Malware
Memory Analysis

Memory Malware Analysis

Malware memory analysis is the process of examining a computer's memory (RAM) to detect and analyze malicious software (malware). This type of analysis helps identify malware that may not be visible on the hard drive and can reveal hidden or running malicious activities.

For beginners, the key points are:

- Memory (RAM): A temporary storage area that holds data and programs while the computer is in use.
- Malware: Malicious software designed to damage, disrupt, or gain unauthorized access to computer systems.
- Analysis: The examination of memory content to find suspicious patterns or behaviors indicative of malware.
-

Memory analysis involves using specialized tools to capture the contents of RAM and then scrutinize it for signs of malicious activity. This can include searching for hidden processes, network connections, and unusual patterns that are characteristic of malware.

Paper By

Diyar Saadi Ali

Malware
Memory Analysis

Why we need Malware Analysis ?

Malware memory analysis is essential because it provides a comprehensive approach to detecting and understanding malicious software that may not be visible or accessible through traditional file-based analysis methods. By examining the contents of a computer's RAM, analysts can identify malware that operates solely in memory, bypassing standard detection techniques that focus on the hard drive. This is particularly important for uncovering sophisticated threats that employ advanced evasion tactics to remain undetected.

Memory analysis allows for the detection of active malware processes, providing real-time insights into ongoing attacks and enabling quicker response and mitigation. It can reveal hidden processes, anomalous network connections, and suspicious behaviors that are indicative of malware activity. Furthermore, memory analysis can recover valuable volatile data, such as encryption keys, passwords, and session tokens, which are critical for understanding the full scope of an attack and potentially forensically linking different elements of a security breach.

Incorporating memory analysis into a security strategy enhances the overall ability to detect, analyze, and respond to threats, thereby improving the resilience and security of computer systems. This deeper level of analysis is vital for identifying and neutralizing advanced persistent threats (APTs) and other sophisticated forms of malware that traditional security measures might overlook.

Malware
Memory Analysis

Common Malware Analysis Toolkit

For memory forensics, several specialized tools are used to analyze the contents of a computer's memory (RAM) to detect and understand malicious activities. Here are some of the most common tools:

Memory Forensics Tools

1. Volatility Framework:
   - An open-source memory forensics framework for incident response and malware analysis.
   - Supports multiple operating systems and provides numerous plugins for extracting information from memory dumps, such as running processes, open network connections, and loaded drivers.
2. Rekall:
   - Another open-source memory forensics tool similar to Volatility, which originated as a fork of Volatility.
   - It offers powerful analysis capabilities and extensive documentation.
3. FTK Imager:
   - A tool by AccessData for creating forensic images of memory and other data sources.
   - It can capture live memory and is often used to acquire data before analysis.
4. LiME (Linux Memory Extractor):
   - A tool for acquiring memory dumps from Linux systems.
   - It allows the extraction of RAM content from volatile memory for forensic analysis.
5. Redline:
   - A tool by FireEye that provides host investigative capabilities, including memory and file analysis.
   - It assists in collecting memory dumps and analyzing them for signs of malicious activity.
6. MemDump:
   - A simple tool for dumping the contents of system memory to a file for later analysis.
   - Often used to create a snapshot of memory for offline analysis.
7. DumpIt:
   - A free tool for capturing memory from Windows systems.
   - It is easy to use and creates a memory dump that can be analyzed with other forensics tools.

Malware
Memory Analysis

Memory Analysis Study Case (Cridex)

Overview: Cridex (or Dridex) is a banking Trojan that employs advanced techniques to evade detection and facilitate the theft of financial information. Memory forensics is crucial in analyzing Cridex due to its ability to operate in memory and evade traditional file-based detection methods.

Memory Acquisition:

- Live Memory Dumping: Tools like FTK Imager or DumpIt are used to capture the contents of RAM while the system is running. This helps in analyzing the active processes and network connections associated with Cridex.

Memory Analysis Steps:

1. Using Volatility or Rekall:
   - Load the memory dump into a forensics tool like Volatility.
   - Use plugins to extract information about running processes, network sockets, and loaded DLLs.
2. Identifying Malicious Processes:
   - Look for processes that exhibit suspicious behavior, such as unusual names or those running from unexpected locations.
   - Check for injected code or modified processes that may indicate Cridex activity.
3. Network Connections:
   - Analyze active network connections to identify communications with known Cridex command and control servers.
   - Use the netscan or connscan plugins to identify any abnormal network activity.
4. Recovering Artifacts:
   - Extract artifacts like clipboard content, which might contain stolen information, or passwords saved in memory.
   - Use the cmdscan or consoles plugins to examine command history that might reveal user interactions with the malware.
5. Detecting Persistence Mechanisms:
   - Analyze the registry keys and services that might indicate how Cridex maintains persistence on the infected system.
   - Look for unusual entries that may have been created by the malware.

Malware
Memory Analysis

Tools and Sample Download Links .

- Volatility Framework 2 : https://github.com/volatilityfoundation/volatility/releases

- Dumpit Download Link : https://www.magnetforensics.com/resources/magnet-dumpit-for-windows/

- Cridex Malware Sample : https://ics.muni.cz/~valor/pv204/images/cridex.vmem.bz2

Malware
Memory Analysis

Tools and Sample Download Links .

- Volatility Framework 2 : https://github.com/volatilityfoundation/volatility/releases

- Dumpit Download Link : https://www.magnetforensics.com/resources/magnet-dumpit-for-windows/

