BlackEnergy Lab
Analyst: Ruslan
Date: 2026-01-26

Overview

This report provides the findings from the analysis of a compromised system, potentially infected with the BlackEnergy malware. The analysis was conducted using memory dump analysis techniques to identify suspicious processes, injected code, and other indicators of compromise.

Findings

1. **Volatility Profile Selection**
   The best volatility profile for the memory image was identified as **WinXPSP2x86**, corresponding to a 32-bit version of Windows XP Service Pack 2. The correct profile was crucial for accurate memory structure interpretation, ensuring the analysis was conducted within the correct system context.

2. **Processes Running at the Time of Capture**
   The system had **19 processes** running at the time the memory image was acquired. This indicates a normal operating state for a Windows XP system, with no immediate signs of excessive processes that would suggest abnormal behavior, such as the presence of hidden malicious processes.

3. **Identification of cmd.exe Process**
   The process ID (PID) of `cmd. exe` was found to be **1960**. This standard command-line process was running at the time of acquisition, which is typical for Windows systems. While cmd.exe can be used by attackers for command execution, no evidence of malicious activity was directly linked to this process based on the current analysis.

4. **Suspicious Process Identified**
   The process identified as most suspicious was **rootkit.exe**. This is a known name associated with rootkits, which are malware designed to hide their presence and provide unauthorized system access. The presence of this process strongly suggests that the system may have been compromised and could be under the control of an attacker.

5. **Code Injection Likelihood**
   The process with the highest likelihood of code injection was identified as **svchost.exe**. This is a critical Windows system process that runs services. However, it is also commonly targeted by malware for code injection. The injection of malicious code into svchost.exe indicates that the system was likely compromised and the malicious code was running within a trusted system process to evade detection.

6. **Suspicious File Reference**
   A suspicious file was found referenced by a process:
   C:\WINDOWS\system32\drivers\str.sys. This file is not a standard Windows system file, and its presence in the system's driver folder raises concerns about potential rootkit or kernel-level malware activity. Malicious drivers can provide attackers with deep access to the system, allowing them to operate stealthily and maintain persistence.

7. **Injected DLL File**
   The injected DLL file loaded by a recent process was identified as **msxml3r.dll**. This DLL is not part of the standard Windows library, suggesting that it was injected by the attacker to facilitate further malicious activity. Injected DLLs are commonly used by malware to alter the behavior of legitimate processes or to load additional malicious code.

8. **Base Address of Injected DLL**
   The base address of the injected DLL was found to be **0x980000**. This address provides a specific location in memory where the injected DLL resides. Understanding the base address is important for further investigation, as it allows for the extraction and analysis of the DLL to determine its function and how it interacts with other system components.

Conclusion

The analysis of the memory image has revealed multiple indicators of compromise, including the presence of suspicious processes (e.g., `rootkit.exe`), injected code (e.g., in `svchost.exe`), and abnormal files (e.g., `str.sys`). These findings strongly suggest that the system has been compromised by the BlackEnergy malware or a similar rootkit-based attack. Further investigation is required to fully analyze the injected DLLs and malicious files to understand the scope of the attack and potential data exfiltration or other malicious activities.

