Malware Analysis and Memory Forensics

Report By
Bhanu PEDDIRAPPAGARI

Table of contents

Summary

Malware:

Malware also known as malicious software , is a program developed for the purpose of harming a computer, without the concern of the user.

This report shows, behaviour of this malware “Sample_7_exam.exe” in computer by doing malware analysis and digital forensics.

Identification:

We can identify malware using sha256, file, strings, CFF Explorer.

Dynamic analysis:

Dynamic Analysis is performed Using digital forensics tools: Procmon, TCPView, Autorun, Memory dump generation.

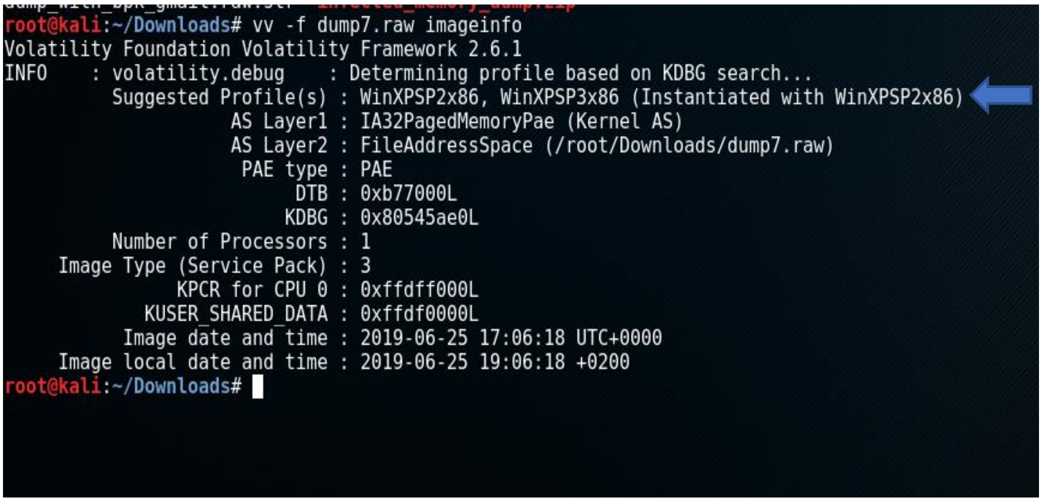
Memory forensics analysis:

Memory forensics analysis is performed by using command options: conncections, connscan, sockets, pslist, psxview.

Questions and Answers:

1. **From which operating system's version this image was taken?**

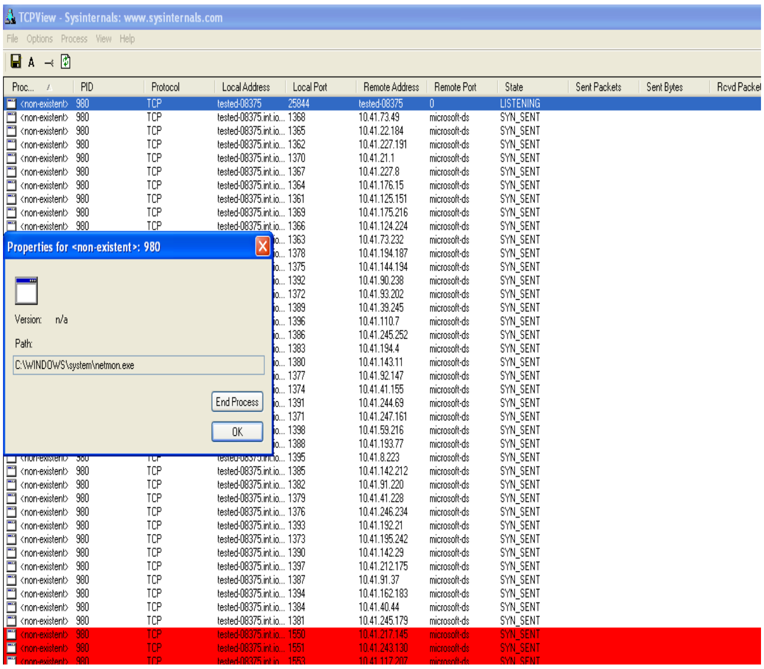
    - The image was taken from **WinXPSP2x86, WinXPSP3x86.**



```
root@kali:~/Downloads# vv -f dump7.raw imageinfo
Volatility Foundation Volatility Framework 2.6.1
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/Downloads/dump7.raw)
                      PAE type : PAE
                           DTB : 0xb77000L
                          KDBG : 0x80545ae0L
          Number of Processors : 1
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2019-06-25 17:06:18 UTC+0000
     Image local date and time : 2019-06-25 19:06:18 +0200
root@kali:~/Downloads# 
```

2. **What are the strange processes? Are they malicious? Why?**

    - Using TCP view , found a strange process as below after malware has been executed which was stored in the system C:\ windows\system\netmon.exe