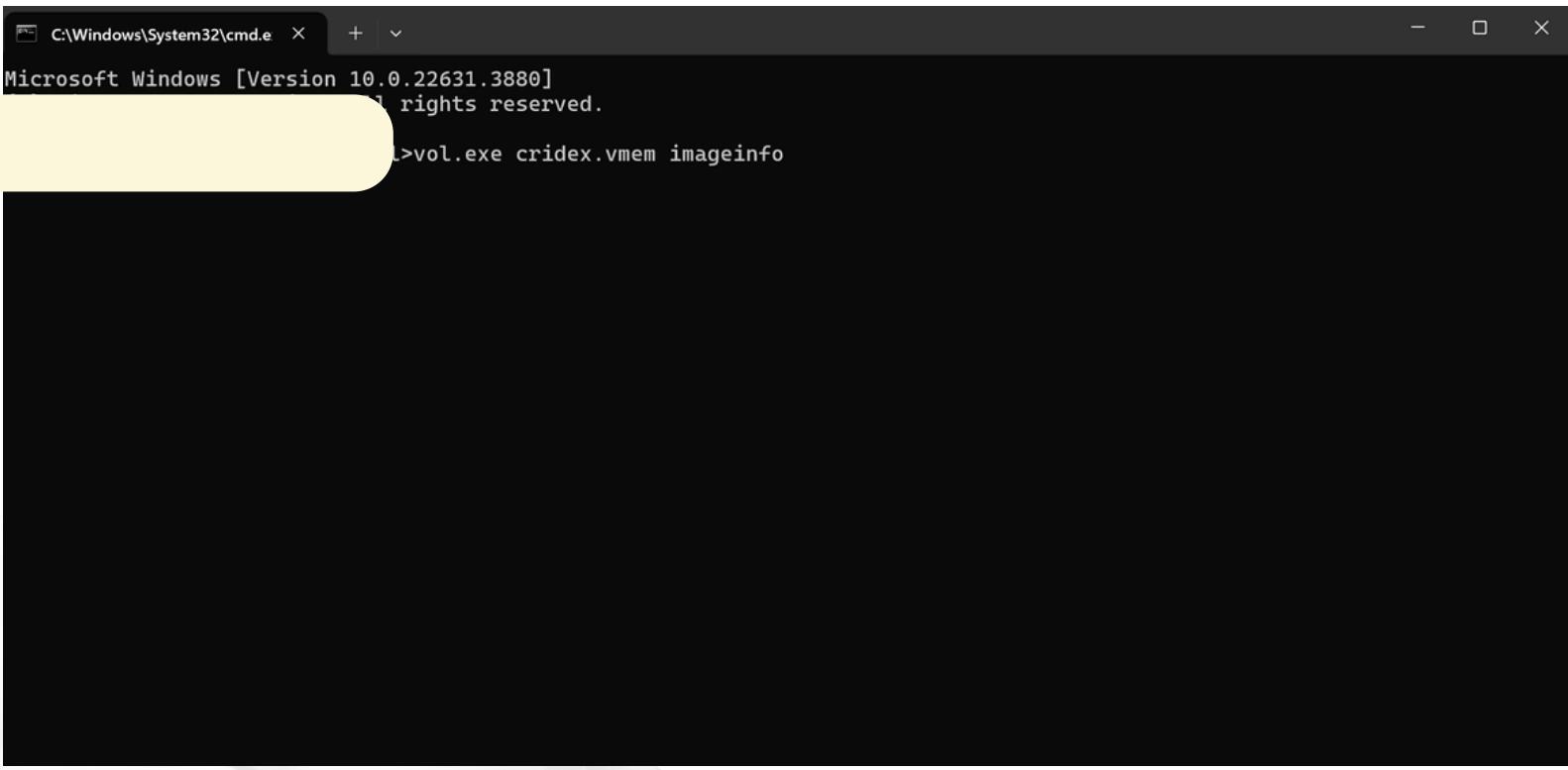
- Cridex Malware Sample : https://ics.muni.cz/~valor/pv204/images/cridex.vmem.bz2

Malware
Memory Analysis

Checking Image info of infected host

As security researcher or incident responder we should detect the image info of infected host machine regarding to profile parameter in volatility framework . because without indicating the profile of infected host machine it is not possible to use volatility framework and continue to analyzing our infected host machine

command to use : vol.exe -f cridex.vmem imageinfo



Malware
Memory Analysis

Checking Process List

In Volatility, checking the process list involves using the pslist plugin to extract and display a list of processes that were running in the memory image at the time it was captured. This information can be crucial for identifying suspicious or malicious processes.

command to use : vol.exe -f cridex.vmem --profile=WinXPSP3x86 pslist

C:\Windows\System32\cmd.e

```
vol.exe -f cridex.vmem --profile=WinXPSP3x86 pslist
 Framework 2.6
                             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
```

Malware
Memory Analysis

Checking Process Tree

In Volatility, checking the process tree involves using the pstree plugin, which provides a hierarchical view of all running processes at the time the memory image was captured. This visualization is useful for understanding the parent-child relationships between processes and identifying potentially malicious activity.

command to use : vol.exe -f cridex.vmem --profile=WinXPSP3x86 pstree

```
>vol.exe -f cridex.vmem --profile=WinXPSP3x86 pstree
ty 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
```

Malware
Memory Analysis

Common Tips During Checking Pslist #1

Regarding to your experience during memory analysis journey it is important to understand which process should have multiple running in infected machine . because there some process that should have only one time running not other . understanding this strategy will save you from wasting your time

Process Name	Description	Multiple Instances Normal?
`lsass.exe`	Local Security Authority Subsystem Service	No
`csrss.exe`	Client/Server Runtime Subsystem	No
`winlogon.exe`	Windows Logon Application	No
`services.exe`	Service Control Manager	No
`smss.exe`	Session Manager Subsystem	No
`wininit.exe`	Windows Initialization Process	No
`spoolsv.exe`	Printer Spooler Service	No
`system`	Kernel process	No
`msmpeng.exe`	Windows Defender Antivirus Service	No

Malware
Memory Analysis

Common Tips During Checking Pslist #2

Regarding to your experience during memory analysis journey it is important to understand which process should have multiple running in infected machine . because there some process that should have only one time running not other . understanding this strategy will save you from wasting your time

`msmpeng.exe`	Windows Defender Antivirus Service	No
`ctfmon.exe`	CTF Loader (Alternative User Input Text Input Processor)	Yes
`searchindexer.exe`	Windows Search Indexer	No
`wuauserv`	Windows Update Service	No
`sppsvc.exe`	Software Protection Platform Service	No
`wuauclt.exe`	Windows Update Client	Yes
`trustedinstaller.exe`	Windows Module Installer	Yes, if updates are running

Malware
Memory Analysis

Common Tips During Checking Pslist #3

Regarding to your experience during memory analysis journey it is important to understand which process should have multiple running in infected machine . because there some process that should have only one time running not other . understanding this strategy will save you from wasting your time

Process Name	Description	Multiple Instances Normal?
`msdt.exe`	Microsoft Support Diagnostic Tool	No
`mspmsnsv.exe`	Windows Media Player Network Sharing Service	No
`mspmsnsv.exe`	Windows Media Player Network Sharing Service	No
`dfrgui.exe`	Disk Defragmenter GUI	No
`rsvpsrv.exe`	Windows Remote Access Connection Manager	No
`dwm.exe`	Desktop Window Manager	No
`lpksetup.exe`	Language Pack Installer	No
`sfc.exe`	System File Checker	No
`wmiadap.exe`	WMI Performance Adapter	No
`iphlpsvc.dll`	IP Helper Service	No

Malware
Memory Analysis

Common Tips During Checking Pslist #4

Regarding to your experience during memory analysis journey it is important to understand which process should have multiple running in infected machine . because there some process that should have only one time running not other . understanding this strategy will save you from wasting your time

Process Name	Description	Multiple Instances Normal?
`winlogon.exe`	Windows Logon Application	No
`mspmsnsv.exe`	Windows Media Player Network Sharing Service	No
`msdtc.exe`	Microsoft Distributed Transaction Coordinator	No
`wuauserv`	Windows Update Service	No
`perfhost.exe`	Performance Host	No
`SystemSettings.exe`	Settings Application	No
`TaskHost.exe`	Task Host Process	No
`userinit.exe`	User Initialization process	No
`dcomcnfg.exe`	Component Services Configuration	No
`wbengine.exe`	Windows Backup Engine	No

Malware
Memory Analysis

Investigation Running Process Part 1

Investigating running processes is a crucial step in memory forensics, especially when analyzing for potential malware like Cridex. Here's how you can approach the investigation of running processes using tools like Volatility :

- Checking For Suspicious Process name
- Checking for Process with different parent process id (PPID)

in this case we have the process name known as reader_sl.exe

command to use : vol.exe -f cridex.vmem --profile=WinXPSP3x86 pslist

```
>vol.exe -f cridex.vmem --profile=WinXPSP3x86 pslist
y 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
0x81e7bda8 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
```

Investigation Running Process Part 1

While selecting the suspecious process name we will have to know what is the process functionality in additionw what is the purpose of this supecious process

What is Reader_sl.exe?