Recommendations

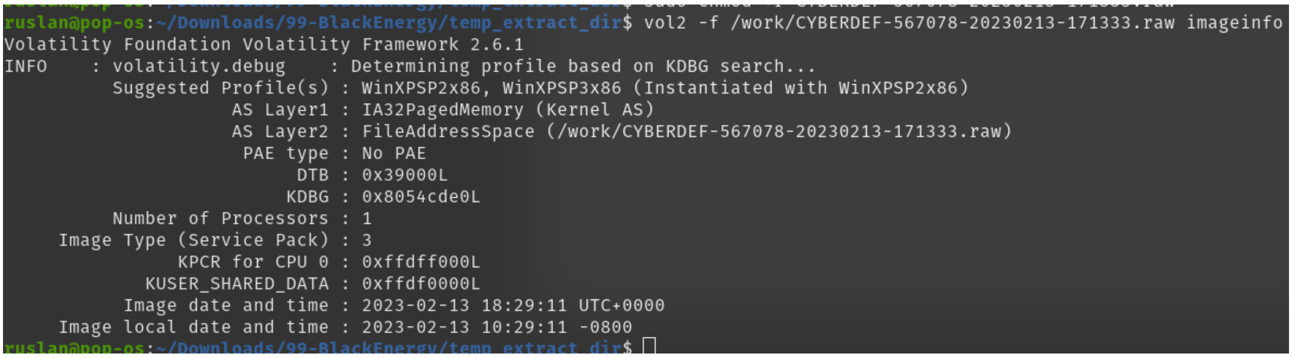
- Conduct a thorough investigation of the identified suspicious files, processes, and injected DLLs.
- Isolate the affected system to prevent further spread of the malware.
- Perform a full malware scan to identify and remove any additional malicious components.
- Update the system and apply security patches to mitigate future vulnerabilities.
- Consider performing a system-wide forensic investigation to assess the full extent of the compromise.

1. Which volatility profile would be best for this machine?

This command uses Volatility, a memory analysis framework, to inspect the memory image (CYBERDEF-567078-20230213-171333.raw). The imageinfo plugin extracts metadata about the image, including the best volatility profile for analysis. A volatility profile determines the specific operating system and architecture for which the memory image is optimized. In this case, the best profile identified was WinXPSP2x86, which refers to a 32-bit version of Windows XP Service Pack

2.

```
vol2 -f /work/CYBERDEF-567078-20230213-171333.raw imageinfo
```



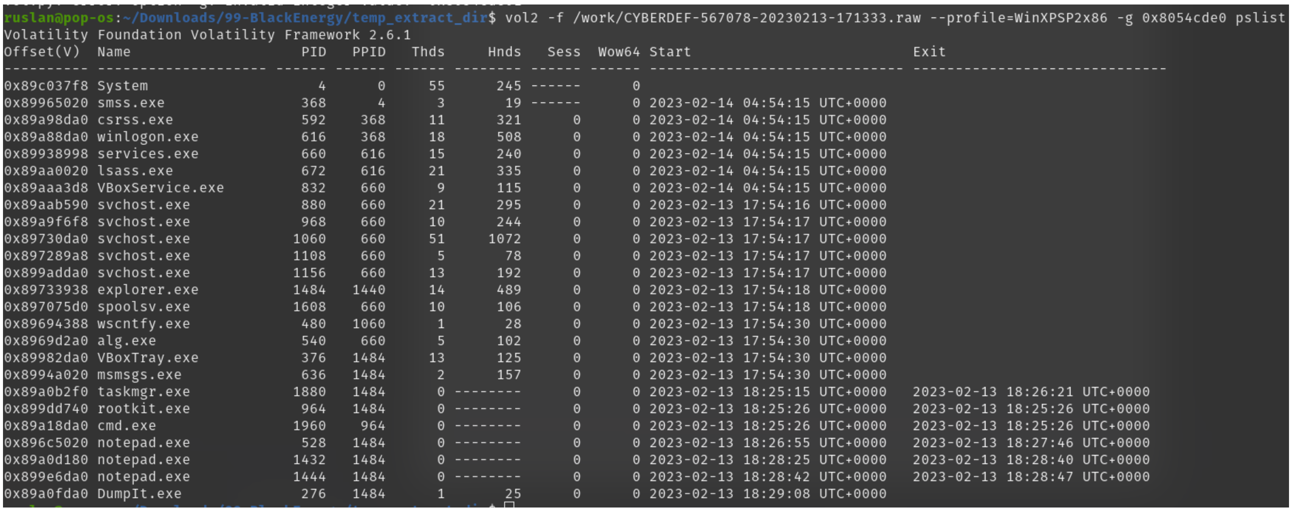
```
ruslan@pop-os:~/Downloads/99-BlackEnergy/temp_extract_dir$ vol2 -f /work/CYBERDEF-567078-20230213-171333.raw imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/work/CYBERDEF-567078-20230213-171333.raw)
                      PAE type : No PAE
                           DTB : 0x39000L
                          KDBG : 0x8054cde0L
          Number of Processors : 1
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2023-02-13 18:29:11 UTC+0000
     Image local date and time : 2023-02-13 10:29:11 -0800
ruslan@pop-os:~/Downloads/99-BlackEnergy/temp_extract_dir$ 
```

