32 EXE	MFC100JPN.DLL
2013-04-22	11 / 45	Network capture	EK_Phoenix_2012-04.pcap
2021-10-14	56 / 65	Win32 EXE	kb00113312.exe
2013-04-19	38 / 44	Win32 EXE	cc96809bee59f0e45b367539c9292f6.exe
2015-08-10	7 / 56	Network capture	jennhwee.com-2012.05.13.pcap
2022-01-14	56 / 66	Win32 EXE	KB01108787.exe



# 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/Volimages

Volatility Foundation Volatility Framework 2.6
Process(V) ImageBase Name Result
-----
0x81e7bda0 0x00400000 reader_sl.exe OK: executable.1640.exe

Volatility Foundation Volatility Framework 2.6
# volatility -f /root/Desktop/Volimages/cridex.vmem --profile=WinXPSP2x86 memdump -p 1640 -D /root/Desktop/Volimages

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/Volimages

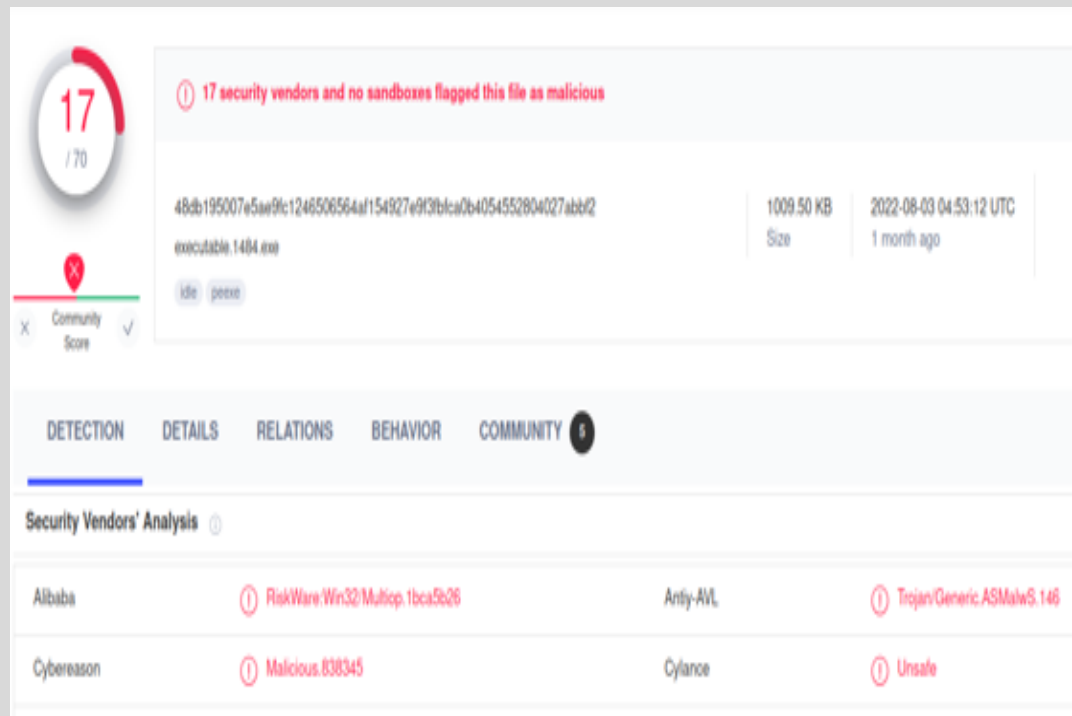
Volatility Foundation Volatility Framework 2.6
Process(V) ImageBase Name Result
-----
0x821dea70 0x01000000 explorer.exe OK: executable.1484.exe

Volatility Foundation Volatility Framework 2.6
# volatility -f /root/Desktop/Volimages/cridex.vmem --profile=WinXPSP2x86 memdump -p 1484 -D /root/Desktop/Volimages

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.



17 / 70

17 security vendors and no sandboxes flagged this file as malicious

48db195007e5ae9fc1246506564af154927e9f3fbca0b4054552804027abbf2  
executable.1484.exe

1009.50 KB  
Size

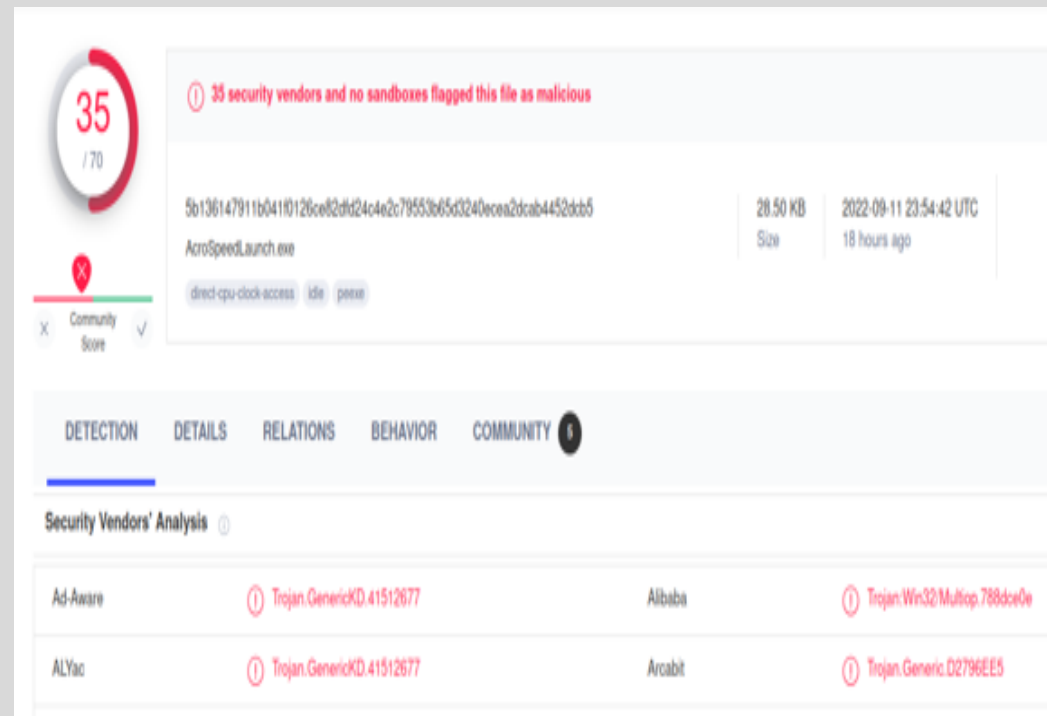
2022-08-03 04:53:12 UTC  
1 month ago

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Security Vendors' Analysis

Alibaba	RiskWare:Win32/Multip.1bca5b26	Antiy-AVL	Trojan.Generic.ASMalwS.146
Cybereason	Malicious.838345	Cylance	Unsafe



35 / 70

35 security vendors and no sandboxes flagged this file as malicious

5b136147911b041f0126ce82dd24c4e2c79553665d3240eeea2dcab4452dbb5  
AcroSpeedLaunch.exe

28.50 KB  
Size

2022-09-11 23:54:42 UTC  
18 hours ago

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Security Vendors' Analysis

Ad-Aware	Trojan.GenericKD.41512677	Alibaba	Trojan.Win32/Multip.788dce0e
ALYac	Trojan.GenericKD.41512677	Arcabit	Trojan.Generic.D2796EE5

# References:

---

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

<https://www.volatilityfoundation.org/>

Thank You

---