The genuine *Reader_sl.exe* file is a software component of *Adobe Acrobat* by *Adobe Systems*.
Reader_sl.exe is an executable file that belongs to Adobe Acrobat, a group of software and web services created by Adobe, to create, view, modify and print files in the Portable Document Format (PDF). Reader SpeedLauncher reduces the time required to launch Acrobat Reader. This is not a critical Windows component and should be removed if known to cause problems. Adobe Acrobat comes bundles with Reader (formerly Acrobat Reader), a freeware tool that can view, print and annotate PDF files; Acrobat (formerly Acrobat Exchange), a paid software that can create PDF documents; and Acrobat.com, a file hosting service. Adobe Systems Incorporated is an American software giant that develops software products for web design, video editing, web hosting, image editing, servers, as well as formats such as Flash and PDF. The company was established in 1982 by Charles Geschke and John Warnockin and is currently headquartered in San Jose, California.

based on the search that maybe a infected host machine has been compromised by malicious documents such as .pdf or .docx

Malware Memory Analysis

Investigation Running Process Part 1

another plugin from volatility we can use for indicating which process or which program created a reader_sl.exe because it can give us more indicator .

command to use : vol.exe -f cridex.vmem --profile=WinXPSP3x86 pstree

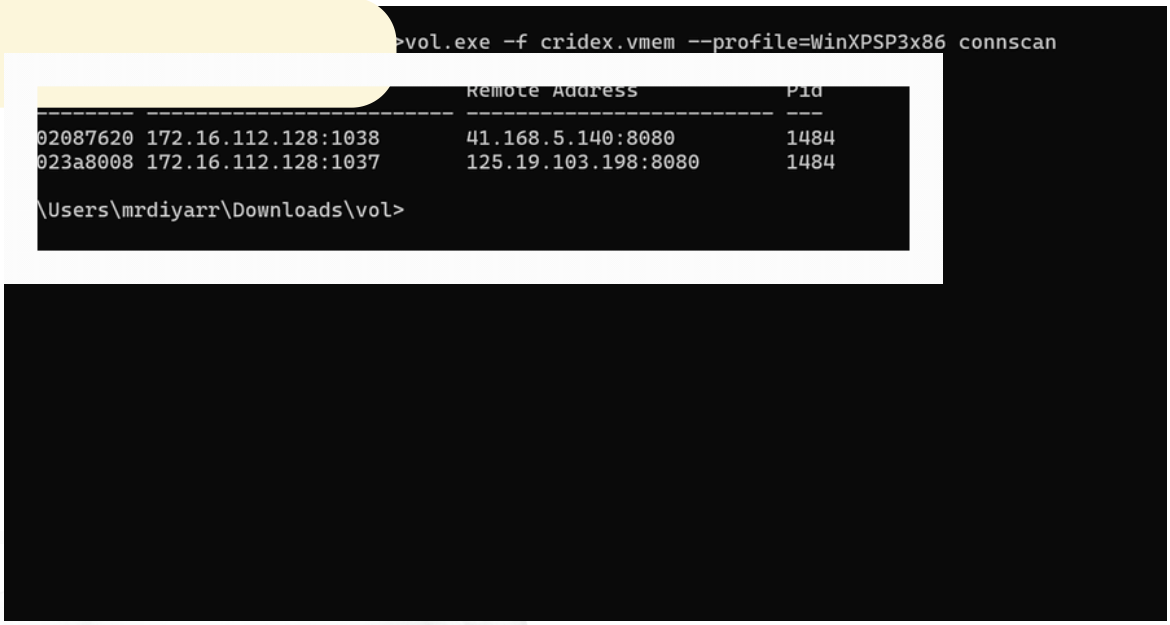
```
C:\Users\mrdiyarr\Downloads\vol>vol.exe -f cridex.vmem --profile=WinXPSP3x86 pstree
Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 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
                                                      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
```

based on the details of pstree plugin we have clue that explorer.exe is creating reader_sl.exe . it maybe lead to that infected host machine opened the malicious documents that recevied by attacker .

Investigating Process Internet Connection

Investigating a process's internet connection in memory forensics is crucial for identifying potential malicious activity, such as communication with command and control (C&C) servers. Here's how to conduct this investigation using Volatility:

command to use : vol.exe -f cridex.vmem --profile=WinXPSP3x86 connscan

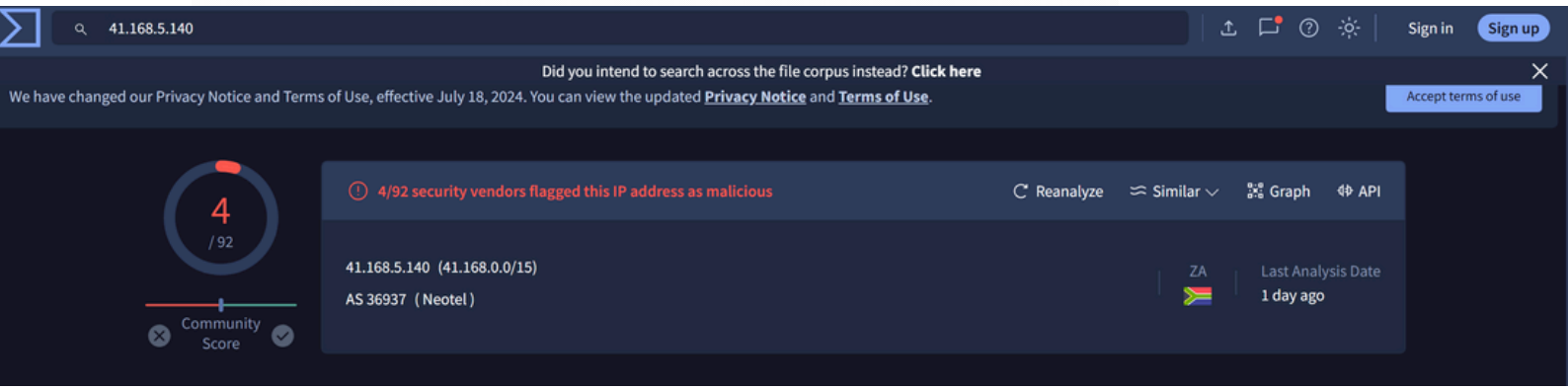


There two process made a connection with remote address on of them is explorer.exe and other one is suspected process reader_sl.exe . but we have to ask a logical question to us : why should reader_sl.exe make a internet connection ? let is check the remote IP Address on VirusTotal .