Answer: WinXPSP2x86

2. How many processes were running when the image was acquired?

The pslist plugin lists all the processes running at the time the memory image was captured. The -g parameter is used to specify the address of the kernel's process list, which is provided as 0x8054cde0. By using the specified profile (WinXPSP2x86), Volatility can interpret the memory structure and provide a list of active processes.

vol2 -f /work/CYBERDEF-567078-20230213-171333.raw --profile=WinXPSP2x86 -g 0x8054cde0 pslist



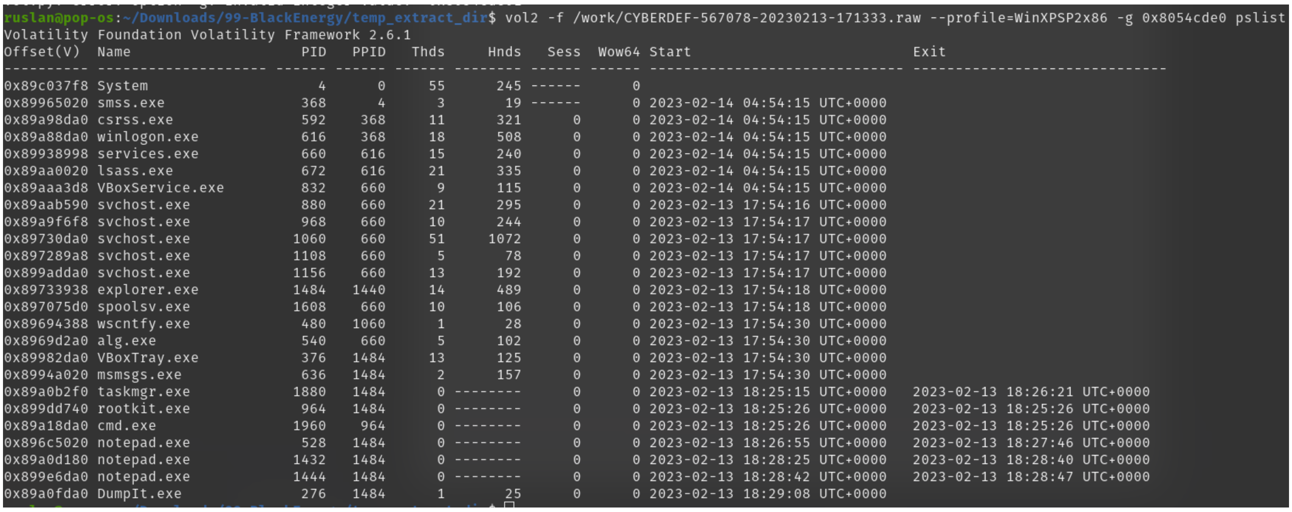
```
ruslan@pop-os:~/Downloads/99-BlackEnergy/temp_extract_dir$ vol2 -f /work/CYBERDEF-567078-20230213-171333.raw --profile=WinXPSP2x86 -g 0x8054cde0 pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x89c037f8 System                    4      0     55      245 ------      0
0x89965020 smss.exe                368      4      3       19 ------      0 2023-02-14 04:54:15 UTC+0000
0x89a98da0 csrss.exe               592    368     11      321      0      0 2023-02-14 04:54:15 UTC+0000
0x89a88da0 winlogon.exe            616    368     18      508      0      0 2023-02-14 04:54:15 UTC+0000
0x89938998 services.exe            660    616     15      240      0      0 2023-02-14 04:54:15 UTC+0000
0x89aa0020 lsass.exe               672    616     21      335      0      0 2023-02-14 04:54:15 UTC+0000
0x89aaa3d8 VBoxService.exe         832    660      9      115      0      0 2023-02-14 04:54:15 UTC+0000
0x89aab590 svchost.exe             880    660     21      295      0      0 2023-02-13 17:54:16 UTC+0000
0x89a9f6f8 svchost.exe             968    660     10      244      0      0 2023-02-13 17:54:17 UTC+0000
0x89730da0 svchost.exe            1060    660     51     1072      0      0 2023-02-13 17:54:17 UTC+0000
0x897289a8 svchost.exe            1108    660      5       78      0      0 2023-02-13 17:54:17 UTC+0000
0x899adda0 svchost.exe            1156    660     13      192      0      0 2023-02-13 17:54:17 UTC+0000
0x89733938 explorer.exe           1484   1440     14      489      0      0 2023-02-13 17:54:18 UTC+0000
0x897075d0 spoolsv.exe            1608    660     10      106      0      0 2023-02-13 17:54:18 UTC+0000
0x89694388 wscntfy.exe             480   1060      1       28      0      0 2023-02-13 17:54:30 UTC+0000
0x8969d2a0 alg.exe                 540    660      5      102      0      0 2023-02-13 17:54:30 UTC+0000
0x89982da0 VBoxTray.exe            376   1484     13      125      0      0 2023-02-13 17:54:30 UTC+0000
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
```