TCPView - Sysinternals: www.sysinternals.com

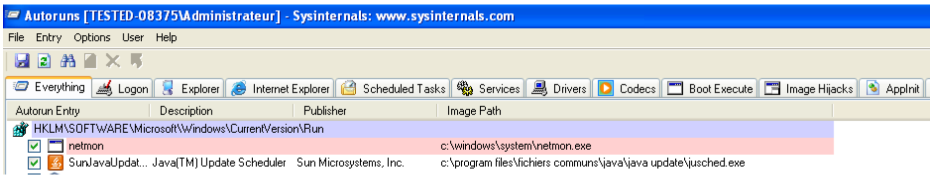
Proc...	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packet
<non-existent>	980	TCP	tested-08375	25844	tested-08375	0	LISTENING			
<non-existent>	980	TCP	tested-08375.int.io...	1368	10.41.73.49	microsoft-ds	SYN_SENT			
<non-existent>	980	TCP	tested-08375.int.io...	1365	10.41.22.184	microsoft-ds	SYN_SENT			
<non-existent>	980	TCP	tested-08375.int.io...	1362	10.41.227.191	microsoft-ds	SYN_SENT			
<non-existent>	980	TCP	tested-08375.int.io...	1370	10.41.21.1	microsoft-ds	SYN_SENT			
<non-existent>	980	TCP	tested-08375.int.io...	1367	10.41.227.8	microsoft-ds	SYN_SENT			
<non-existent>	980	TCP	tested-08375.int.io...	1364	10.41.176.15	microsoft-ds	SYN_SENT			
<non-existent>	980	TCP	tested-08375.int.io...	1361	10.41.125.151	microsoft-ds	SYN_SENT			
<non-existent>	980	TCP	tested-08375.int.io...	1369	10.41.175.216	microsoft-ds	SYN_SENT			
<non-existent>	980	TCP	tested-08375.int.io...	1366	10.41.124.224	microsoft-ds	SYN_SENT			
			io...	1363	10.41.73.232	microsoft-ds	SYN_SENT			
			io...	1378	10.41.194.187	microsoft-ds	SYN_SENT			
			io...	1375	10.41.144.194	microsoft-ds	SYN_SENT			
			io...	1392	10.41.90.238	microsoft-ds	SYN_SENT			
			io...	1372	10.41.93.202	microsoft-ds	SYN_SENT			
			io...	1389	10.41.39.245	microsoft-ds	SYN_SENT			
			io...	1396	10.41.110.7	microsoft-ds	SYN_SENT			
			io...	1386	10.41.245.252	microsoft-ds	SYN_SENT			
			io...	1383	10.41.194.4	microsoft-ds	SYN_SENT			
			io...	1380	10.41.143.11	microsoft-ds	SYN_SENT			
			io...	1377	10.41.92.147	microsoft-ds	SYN_SENT			
			io...	1374	10.41.41.155	microsoft-ds	SYN_SENT			
			io...	1391	10.41.244.69	microsoft-ds	SYN_SENT			
			io...	1371	10.41.247.161	microsoft-ds	SYN_SENT			
			io...	1398	10.41.59.216	microsoft-ds	SYN_SENT			
			io...	1388	10.41.193.77	microsoft-ds	SYN_SENT			
<non-existent>	980	TCP	tested-08375.int.io...	1395	10.41.8.223	microsoft-ds	SYN_SENT			
<non-existent>	980	TCP	tested-08375.int.io...	1385	10.41.142.212	microsoft-ds	SYN_SENT			
<non-existent>	980	TCP	tested-08375.int.io...	1382	10.41.91.220	microsoft-ds	SYN_SENT			
<non-existent>	980	TCP	tested-08375.int.io...	1379	10.41.41.228	microsoft-ds	SYN_SENT			
<non-existent>	980	TCP	tested-08375.int.io...	1376	10.41.246.234	microsoft-ds	SYN_SENT			
<non-existent>	980	TCP	tested-08375.int.io...	1393	10.41.192.21	microsoft-ds	SYN_SENT			
<non-existent>	980	TCP	tested-08375.int.io...	1373	10.41.195.242	microsoft-ds	SYN_SENT			
<non-existent>	980	TCP	tested-08375.int.io...	1390	10.41.142.29	microsoft-ds	SYN_SENT			
<non-existent>	980	TCP	tested-08375.int.io...	1397	10.41.212.175	microsoft-ds	SYN_SENT			
<non-existent>	980	TCP	tested-08375.int.io...	1387	10.41.91.37	microsoft-ds	SYN_SENT			
<non-existent>	980	TCP	tested-08375.int.io...	1394	10.41.162.183	microsoft-ds	SYN_SENT			
<non-existent>	980	TCP	tested-08375.int.io...	1384	10.41.40.44	microsoft-ds	SYN_SENT			
<non-existent>	980	TCP	tested-08375.int.io...	1381	10.41.245.179	microsoft-ds	SYN_SENT			
<non-existent>	980	TCP	tested-08375.int.io...	1550	10.41.217.145	microsoft-ds	SYN_SENT			
<non-existent>	980	TCP	tested-08375.int.io...	1551	10.41.243.130	microsoft-ds	SYN_SENT			
<non-existent>	980	TCP	tested-08375.int.io...	1553	10.41.117.207	microsoft-ds	SYN_SENT			