Note : 1484 is reader_sl.exe Parent Process ID (PPID)

Checking reader_sl.exe remote IP Address

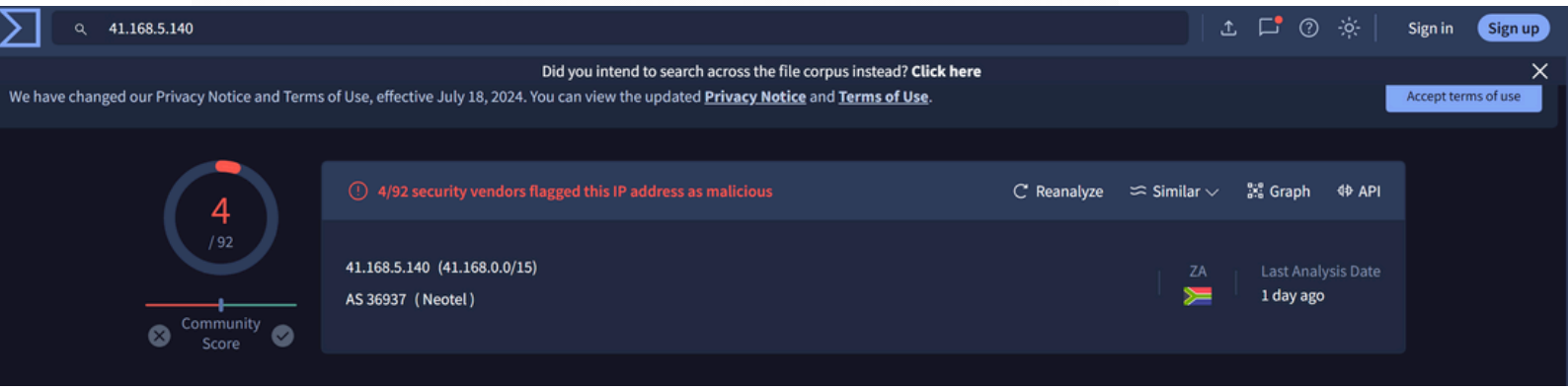
IDuring investigation the suspected process reader_sl.exe and their remote IP Address that tried to make a connection with it we will checking this remote IP Address on VT (VirusTotal) to indicate this Remote IP Address is malicious or not .



The Suspected reader_sl.exe process and their remote IP Address spotted by 4 detection engines as malicious . so we have the basic clue that there something wrong at infected host machine . let is continue our analysis .

Checking reader_sl.exe remote IP Address

IDuring investigation the suspected process reader_sl.exe and their remote IP Address that tried to make a connection with it we will checking this remote IP Address on VT (VirusTotal) to indicate this Remote IP Address is malicious or not .



The Suspected reader_sl.exe process and their remote IP Address spotted by 4 detection engines as malicious . so we have the basic clue that there something wrong at infected host machine . let is continue our analysis .

Malware
Memory Analysis

Checking Command History on Infected Host

Checking command history on an infected host is an important step in memory forensics, as it can reveal user interactions with the malware or other suspicious activities. Here's how to investigate command history using Volatility:

Command to use : vol.exe -f cridex.vmem --profile=WinXPSP3x86 cmdline

```
**************************************************
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
                                    ost.exe -k LocalService
**********************************  **********************************
xplorer.exe pid:   1484
ommand line : C:\WINDOWS\Explorer.EXE
**********************************  **********************************
spoolsv.exe pid:   1512
Command line : C:\WINDOWS\system32\spoolsv.exe
```

Note : Something abnormal available on cmdline plugin result . the real location of explorer.exe is C:\Windows\System32 . but in this case the explorer.exe location is C:/Windows . it may be process injection happened or replacing the legitimate explorer.exe to other one .

Malware
Memory Analysis

Checking DLL List of running process

Checking the DLL list of a running process is a critical step in memory forensics. It helps identify any loaded libraries that may be unusual or potentially malicious. Here's how to perform this task using Volatility:

Command to use : vol.exe -f cridex.vmem --profile=WinXPSP3x86 dlllist

```
vol.exe -f cridex.vmem --profile=WinXPSP3x86 dlllist
y Framework 2.6
************************************************************************
System pid:      4
Unable to read PEB for task.
************************************************************************
smss.exe pid:    368
Command line : \SystemRoot\System32\smss.exe


Base             Size  LoadCount Path
---------- ---------- ---------- ----
0x48580000     0xf000     0xffff \SystemRoot\System32\smss.exe
0x7c900000    0xaf000     0xffff C:\WINDOWS\system32\ntdll.dll
************************************************************************
csrss.exe pid:    584
Command line : C:\WINDOWS\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,3072,512 Windows=On SubSystemType=Windows ServerDll=basesrv
,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ProfileControl=Off MaxRequestThreads=16
Service Pack 3

Base             Size  LoadCount Path
---------- ---------- ---------- ----
0x4a680000     0x5000     0xffff \??\C:\WINDOWS\system32\csrss.exe
0x7c900000    0xaf000     0xffff C:\WINDOWS\system32\ntdll.dll
0x75b40000     0xb000     0xffff C:\WINDOWS\system32\CSRSRV.dll
0x75b50000    0x10000        0x3 C:\WINDOWS\system32\basesrv.dll
0x75b60000    0x4b000        0x2 C:\WINDOWS\system32\winsrv.dll
0x77f10000    0x49000        0x5 C:\WINDOWS\system32\GDI32.dll
0x7c800000    0xf6000       0x10 C:\WINDOWS\system32\KERNEL32.dll
0x7e410000    0x91000        0x6 C:\WINDOWS\system32\USER32.dll
0x7e720000    0xb0000        0x1 C:\WINDOWS\system32\sxs.dll
0x77dd0000    0x9b000        0x5 C:\WINDOWS\system32\ADVAPI32.dll
```

Checking for Malware malfind plugin

The malfind plugin in Volatility is a powerful tool for identifying potential malware within a memory dump. It scans for injected code or anomalous memory sections typically associated with malware. Here's how to use the malfind plugin effectively:

Command to use : vol.exe -f cridex.vmem --profile=WinXPSP3x86 malfind

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

0x003d0000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00   MZ..............
0x003d0010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ........@.......
0x003d0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x003d0030  00 00 00 00 00 00 00 00 00 00 00 00 e0 00 00 00   ................

0x003d0000 4d              DEC EBP
0x003d0001 5a              POP EDX
0x003d0002 90              NOP
0x003d0003 0003            ADD [EBX], AL
0x003d0005 0000            ADD [EAX], AL
0x003d0007 000400          ADD [EAX+EAX], AL
0x003d000a 0000            ADD [EAX], AL
0x003d000c ff              DB 0xff
0x003d000d ff00            INC DWORD [EAX]
0x003d000f 00b800000000    ADD [EAX+0x0], BH
0x003d0015 0000            ADD [EAX], AL
0x003d0017 004000          ADD [EAX+0x0], AL
0x003d001a 0000            ADD [EAX], AL
0x003d001c 0000            ADD [EAX], AL
0x003d001e 0000            ADD [EAX], AL
0x003d0020 0000            ADD [EAX], AL
0x003d0022 0000            ADD [EAX], AL
0x003d0024 0000            ADD [EAX], AL
0x003d0026 0000            ADD [EAX], AL
0x003d0028 0000            ADD [EAX], AL
0x003d002a 0000            ADD [EAX], AL
0x003d002c 0000            ADD [EAX], AL
0x003d002e 0000            ADD [EAX], AL
0x003d0030 0000            ADD [EAX], AL
0x003d0032 0000            ADD [EAX], AL
0x003d0034 0000            ADD [EAX], AL
0x003d0036 0000            ADD [EAX], AL
0x003d0038 0000            ADD [EAX], AL
0x003d003a 0000            ADD [EAX], AL
0x003d003c e000            LOOPNZ 0x3d003e
0x003d003e 0000            ADD [EAX], AL
```

Malware
Memory Analysis

Checking for files filescan plugin

The filescan plugin in Volatility is used to identify file objects in memory that may not have been mapped to disk, making it useful for detecting hidden or injected files used by malware. Here's how to use the filescan plugin effectively:

Command to use : vol.exe -f cridex.vmem --profile=WinXPSP3x86 filescan