Answer: 19

3. What is the process ID of cmd.exe?

The process ID (PID) of cmd.exe is 1960. This is significant because cmd.exe is the Windows command shell, often used by attackers to execute commands in a compromised system. By identifying its PID, investigators can confirm that the system was running legitimate processes and may also look for unusual activity associated with this process, such as command execution by an attacker.

vol2 -f /work/CYBERDEF-567078-20230213-171333.raw --profile=WinXPSP2x86 -g 0x8054cde0 pslist



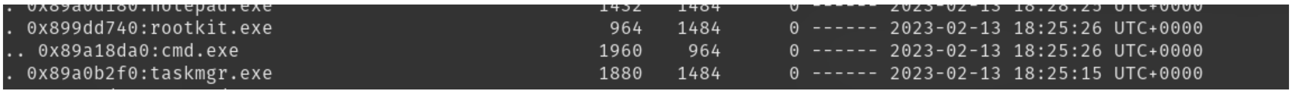
```
ruslan@pop-os:~/Downloads/99-BlackEnergy/temp_extract_dir$ vol2 -f /work/CYBERDEF-567078-20230213-171333.raw --profile=WinXPSP2x86 -g 0x8054cde0 pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x89c037f8 System                    4      0     55      245 ------      0
0x89965020 smss.exe                368      4      3       19 ------      0 2023-02-14 04:54:15 UTC+0000
0x89a98da0 csrss.exe               592    368     11      321      0      0 2023-02-14 04:54:15 UTC+0000
0x89a88da0 winlogon.exe            616    368     18      508      0      0 2023-02-14 04:54:15 UTC+0000
0x89938998 services.exe            660    616     15      240      0      0 2023-02-14 04:54:15 UTC+0000
0x89aa0020 lsass.exe               672    616     21      335      0      0 2023-02-14 04:54:15 UTC+0000
0x89aaa3d8 VBoxService.exe         832    660      9      115      0      0 2023-02-14 04:54:15 UTC+0000
0x89aab590 svchost.exe             880    660     21      295      0      0 2023-02-13 17:54:16 UTC+0000
0x89a9f6f8 svchost.exe             968    660     10      244      0      0 2023-02-13 17:54:17 UTC+0000
0x89730da0 svchost.exe            1060    660     51     1072      0      0 2023-02-13 17:54:17 UTC+0000
0x897289a8 svchost.exe            1108    660      5       78      0      0 2023-02-13 17:54:17 UTC+0000
0x899adda0 svchost.exe            1156    660     13      192      0      0 2023-02-13 17:54:17 UTC+0000
0x89733938 explorer.exe           1484   1440     14      489      0      0 2023-02-13 17:54:18 UTC+0000
0x897075d0 spoolsv.exe            1608    660     10      106      0      0 2023-02-13 17:54:18 UTC+0000
0x89694388 wscntfy.exe             480   1060      1       28      0      0 2023-02-13 17:54:30 UTC+0000
0x8969d2a0 alg.exe                 540    660      5      102      0      0 2023-02-13 17:54:30 UTC+0000
0x89982da0 VBoxTray.exe            376   1484     13      125      0      0 2023-02-13 17:54:30 UTC+0000
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
```