Properties for <non-existent>: 980

Version: n/a

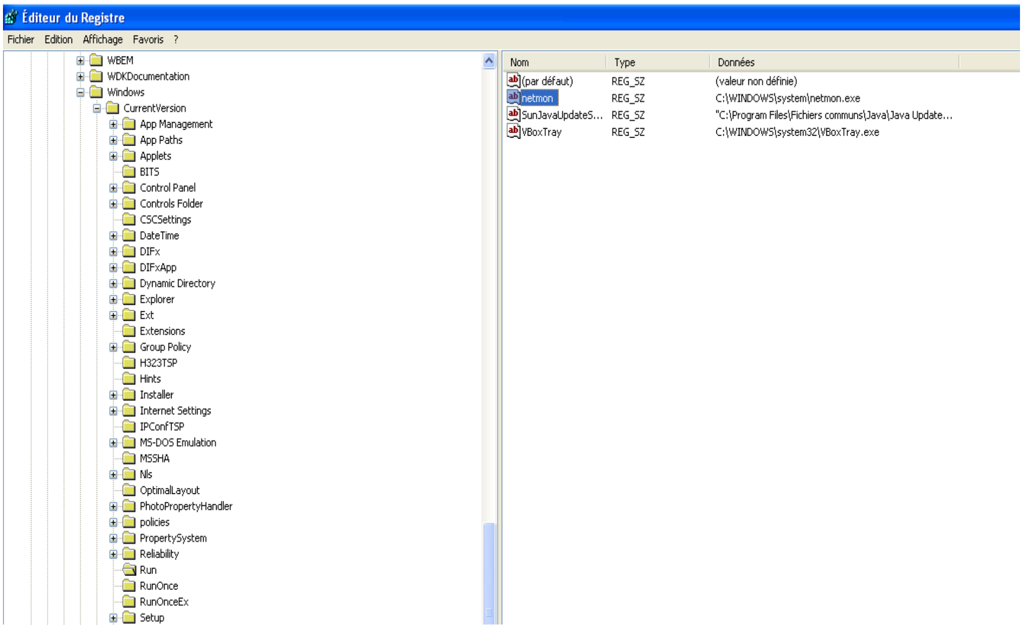
Path: C:\WINDOWS\system\netmon.exe

- Same netmon.exe process found while checking with Autorun as below


Autoruns [TESTED-08375\Administrateur] - Sysinternals: www.sysinternals.com
File Entry Options User Help
Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Codecs Boot Execute Image Hijacks AppInit

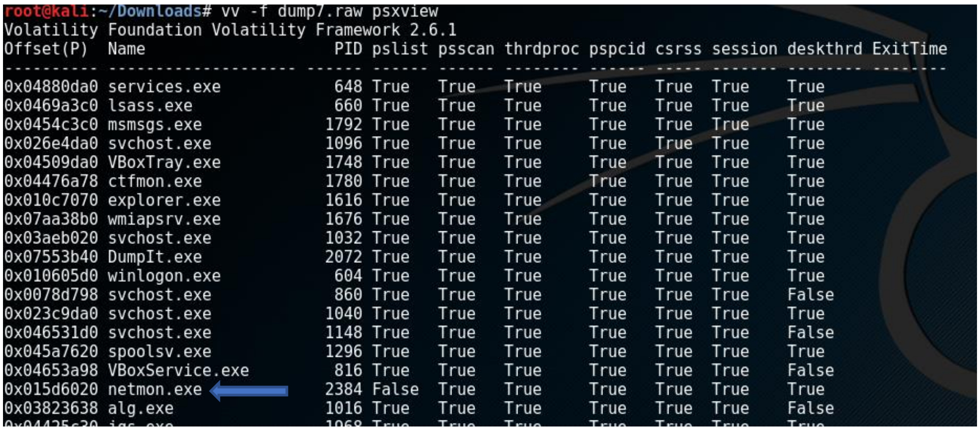
Autorun Entry	Description	Publisher	Image Path
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
☑ netmon			c:\windows\system\netmon.exe
☑ SunJavaUpdat...	Java(TM) Update Scheduler	Sun Microsystems, Inc.	c:\program files\fichiers communs\java\java update\jusched.exe

- When we jump to that process we can see that registry was opened where it had been stored.