```
>vol.exe -f cridex.vmem --profile=WinXPSP3x86 filescan
y Framework 2.6
nd Access Name
------------------ ------ ------ ------ ----
0x0000000001fd4db8      2      1 ------ \Device\Afd\Endpoint
0x0000000001fd6268      1      0 -W-r-d \Device\HarddiskVolume1\WINDOWS\system32\wbem\Logs\wbemcore.log
0x0000000001fdb490      1      0 R--r-d \Device\HarddiskVolume1\WINDOWS\system32\netui0.dll
0x0000000001fdf730      1      0 R--rwd \Device\HarddiskVolume1\Documents and Settings\Robert\Start Menu\Programs\Accessories\desktop.ini
0x0000000001fdf978      1      0 R--rwd \Device\HarddiskVolume1\Documents and Settings\Robert\Start Menu\Programs\desktop.ini
0x0000000001fdfaa0      3      1 R--rwd \Device\HarddiskVolume1\Documents and Settings\Robert\Local Settings\Application Data\Microsoft\CD Burning
0x0000000001fe1220      1      0 R--rwd \Device\HarddiskVolume1\Documents and Settings\Robert\My Documents\My Pictures\Desktop.ini
0x0000000001fe2028      1      1 ------ \Device\NamedPipe\browser
0x0000000001fe2a58      1      0 RW-rwd \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\desktop.ini
0x0000000001fe2df8      1      1 RW---- \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Application Data\Microsoft\Window
s\UsrClass.dat.LOG
0x0000000001fe4028      1      1 RW-rw- \Device\HarddiskVolume1\WINDOWS\WindowsUpdate.log
0x0000000001fe40d8      1      1 RW-rw- \Device\HarddiskVolume1\WINDOWS\WindowsUpdate.log
0x0000000001fe41a0      2      1 ------ \Device\NamedPipe\spoolss
0x0000000001fe4608      1      0 R--r-- \Device\HarddiskVolume1\WINDOWS\WinSxS\Manifests\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.762_x-ww_
6b128700.manifest
0x0000000001fe4d18      1      0 R--r-d \Device\HarddiskVolume1\WINDOWS\system32\cryptnet.dll
0x0000000002019298      1      1 RW-rw- \Device\HarddiskVolume1\WINDOWS\WindowsUpdate.log
0x000000000201ab40      2      1 R--rw- \Device\HarddiskVolume1\WINDOWS\system32\mui\0407
0x000000000201af00      2      1 R--rw- \Device\HarddiskVolume1\WINDOWS\system32\mui\0406
0x000000000201cb68      2      1 ------ \Device\NamedPipe\lsass
0x000000000201f028      2      1 R--rw- \Device\HarddiskVolume1\WINDOWS\system32\mui\0419
0x000000000201f0e0      2      1 R--rw- \Device\HarddiskVolume1\WINDOWS\system32\mui\041b
```

Note : regarding to your time . we can use | findstr in windows or | grep in Linux to search for specfic file on this

```
vol.exe -f cridex.vmem --profile=WinXPSP3x86 filescan | findstr ".exe"
 Framework 2.6
0x0000000002036f90      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\explorer.exe
0x0000000002036d28      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\ntkrnlpa.exe
0x0000000002036f28      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\ntoskrnl.exe
0x000000000207fd00      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\logonui.exe
0x0000000002081f90      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\lsass.exe
0x000000000209fdf8      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\verclsid.exe
0x00000000020b53f0      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\spider.exe
0x00000000020b5600      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\mshearts.exe
0x00000000020b5808      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\Restore\rstrui.exe
0x00000000020c3c70      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\userinit.exe
0x00000000022c45b8      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\autochk.exe
0x0000000002345bd0      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\rundll32.exe
0x000000000234bab8      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\services.exe
0x000000000238c778      1      0 R--rwd \Device\HarddiskVolume1\Documents and Settings\Robert\Application Data\KB00207877.exe
0x00000000023ad028      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\winlogon.exe
0x00000000023b8380      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\lsass.exe
0x00000000023c6e70      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\logonui.exe.manifest
0x00000000023ccf90      1      0 R--rwd \Device\HarddiskVolume1\Program Files\Adobe\Reader 9.0\Reader\reader_sl.exe
0x00000000023d1b88      1      0 R--r-d \Device\HarddiskVolume1\WINDOWS\system32\wuauclt.exe
0x00000000023d4f00      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\csrss.exe
0x00000000023dd760      1      0 R--rw- \Device\HarddiskVolume1\WINDOWS\explorer.exe
0x0000000002410c78      1      0 R--r-d \Device\HarddiskVolume1\Documents and Settings\Robert\Application Data\KB00207877.exe
```

Malware Memory Analysis

Spotting Suspicious .exe file in filescan plugin

In previous file scanning within filescan plugin in volatility and performing findstr | “.exe” we have spotted suspicious file known as “ \KB00207877.exe “

Command to use : vol.exe -f cridex.vmem --profile=WinXPSP3x86