Answer: 1960

4. What is the name of the most suspicious process?

The process identified as the most suspicious is rootkit.exe. This is a common name for malicious software that is designed to hide itself and maintain unauthorized access to a system. Finding rootkit.exe in the process list is a strong indicator of a compromised machine, as rootkits are often used to mask the presence of other malicious processes and activities.

vol2 -f /work/CYBERDEF-567078-20230213-171333.raw --profile=WinXPSP2x86 -g 0x8054cde0 pstree



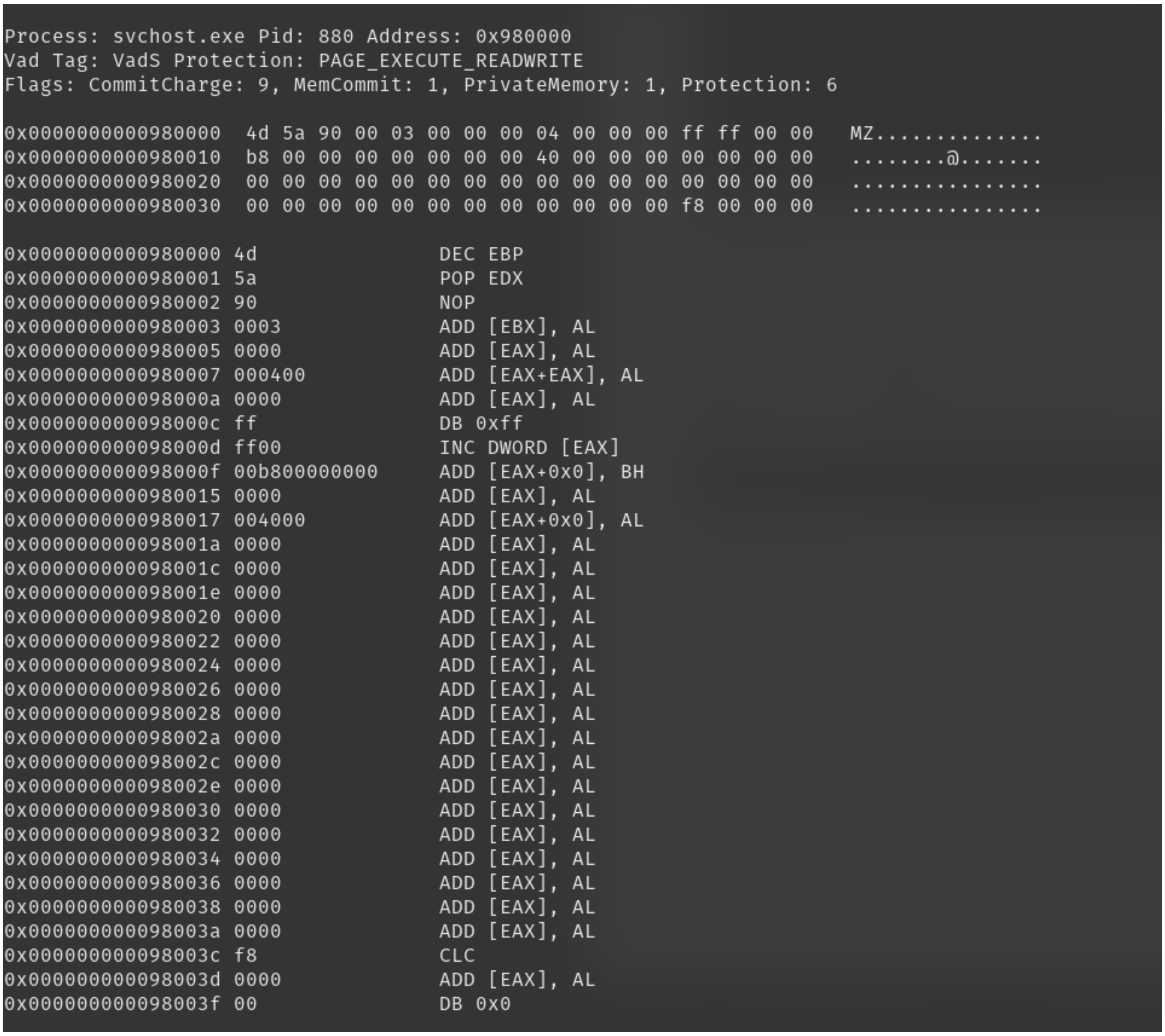
```
. 0x89a0d180:notepad.exe                           1432   1484      0 ------ 2023-02-13 18:28:25 UTC+0000
. 0x899dd740:rootkit.exe                            964   1484      0 ------ 2023-02-13 18:25:26 UTC+0000
.. 0x89a18da0:cmd.exe                              1960    964      0 ------ 2023-02-13 18:25:26 UTC+0000
. 0x89a0b2f0:taskmgr.exe                           1880   1484      0 ------ 2023-02-13 18:25:15 UTC+0000
```

