BlackEnergy Lab (Cyber Defenders) - Walkthrough

Sunday, September 15, 2024 4:46 PM

Story:
A multinational corporation has been hit by a cyber-attack that has led to the theft of sensitive data. The attack was carried out using a variant of the BlackEnergy v2 malware that has never been seen before. The company's security team has acquired a memory dump of the infected machine, and they want you, as a soc analyst, to analyze the dump to understand the attack scope and impact.

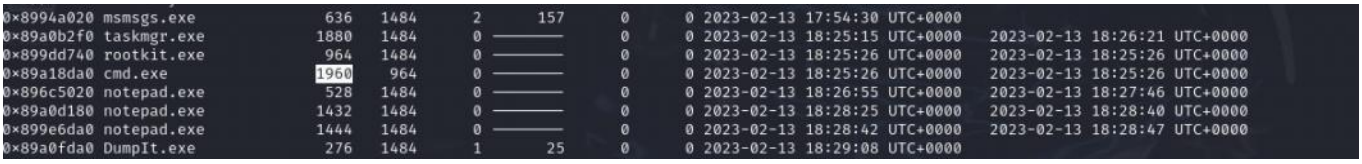
Q1: Which volatility profile would be best for this machine?

- I used 'imageinfo' plugin to find the profile (WinXPSP2x86)

Q2: How many processes were running when the image was acquired?

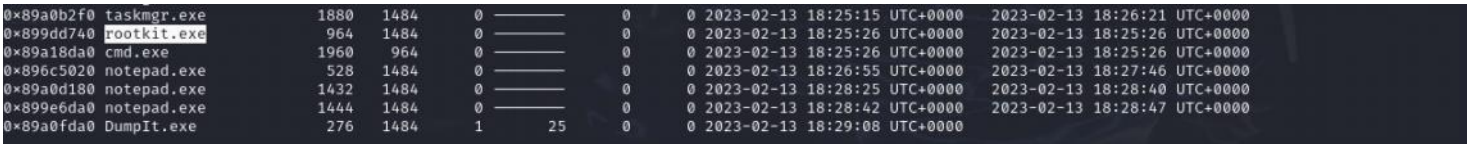
- I used 'pslist' plugin to find the number of the running processes, I send the output to ChatGPT to remove duplicates and found the answer is 19

Q3: What is the process ID of cmd.exe?



```
0x8994a020 msmsgs.exe             636   1484      2      157      0      0 2023-02-13 17:54:30 UTC+0000
0x89a0b2f0 taskmgr.exe           1880   1484      0 ————————      0      0 2023-02-13 18:25:15 UTC+0000   2023-02-13 18:26:21 UTC+0000
0x899dd740 rootkit.exe            964   1484      0 ————————      0      0 2023-02-13 18:25:26 UTC+0000   2023-02-13 18:25:26 UTC+0000
0x89a18da0 cmd.exe               1960    964      0 ————————      0      0 2023-02-13 18:25:26 UTC+0000   2023-02-13 18:25:26 UTC+0000
0x896c5020 notepad.exe            528   1484      0 ————————      0      0 2023-02-13 18:26:55 UTC+0000   2023-02-13 18:27:46 UTC+0000
0x89a0d180 notepad.exe           1432   1484      0 ————————      0      0 2023-02-13 18:28:25 UTC+0000   2023-02-13 18:28:40 UTC+0000
0x899e6da0 notepad.exe           1444   1484      0 ————————      0      0 2023-02-13 18:28:42 UTC+0000   2023-02-13 18:28:47 UTC+0000
0x89a0fda0 DumpIt.exe             276   1484      1       25      0      0 2023-02-13 18:29:08 UTC+0000
```

Q4: What is the name of the most suspicious process?



```
0x89a0b2f0 taskmgr.exe           1880   1484      0 ————————      0      0 2023-02-13 18:25:15 UTC+0000   2023-02-13 18:26:21 UTC+0000
0x899dd740 rootkit.exe            964   1484      0 ————————      0      0 2023-02-13 18:25:26 UTC+0000   2023-02-13 18:25:26 UTC+0000
0x89a18da0 cmd.exe               1960    964      0 ————————      0      0 2023-02-13 18:25:26 UTC+0000   2023-02-13 18:25:26 UTC+0000
0x896c5020 notepad.exe            528   1484      0 ————————      0      0 2023-02-13 18:26:55 UTC+0000   2023-02-13 18:27:46 UTC+0000
0x89a0d180 notepad.exe           1432   1484      0 ————————      0      0 2023-02-13 18:28:25 UTC+0000   2023-02-13 18:28:40 UTC+0000
0x899e6da0 notepad.exe           1444   1484      0 ————————      0      0 2023-02-13 18:28:42 UTC+0000   2023-02-13 18:28:47 UTC+0000
0x89a0fda0 DumpIt.exe             276   1484      1       25      0      0 2023-02-13 18:29:08 UTC+0000
```

Q5:Which process shows the highest likelihood of code injection?