```
ers\mrdiyarr\Downloads\vol>vol.exe -f cridex.vmem --profile=WinXPSP3x86 filescan | findstr ".exe"
ility Foundation Volatility Framework 2.6
0000002030f90      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\explorer.exe
0000002036d28      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\ntkrnlpa.exe
0000002036f28      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\ntoskrnl.exe
000000207fd00      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\logonui.exe
0000002081f90      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\lsass.exe
000000209fdf8      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\verclsid.exe
00000020b53f0      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\spider.exe
00000020b5600      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\mshearts.exe
00000020b5808      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\Restore\rstrui.exe
00000020c3c70      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\userinit.exe
00000022c45b8      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\autochk.exe
0000002345bd0      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\rundll32.exe
000000234bab8      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\services.exe
000000238c778      1      0 R--rwd \Device\HarddiskVolume1\Documents and Settings\Robert\Application D    \KB00207877.exe
00000023ad028      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\winlogon.exe
00000023b8380      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\lsass.exe
00000023c6e70      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\logonui.exe.manifest
00000023ccf90      1      0 R--rwd \Device\HarddiskVolume1\Program Files\Adobe\Reader 9.0\Reader\reade
00000023d1b88      1      0 R--r-d \Device\HarddiskVolume1\WINDOWS\system32\wuauclt.exe
00000023d4f00      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\csrss.exe
00000023dd760      1      0 R--rw- \Device\HarddiskVolume1\WINDOWS\explorer.exe
0000002410c78      1      0 R--r-d \Device\HarddiskVolume1\Documents and Settings\Robert\Application Data\KB00207877.exe
```

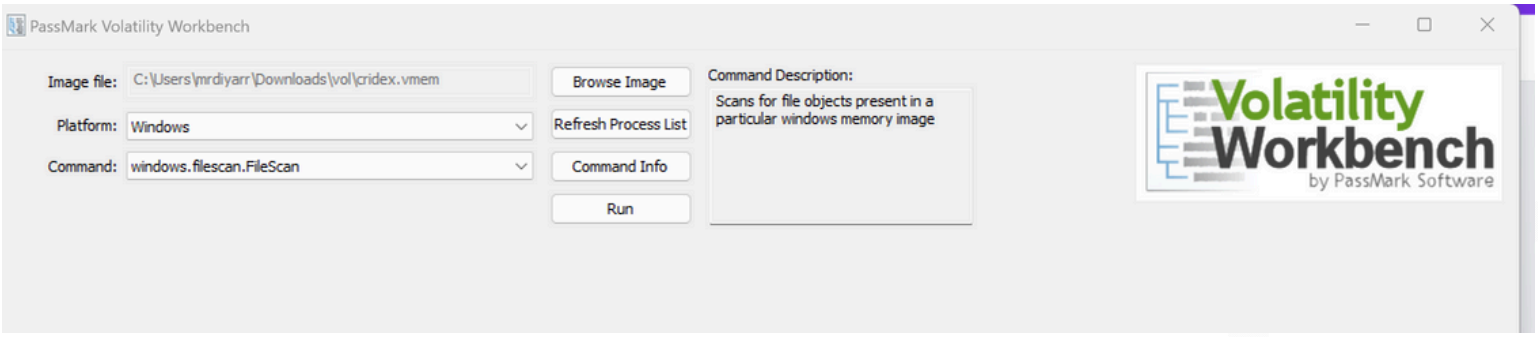
Note : for dumping the suspected file we will use Volatility workbench . it is GUI version of volatility framework . it can make our job easier .

Download Link : https://www.osforensics.com/downloads/VolatilityWorkbench.zip

Dumping Suspected File Volatility GUI

In previous file scanning within filescan plugin in volatility and performing findstr | ".exe" we have spotted suspicious file known as " \KB00207877.exe " we are going to dump it Inshallah by using Volatility GUI .

Guide to filtering and checking files :



Guide to Dumping Files :

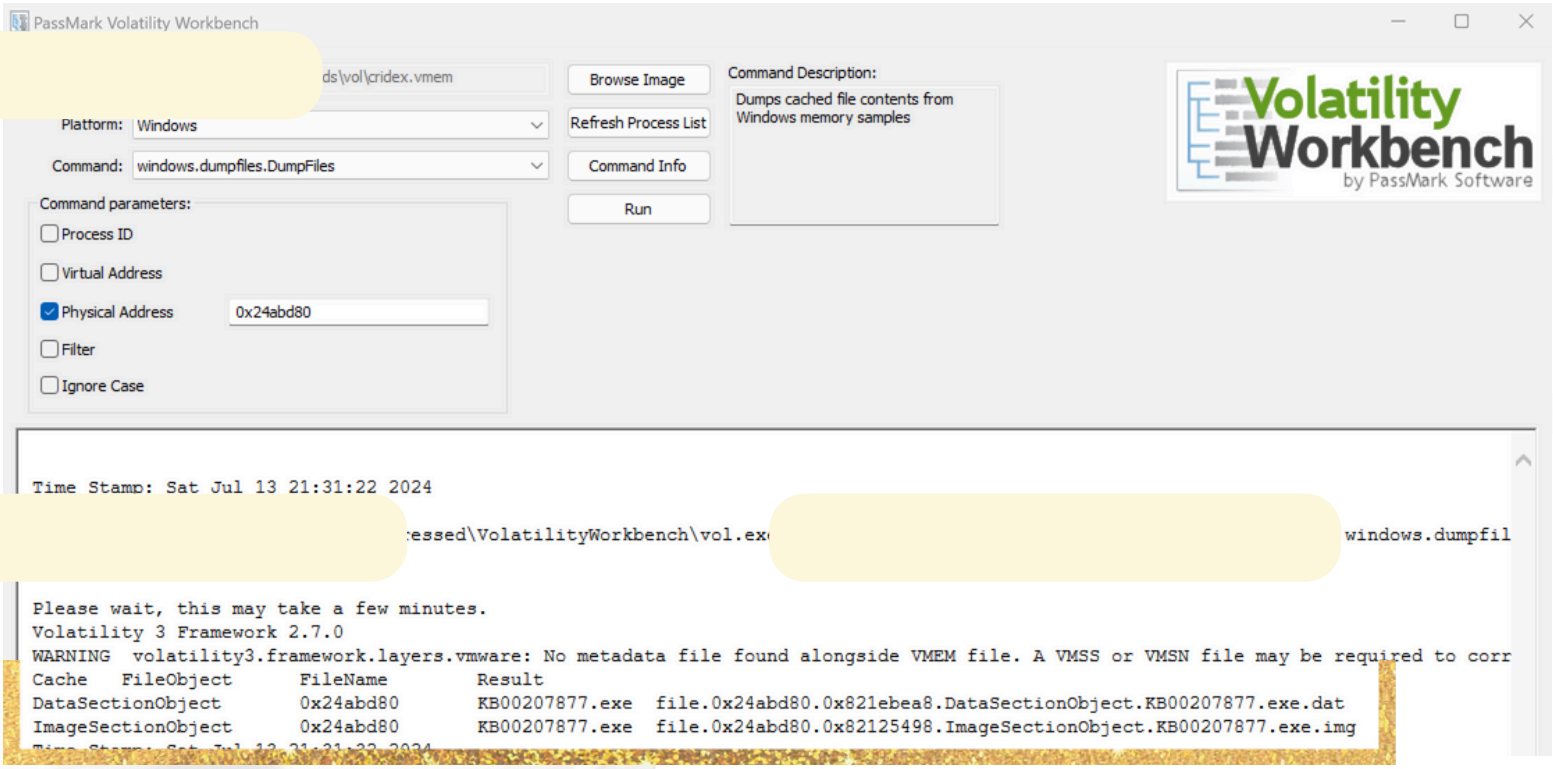
- Copy The Offset or Virtual Address .