Answer: rootkit.exe

5. Which process shows the highest likelihood of code injection?

The process with the highest likelihood of code injection is svchost.exe. This is important because svchost.exe is a legitimate Windows system process used to run services in the background, but it is also commonly targeted by malware for code injection. The presence of injected code in svchost.exe suggests that the system may have been compromised, and the injected code could be running malicious instructions within a trusted system process.

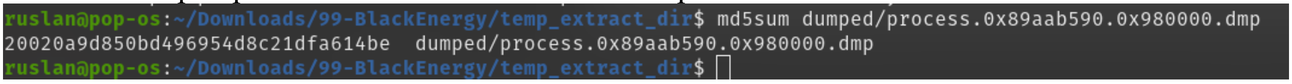
vol2 -f /work/CYBERDEF-567078-20230213-171333.raw --profile=WinXPSP2x86 -g 0x8054cde0 malfind



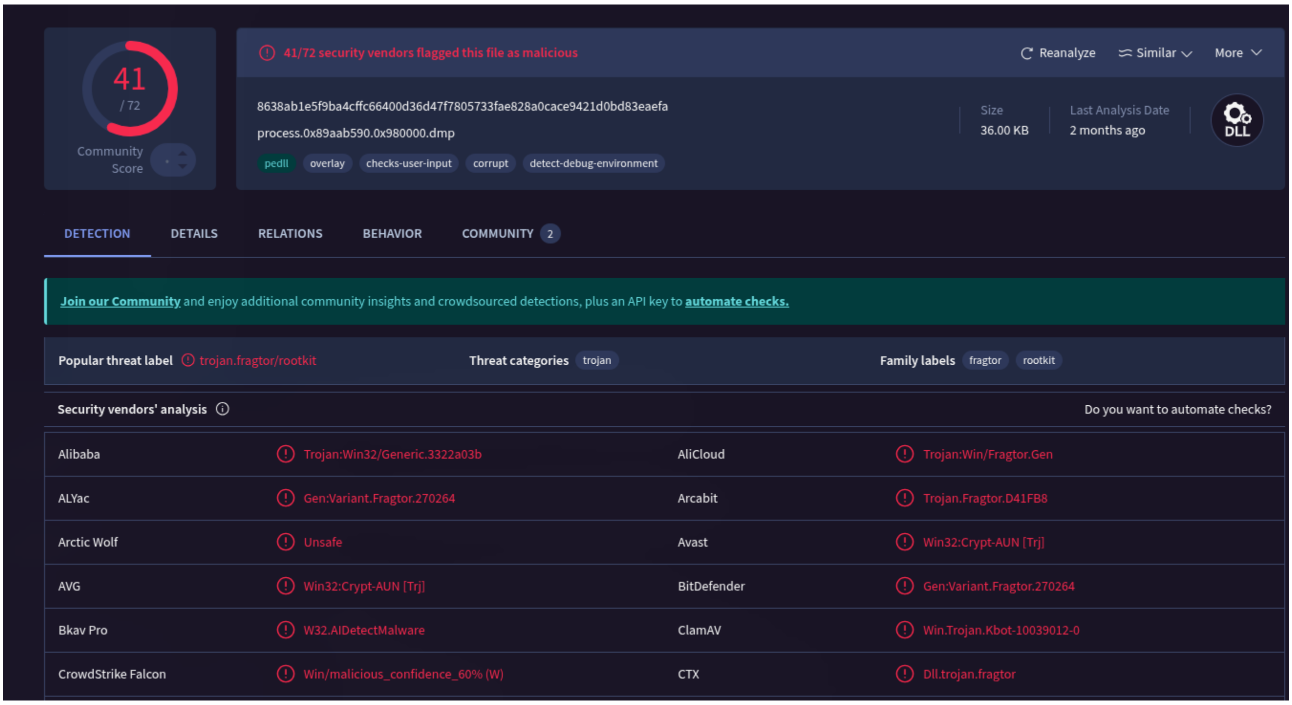
```
Process: svchost.exe Pid: 880 Address: 0x980000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 9, MemCommit: 1, PrivateMemory: 1, Protection: 6

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   ................

0x0000000000980000 4d               DEC EBP
0x0000000000980001 5a               POP EDX
0x0000000000980002 90               NOP
0x0000000000980003 0003             ADD [EBX], AL
0x0000000000980005 0000             ADD [EAX], AL
0x0000000000980007 000400           ADD [EAX+EAX], AL
0x000000000098000a 0000             ADD [EAX], AL
0x000000000098000c ff               DB 0xff
0x000000000098000d ff00             INC DWORD [EAX]
0x000000000098000f 00b800000000     ADD [EAX+0x0], BH
0x0000000000980015 0000             ADD [EAX], AL
0x0000000000980017 004000           ADD [EAX+0x0], AL