Nom	Type	Données
(par défaut)	REG_SZ	(valeur non définie)
netmon	REG_SZ	C:\WINDOWS\system\netmon.exe
SunJavaUpdateS...	REG_SZ	"C:\Program Files\Fichiers communs\Java\Java Update...
VBoxTray	REG_SZ	C:\WINDOWS\system32\VBoxTray.exe

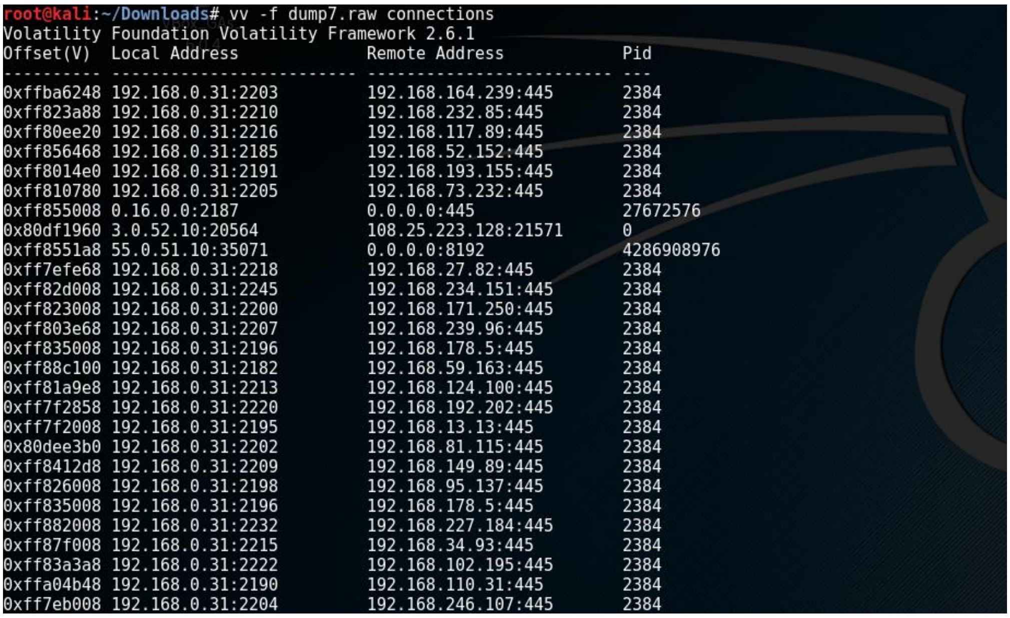
- When checked with pslist, pstree and cmdline no suspicious process were found and when with psxview, found offset & pid of netmon.exe as below,



```
root@kali:~/Downloads# vv -f dump7.raw psxview
Volatility Foundation Volatility Framework 2.6.1
Offset(P)  Name                    PID pslist psscan thrdproc pspcid csrss session deskthrd ExitTime
---------- -------------------- ------ ------ ------ -------- ------ ----- ------- -------- --------
0x04880da0 services.exe            648 True   True   True     True   True  True    True
0x0469a3c0 lsass.exe               660 True   True   True     True   True  True    True
0x0454c3c0 msmsgs.exe             1792 True   True   True     True   True  True    True
0x026e4da0 svchost.exe            1096 True   True   True     True   True  True    True
0x04509da0 VBoxTray.exe           1748 True   True   True     True   True  True    True
0x04476a78 ctfmon.exe             1780 True   True   True     True   True  True    True
0x010c7070 explorer.exe           1616 True   True   True     True   True  True    True
0x07aa38b0 wmiapsrv.exe           1676 True   True   True     True   True  True    True
0x03aeb020 svchost.exe            1032 True   True   True     True   True  True    True
0x07553b40 DumpIt.exe             2072 True   True   True     True   True  True    True
0x010605d0 winlogon.exe            604 True   True   True     True   True  True    True
0x0078d798 svchost.exe             860 True   True   True     True   True  True    False
0x023c9da0 svchost.exe            1040 True   True   True     True   True  True    True
0x046531d0 svchost.exe            1148 True   True   True     True   True  True    False
0x045a7620 spoolsv.exe            1296 True   True   True     True   True  True    True
0x04653a98 VBoxService.exe         816 True   True   True     True   True  True    False
0x015d6020 netmon.exe             2384 False  True   True     True   True  True    True
0x03823638 alg.exe                1016 True   True   True     True   True  True    False
```

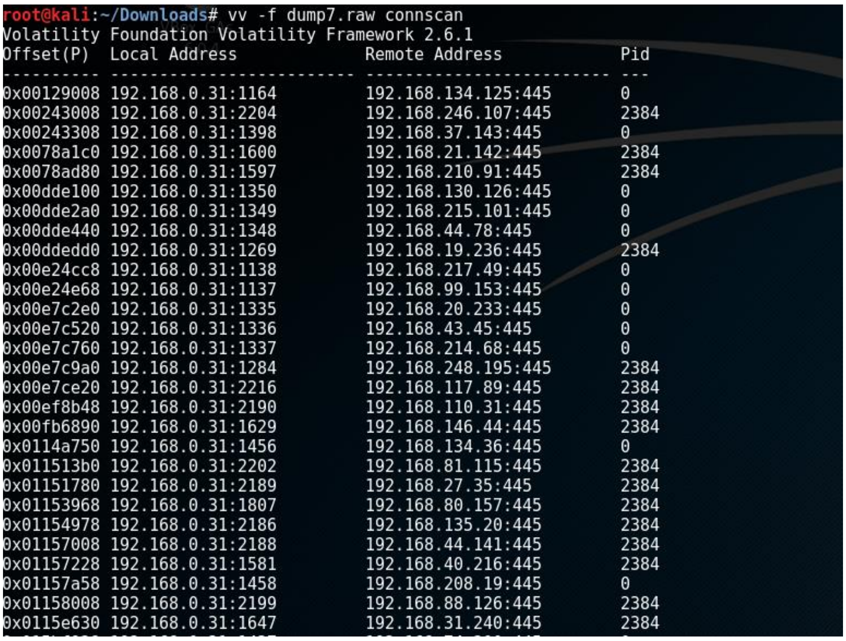
3. Which process is making network connections?