```
0x24a6dd0       \WINDOWS\system32\wbem\wbemprox.dll     112
0x24a6f18       \WINDOWS\WindowsUpdate.log      112
0x24a7028       \WINDOWS\system32\wuapi.dll     112
0x24a72b8       \WINDOWS\system32\ssdpapi.dll   112
0x24a7700       \WINDOWS\system32\svchost.exe   112
0x24a82c8       \WINDOWS\system32\netmsg.dll    112
0x24a8640       \WINDOWS\system32\win32spl.dll  112
0x24a8a90       \WINDOWS\system32\usbmon.dll    112
0x24a8f90       \WINDOWS\system32\dpcdll.dll    112
0x24a9678       \browser        112
0x24aa210       \PIPE_EVENTROOT\CIMV2SCM EVENT PROVIDER 112
0x24aaed0       \WINDOWS\system32\resutils.dll  112
0x24ab230       \WINDOWS\system32\logonui.exe   112
0x24ab9e0       \Documents and Settings\Robert\NetHood  112
0x24abbb0       \WINDOWS\system32\dnsrslvr.dll  112
0x24abd80       \Documents and Settings\Robert\Application Data\KB00207877.exe  112
```

Dumping Suspected File Volatility GUI

In previous file scanning within filescan plugin in volatility and performing findstr | ".exe" we have spotted suspicious file known as " \KB00207877.exe " we are going to dump it Inshallah by using Volatility GUI .

Guide to Dump Suspected File ;

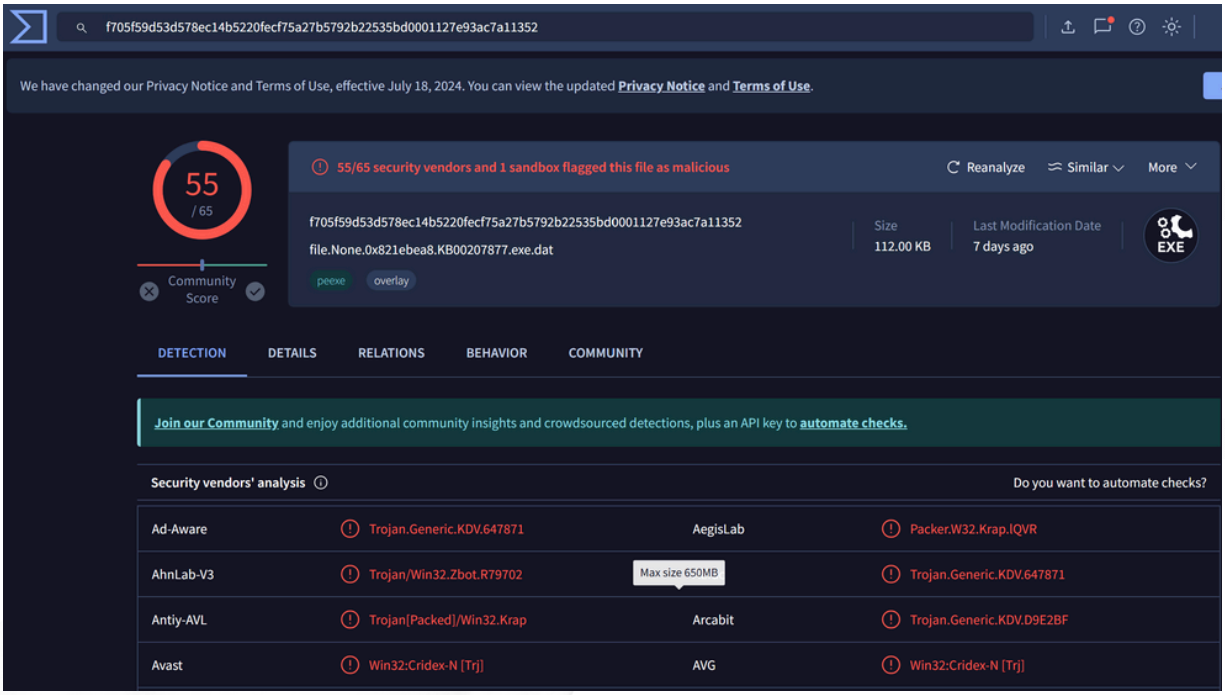


Note : The Suspected file has been successfully dumped on volatility workbench folder . then we can upload it into VT (VirusTotal) regarding to it is a malicious file or not .

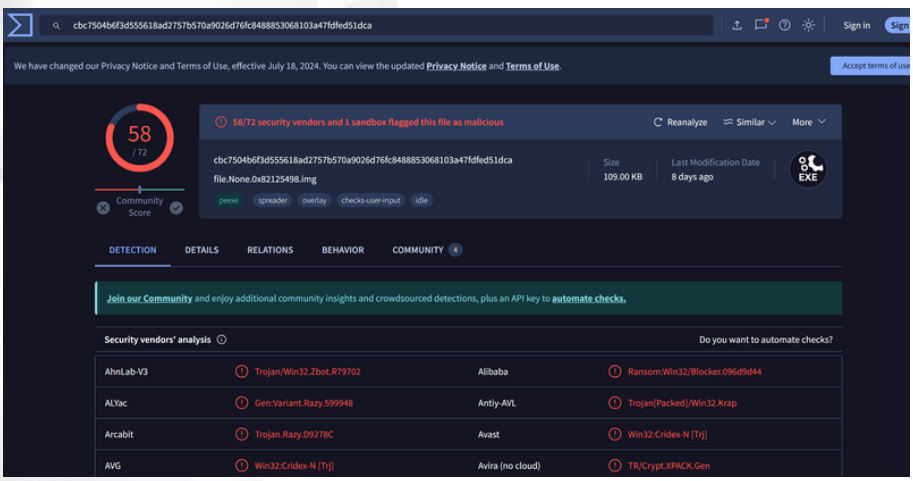
Uploading Dumped File into VT

After Dumping the suspicious file we will going to upload the dumped file into VT (VirusTotal) to have enough information to indicate this dumped file is malicious or only false posative .

- Result File 1 :



- Result File 2 :



Malware
Memory Analysis

Investigating Timeline timliner plugin

The timeliner plugin in Volatility is used to create a timeline of events based on timestamps extracted from various artifacts in the memory image. This can help in understanding the sequence of actions taken by a system, which is particularly useful during incident response or forensic investigations.

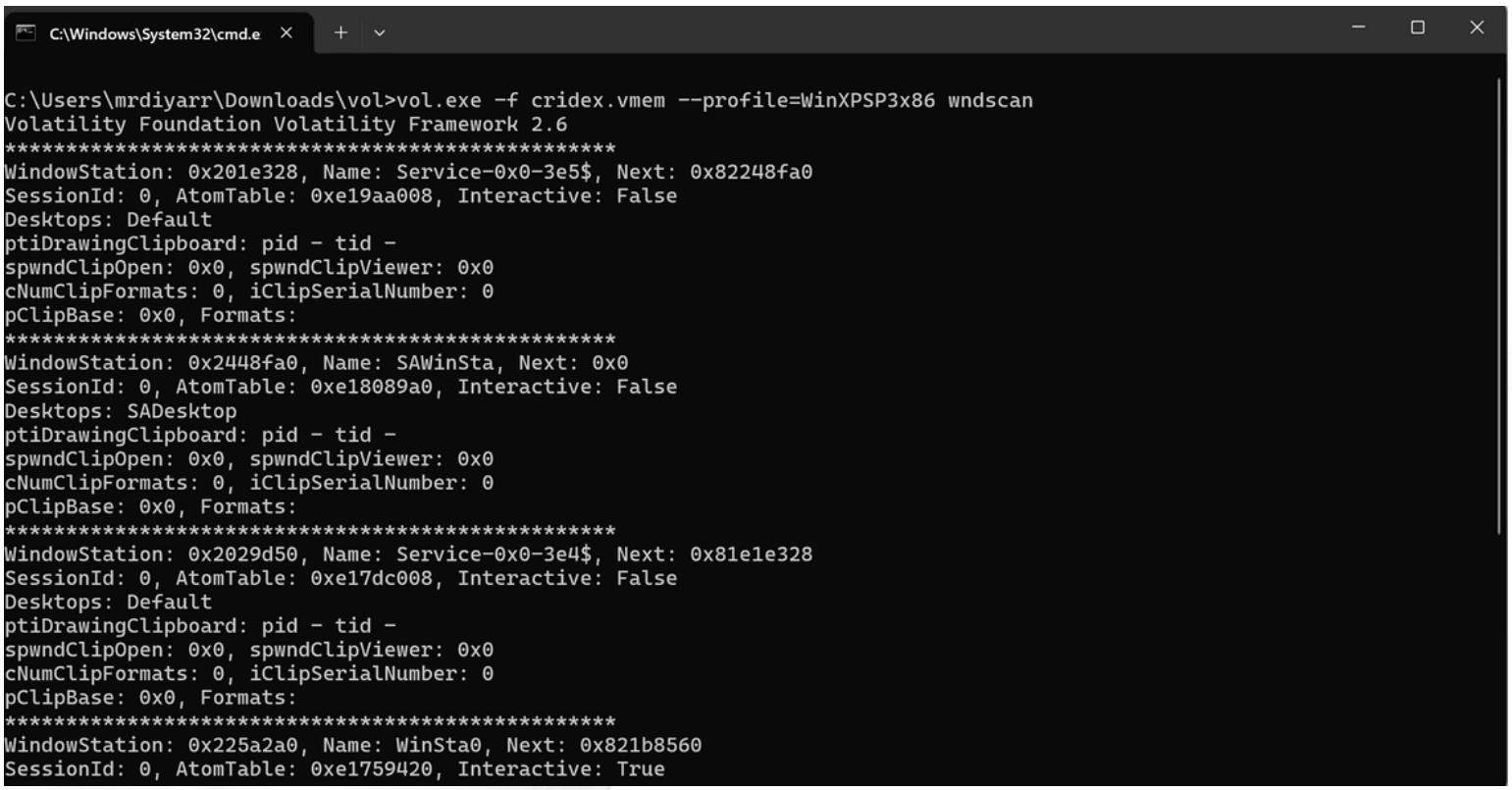
Command to use (normal use) : vol.exe -f cridex.vmem --profile=WinXPSP3x86 timeliner
Command to use (pipe into txt file) : vol.exe -f cridex.vmem --profile=WinXPSP3x86 timeliner > timeline.txt