- I used 'malfind' plugin to find the injected process which is 'svchost.exe'

```
Process: svchost.exe Pid: 880 Address: 0x980000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 9, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x0000000000980000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00   MZ..............
0x0000000000980010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ........@.......
0x0000000000980020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x0000000000980030  00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00   ................
```

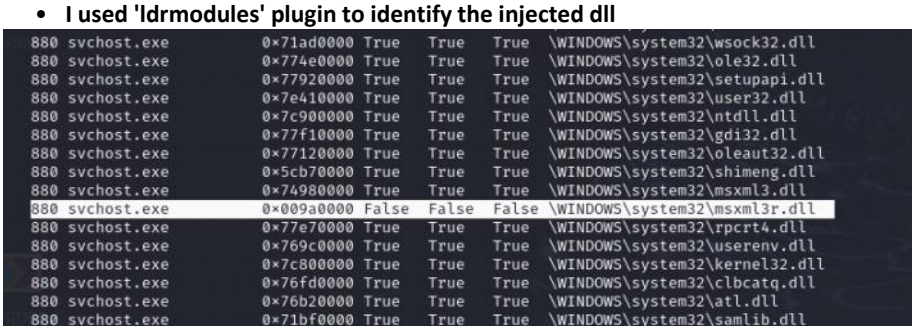
Q6:There is an odd file referenced in the recent process. Provide the full path of that file.

- **To address this question, I took the PID of the injected process and used 'handles' to find the odd file**

```
0x896862b8    880      0x330   0x1f0001 Mutant          {3D5A1694-CC2C-4ee7-A3D5-A879A9E3A623}
0x89a0da50    880      0x334   0x1f03ff Thread          TID 1704 PID 880
0x89b9d840    880      0x338   0x1f0001 Mutant
0x89a00f90    880      0x33c   0x12019f File            \Device\{9DD6AFA1-8646-4720-836B-EDCB1085864A}
0x89af0cf0    880      0x340   0x12019f File            \Device\HarddiskVolume1\WINDOWS\system32\drivers\str.sys
0xe1155570    880      0x344    0xf003f Key             MACHINE\SOFTWARE\CLASSES
0xe1139bb0    880      0x348    0xf003f Key             MACHINE\SOFTWARE\CLASSES
0x89986d98    880      0x34c   0x1f0003 Event
0xe1bb4cf0    880      0x350    0xf003f Key             MACHINE\SOFTWARE\MICROSOFT\COM3
0x89986dc8    880      0x354   0x1f0003 Event
```

Q8: What is the name of the injected dll file loaded from the recent process?

- **I used 'ldrmodules' plugin to identify the injected dll**



```
880 svchost.exe          0x71ad0000 True   True   True  \WINDOWS\system32\wsock32.dll
880 svchost.exe          0x774e0000 True   True   True  \WINDOWS\system32\ole32.dll
880 svchost.exe          0x77920000 True   True   True  \WINDOWS\system32\setupapi.dll
880 svchost.exe          0x7e410000 True   True   True  \WINDOWS\system32\user32.dll
880 svchost.exe          0x7c900000 True   True   True  \WINDOWS\system32\ntdll.dll
880 svchost.exe          0x77f10000 True   True   True  \WINDOWS\system32\gdi32.dll
880 svchost.exe          0x77120000 True   True   True  \WINDOWS\system32\oleaut32.dll
880 svchost.exe          0x5cb70000 True   True   True  \WINDOWS\system32\shimeng.dll
880 svchost.exe          0x74980000 True   True   True  \WINDOWS\system32\msxml3.dll
880 svchost.exe          0x009a0000 False  False  False \WINDOWS\system32\msxml3r.dll
880 svchost.exe          0x77e70000 True   True   True  \WINDOWS\system32\rpcrt4.dll
880 svchost.exe          0x769c0000 True   True   True  \WINDOWS\system32\userenv.dll
880 svchost.exe          0x7c800000 True   True   True  \WINDOWS\system32\kernel32.dll
880 svchost.exe          0x76fd0000 True   True   True  \WINDOWS\system32\clbcatq.dll
880 svchost.exe          0x76b20000 True   True   True  \WINDOWS\system32\atl.dll
880 svchost.exe          0x71bf0000 True   True   True  \WINDOWS\system32\samlib.dll
```

Q9: What is the base address of the injected dll?

- We already found the answer at question 5 (0x980000)