- After doing connections scan, below are the found active connections with port no 445 having same pid 2384.



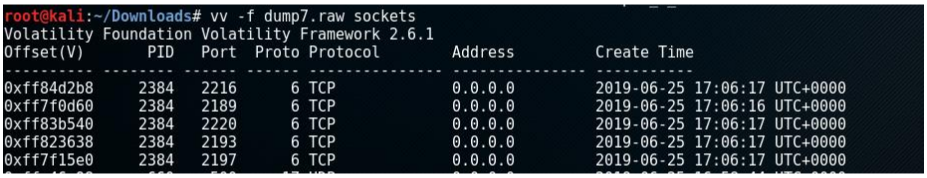
```
root@kali:~/Downloads# vv -f dump7.raw connections
Volatility Foundation Volatility Framework 2.6.1
Offset(V)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
0xffba6248 192.168.0.31:2203         192.168.164.239:445       2384
0xff823a88 192.168.0.31:2210         192.168.232.85:445        2384
0xff80ee20 192.168.0.31:2216         192.168.117.89:445        2384
0xff856468 192.168.0.31:2185         192.168.52.152:445        2384
0xff8014e0 192.168.0.31:2191         192.168.193.155:445       2384
0xff810780 192.168.0.31:2205         192.168.73.232:445        2384
0xff855008 0.16.0.0:2187             0.0.0.0:445               27672576
0x80df1960 3.0.52.10:20564           108.25.223.128:21571      0
0xff8551a8 55.0.51.10:35071          0.0.0.0:8192              4286908976
0xff7efe68 192.168.0.31:2218         192.168.27.82:445         2384
0xff82d008 192.168.0.31:2245         192.168.234.151:445       2384
0xff823008 192.168.0.31:2200         192.168.171.250:445       2384
0xff803e68 192.168.0.31:2207         192.168.239.96:445        2384
0xff835008 192.168.0.31:2196         192.168.178.5:445         2384
0xff88c100 192.168.0.31:2182         192.168.59.163:445        2384
0xff81a9e8 192.168.0.31:2213         192.168.124.100:445       2384
0xff7f2858 192.168.0.31:2220         192.168.192.202:445       2384
0xff7f2008 192.168.0.31:2195         192.168.13.13:445         2384
0x80dee3b0 192.168.0.31:2202         192.168.81.115:445        2384
0xff8412d8 192.168.0.31:2209         192.168.149.89:445        2384
0xff826008 192.168.0.31:2198         192.168.95.137:445        2384
0xff835008 192.168.0.31:2196         192.168.178.5:445         2384
0xff882008 192.168.0.31:2232         192.168.227.184:445       2384
0xff87f008 192.168.0.31:2215         192.168.34.93:445         2384
0xff83a3a8 192.168.0.31:2222         192.168.102.195:445       2384
0xffa04b48 192.168.0.31:2190         192.168.110.31:445        2384
0xff7eb008 192.168.0.31:2204         192.168.246.107:445       2384
```

- Now checking with connscan, below are the found active connections with port no 445 having same pid 2384.



```
root@kali:~/Downloads# vv -f dump7.raw connscan
Volatility Foundation Volatility Framework 2.6.1
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
0x00129008 192.168.0.31:1164         192.168.134.125:445       0
0x00243008 192.168.0.31:2204         192.168.246.107:445       2384
0x00243308 192.168.0.31:1398         192.168.37.143:445        0
0x0078a1c0 192.168.0.31:1600         192.168.21.142:445        2384
0x0078ad80 192.168.0.31:1597         192.168.210.91:445        2384
0x00dde100 192.168.0.31:1350         192.168.130.126:445       0
0x00dde2a0 192.168.0.31:1349         192.168.215.101:445       0
0x00dde440 192.168.0.31:1348         192.168.44.78:445         0
0x00ddedd0 192.168.0.31:1269         192.168.19.236:445        2384
0x00e24cc8 192.168.0.31:1138         192.168.217.49:445        0
0x00e24e68 192.168.0.31:1137         192.168.99.153:445        0
0x00e7c2e0 192.168.0.31:1335         192.168.20.233:445        0
0x00e7c520 192.168.0.31:1336         192.168.43.45:445         0
0x00e7c760 192.168.0.31:1337         192.168.214.68:445        0
0x00e7c9a0 192.168.0.31:1284         192.168.248.195:445       2384
0x00e7ce20 192.168.0.31:2216         192.168.117.89:445        2384
0x00ef8b48 192.168.0.31:2190         192.168.110.31:445        2384
0x00fb6890 192.168.0.31:1629         192.168.146.44:445        2384
0x0114a750 192.168.0.31:1456         192.168.134.36:445        0
0x011513b0 192.168.0.31:2202         192.168.81.115:445        2384
0x01151780 192.168.0.31:2189         192.168.27.35:445         2384
0x01153968 192.168.0.31:1807         192.168.80.157:445        2384
0x01154978 192.168.0.31:2186         192.168.135.20:445        2384
0x01157008 192.168.0.31:2188         192.168.44.141:445        2384
0x01157228 192.168.0.31:1581         192.168.40.216:445        2384
0x01157a58 192.168.0.31:1458         192.168.208.19:445        0
0x01158008 192.168.0.31:2199         192.168.88.126:445        2384
0x0115e630 192.168.0.31:1647         192.168.31.240:445        2384
```