```
UTC+0000|[LIVE RESPONSE]| (System time)|
UTC+0000|[PROCESS]| winlogon.exe| PID: 608/PPID: 368/POffset: 0x02498700
UTC+0000|[PROCESS LastTrimTime]| winlogon.exe| PID: 608/PPID: 368/POffset: 0x02498700
UTC+0000|[Handle (Key)]| MACHINE| winlogon.exe PID: 608/PPID: 368/POffset: 0x02498700
UTC+0000|[Handle (Key)]| MACHINE\SOFTWARE\CLASSES| winlogon.exe PID: 608/PPID: 368/POffset: 0x02498700
UTC+0000|[Handle (Key)]| USER\.DEFAULT| winlogon.exe PID: 608/PPID: 368/POffset: 0x02498700
UTC+0000|[Handle (Key)]| MACHINE\SYSTEM\CONTROLSET001\SERVICES\WINSOCK2\PARAMETERS\PROTOCOL_CATALOG9| winlogon.exe PID: 608/PPID: 368
UTC+0000|[Handle (Key)]| MACHINE\SYSTEM\CONTROLSET001\SERVICES\WINSOCK2\PARAMETERS\NAMESPACE_CATALOG5| winlogon.exe PID: 608/PPID: 36
UTC+0000|[Handle (Key)]| MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\WINLOGON\NOTIFY\CRYPT32CHAIN| winlogon.exe PID: 608/PPI
UTC+0000|[Handle (Key)]| MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\WINLOGON\NOTIFY\CRYPTNET| winlogon.exe PID: 608/PPID: 3
UTC+0000|[Handle (Key)]| MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\DRIVERS32| winlogon.exe PID: 608/PPID: 368/POffset: 0x0
UTC+0000|[Handle (Key)]| MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\WINLOGON\NOTIFY\SCLGNTFY| winlogon.exe PID: 608/PPID: 3
UTC+0000|[Handle (Key)]| MACHINE\SYSTEM\CONTROLSET001\CONTROL\LSA| winlogon.exe PID: 608/PPID: 368/POffset: 0x02498700
UTC+0000|[Handle (Key)]| MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\WINLOGON| winlogon.exe PID: 608/PPID: 368/POffset: 0x02
UTC+0000|[Handle (Key)]| MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\WINLOGON| winlogon.exe PID: 608/PPID: 368/POffset: 0x02
UTC+0000|[Handle (Key)]| MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\WINLOGON\CREDENTIALS| winlogon.exe PID: 608/PPID: 368/P
UTC+0000|[Handle (Key)]| MACHINE\SYSTEM\SETUP| winlogon.exe PID: 608/PPID: 368/POffset: 0x02498700
UTC+0000|[Handle (Key)]| USER| winlogon.exe PID: 608/PPID: 368/POffset: 0x02498700
UTC+0000|[Handle (Key)]| USER\S-1-5-21-789336058-261478967-1417001333-1003| winlogon.exe PID: 608/PPID: 368/POffset: 0x02498700
UTC+0000|[Handle (Key)]| MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\DRIVERS32| winlogon.exe PID: 608/PPID: 368/POffset: 0x0
UTC+0000|[Handle (Key)]| MACHINE\SYSTEM\CONTROLSET001\CONTROL\NETWORKPROVIDER\HWORDER| winlogon.exe PID: 608/PPID: 368/POffset: 0x024
UTC+0000|[Handle (Key)]| USER\.DEFAULT\SOFTWARE\MICROSOFT\WINDOWS\SHELLNOROAM| winlogon.exe PID: 608/PPID: 368/POffset: 0x02498700
UTC+0000|[Handle (Key)]| USER\.DEFAULT\SOFTWARE\MICROSOFT\WINDOWS\SHELLNOROAM\MUICACHE| winlogon.exe PID: 608/PPID: 368/POffset: 0x02
UTC+0000|[Handle (Key)]| MACHINE\SYSTEM\CONTROLSET001\SERVICES\TCPIP\LINKAGE| winlogon.exe PID: 608/PPID: 368/POffset: 0x02498700
UTC+0000|[Handle (Key)]| MACHINE\SYSTEM\CONTROLSET001\SERVICES\TCPIP\PARAMETERS| winlogon.exe PID: 608/PPID: 368/POffset: 0x02498700
UTC+0000|[Handle (Key)]| MACHINE\SYSTEM\CONTROLSET001\SERVICES\NETBT\PARAMETERS\INTERFACES| winlogon.exe PID: 608/PPID: 368/POffset:
```

Investigation Clipboard hooking

The wndscan plugin in Volatility is used to scan for window objects in memory. This can be useful for identifying visible and hidden windows created by processes, including those that may be associated with malware or suspicious activity.

Command to use (normal use) : vol.exe -f cridex.vmem --profile=WinXPSP3x86 wndscan
Command to use (pipe into txt file) : vol.exe -f cridex.vmem --profile=WinXPSP3x86 wndscan> wnd.txt



Malware
Memory Analysis