- After checking with sockets, below are the found active pid 2384 communicating on different port numbers using “TCP protocol”.



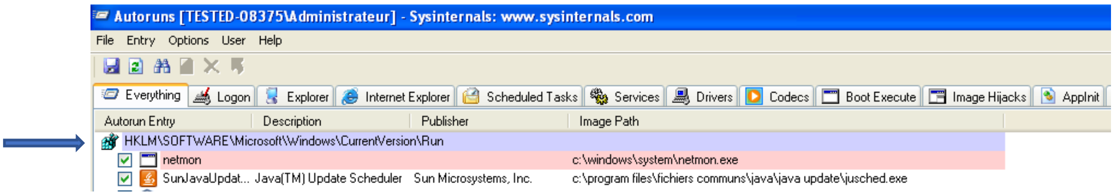
```
root@kali:~/Downloads# vv -f dump7.raw sockets
Volatility Foundation Volatility Framework 2.6.1
Offset(V)       PID   Port  Proto Protocol        Address         Create Time
---------- -------- ------ ------ --------------- --------------- -----------
0xff84d2b8     2384   2216      6 TCP             0.0.0.0         2019-06-25 17:06:17 UTC+0000
0xff7f0d60     2384   2189      6 TCP             0.0.0.0         2019-06-25 17:06:16 UTC+0000
0xff83b540     2384   2220      6 TCP             0.0.0.0         2019-06-25 17:06:17 UTC+0000
0xff823638     2384   2193      6 TCP             0.0.0.0         2019-06-25 17:06:17 UTC+0000
0xff7f15e0     2384   2197      6 TCP             0.0.0.0         2019-06-25 17:06:17 UTC+0000
```

4. Where are the remote ip address located?

- Remote ip address are located at offset of the process.

5.Find where the malicious program is recorded in the registry startup list?

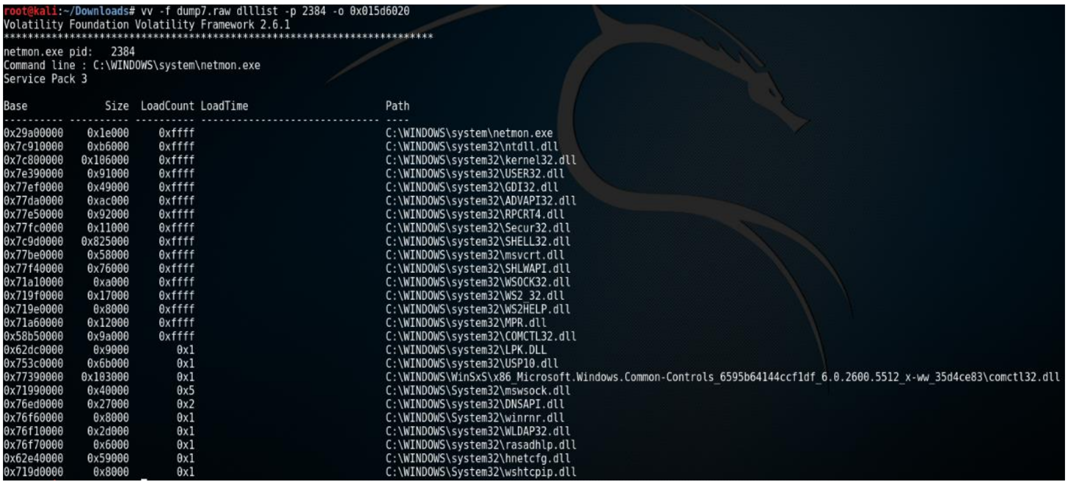
- The malicious program is recorded in the path : HKLM\Software\Microsft\Windows\CurrentVersion\Run, this is identified using autorun.



Autorun Entry	Description	Publisher	Image Path
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
☑ netmon			c:\windows\system\netmon.exe
☑ SunJavaUpdat...	Java(TM) Update Scheduler	Sun Microsystems, Inc.	c:\program files\fichiers communs\java\java update\jusched.exe

6.How does this malware executes its code on the system? dump it.

- Searched for dll list using #vv -f dup.raw dlllist -p 2384 -o 0x015d6020 **,** didn’t find any dll files realted to netmon.exe

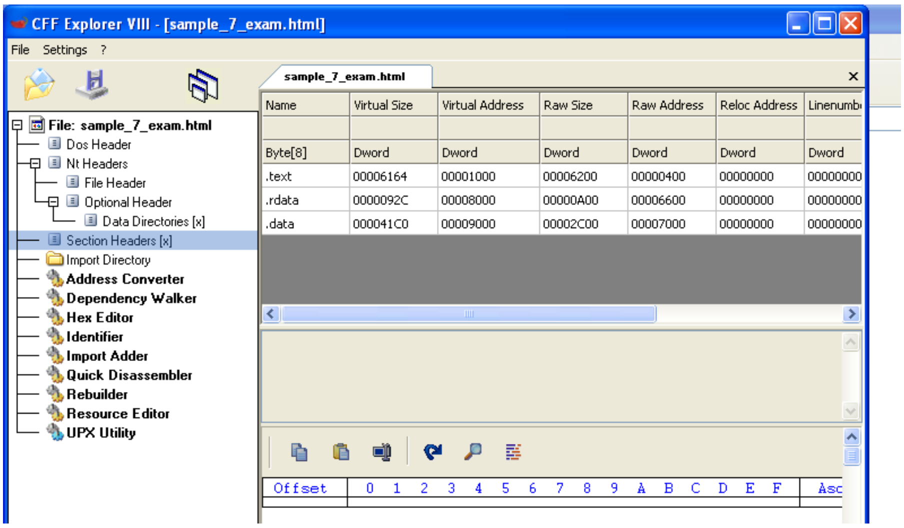


```
root@kali:~/Downloads# vv -f dump7.raw dlllist -p 2384 -o 0x015d6020
Volatility Foundation Volatility Framework 2.6.1
************************************************************************
netmon.exe pid:   2384
Command line : C:\WINDOWS\system\netmon.exe
Service Pack 3

Base             Size  LoadCount LoadTime                       Path
---------- ---------- ---------- ------------------------------ ----
0x29a00000    0x1e000     0xffff                                C:\WINDOWS\system\netmon.exe
0x7c910000    0xb6000     0xffff                                C:\WINDOWS\system32\ntdll.dll
0x7c800000   0x106000     0xffff                                C:\WINDOWS\system32\kernel32.dll
0x7e390000    0x91000     0xffff                                C:\WINDOWS\system32\USER32.dll
0x77ef0000    0x49000     0xffff                                C:\WINDOWS\system32\GDI32.dll
0x77da0000    0xac000     0xffff                                C:\WINDOWS\system32\ADVAPI32.dll
0x77e50000    0x92000     0xffff                                C:\WINDOWS\system32\RPCRT4.dll
0x77fc0000    0x11000     0xffff                                C:\WINDOWS\system32\Secur32.dll
0x7c9d0000   0x825000     0xffff                                C:\WINDOWS\system32\SHELL32.dll
0x77be0000    0x58000     0xffff                                C:\WINDOWS\system32\msvcrt.dll
0x77f40000    0x76000     0xffff                                C:\WINDOWS\system32\SHLWAPI.dll
0x71a10000     0xa000     0xffff                                C:\WINDOWS\system32\WSOCK32.dll
0x719f0000    0x17000     0xffff                                C:\WINDOWS\system32\WS2_32.dll
0x719e0000     0x8000     0xffff                                C:\WINDOWS\system32\WS2HELP.dll
0x71a60000    0x12000     0xffff                                C:\WINDOWS\system32\MPR.dll
0x58b50000    0x9a000     0xffff                                C:\WINDOWS\system32\COMCTL32.dll
0x62dc0000     0x9000        0x1                                C:\WINDOWS\system32\LPK.DLL
0x753c0000    0x6b000        0x1                                C:\WINDOWS\system32\USP10.dll
0x77390000   0x103000        0x1                                C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
0x71990000    0x40000        0x5                                C:\WINDOWS\System32\mswsock.dll
0x76ed0000    0x27000        0x2                                C:\WINDOWS\system32\DNSAPI.dll
0x76f60000     0x8000        0x1                                C:\WINDOWS\System32\winrnr.dll
0x76f10000    0x2d000        0x1                                C:\WINDOWS\system32\WLDAP32.dll
0x76f70000     0x6000        0x1                                C:\WINDOWS\system32\rasadhlp.dll
0x62e40000    0x59000        0x1                                C:\WINDOWS\system32\hnetcfg.dll
0x719d0000     0x8000        0x1                                C:\WINDOWS\System32\wshtcpip.dll
```

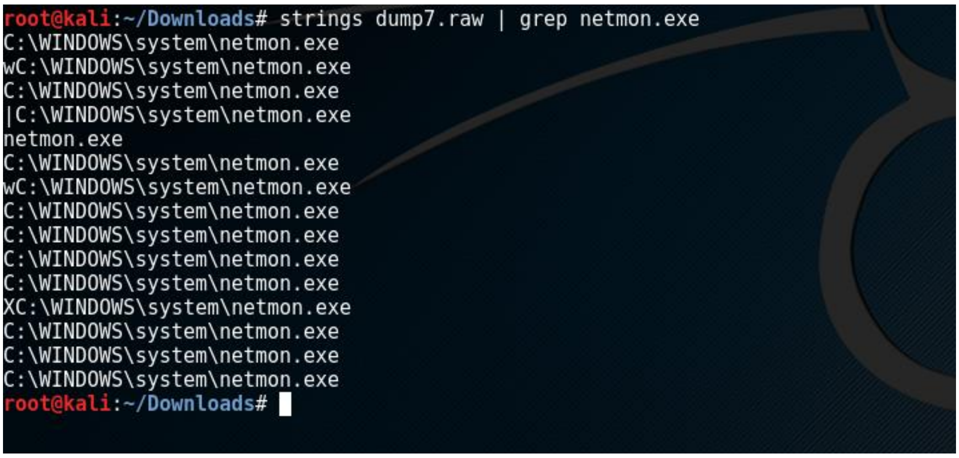
7.What are the sections of this PE file?

- The sections are .text, .rdata, .data for the process file.



Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumb
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword
.text	00006164	00001000	00006200	00000400	00000000	00000000
.rdata	0000092C	00008000	00000A00	00006600	00000000	00000000
.data	000041C0	00009000	00002C00	00007000	00000000	00000000

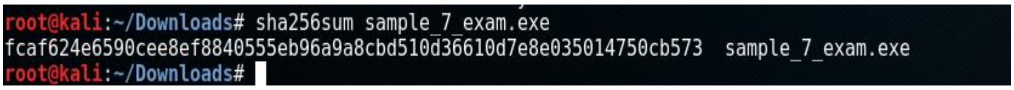
8. Any interesting strings from this malware?



```
root@kali:~/Downloads# strings dump7.raw | grep netmon.exe
C:\WINDOWS\system\netmon.exe
wC:\WINDOWS\system\netmon.exe
C:\WINDOWS\system\netmon.exe
|C:\WINDOWS\system\netmon.exe
netmon.exe
C:\WINDOWS\system\netmon.exe
wC:\WINDOWS\system\netmon.exe
C:\WINDOWS\system\netmon.exe
C:\WINDOWS\system\netmon.exe
C:\WINDOWS\system\netmon.exe
C:\WINDOWS\system\netmon.exe
XC:\WINDOWS\system\netmon.exe
C:\WINDOWS\system\netmon.exe
C:\WINDOWS\system\netmon.exe
C:\WINDOWS\system\netmon.exe
root@kali:~/Downloads#
```

9. What's the SHA256 of this malware?

- I have taken sha256sum for malware file.



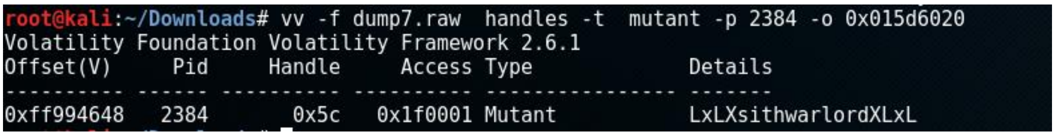
```
root@kali:~/Downloads# sha256sum sample_7_exam.exe
fcaf624e6590cee8ef8840555eb96a9a8cbd510d36610d7e8e035014750cb573  sample_7_exam.exe
root@kali:~/Downloads#
```

10. What is the malware name?

- **The malware name is netmon.exe**

11.Give it’s mutex?

- Below are the mutex found for pid 2384,



```
root@kali:~/Downloads# vv -f dump7.raw  handles -t  mutant -p 2384 -o 0x015d6020
Volatility Foundation Volatility Framework 2.6.1
Offset(V)     Pid     Handle     Access Type             Details
---------- ------ ---------- ---------- ---------------- -------
0xff994648   2384       0x5c   0x1f0001 Mutant           LxLXsithwarlordXLxL
```

13. What is the hooked API? From which processes?

- Didn’t find any hooked API’s.

14. Does this malware propagate/spread itself?

- Yes, once the malware has been executed its running some process on background and when It will start itself after rebooting of pc and ask for user permission to execute or not.

15. Write a script/program to clean an infected system automatically. If you aren't able to do it, show the manual steps.

To clean the infected system,

- Go to registry file “is **HKLM\Software\Microsft\Windows\CurrentVersion\Run**” and delete netmon.exe file.
- Open TCP view, right click on netmon connections and end the process.
- Go to **windows/system/netmon.exe** and delete the file permanently.