0x000000000098001a 0000             ADD [EAX], AL
0x000000000098001c 0000             ADD [EAX], AL
0x000000000098001e 0000             ADD [EAX], AL
0x0000000000980020 0000             ADD [EAX], AL
0x0000000000980022 0000             ADD [EAX], AL
0x0000000000980024 0000             ADD [EAX], AL
0x0000000000980026 0000             ADD [EAX], AL
0x0000000000980028 0000             ADD [EAX], AL
0x000000000098002a 0000             ADD [EAX], AL
0x000000000098002c 0000             ADD [EAX], AL
0x000000000098002e 0000             ADD [EAX], AL
0x0000000000980030 0000             ADD [EAX], AL
0x0000000000980032 0000             ADD [EAX], AL
0x0000000000980034 0000             ADD [EAX], AL
0x0000000000980036 0000             ADD [EAX], AL
0x0000000000980038 0000             ADD [EAX], AL
0x000000000098003a 0000             ADD [EAX], AL
0x000000000098003c f8               CLC
0x000000000098003d 0000             ADD [EAX], AL
0x000000000098003f 00               DB 0x0
```

vol2 -f /work/CYBERDEF-567078-20230213-171333.raw --profile=WinXPSP2x86 -g 0x8054cde0 malfind -p 880 -D /work/dumped

md5sum dumped/process.0x89aab590.0x980000.dmp



```
ruslan@pop-os:~/Downloads/99-BlackEnergy/temp_extract_dir$ md5sum dumped/process.0x89aab590.0x980000.dmp
20020a9d850bd496954d8c21dfa614be  dumped/process.0x89aab590.0x980000.dmp
ruslan@pop-os:~/Downloads/99-BlackEnergy/temp_extract_dir$ 
```



41/72 security vendors flagged this file as malicious

8638ab1e5f9ba4cffc66400d36d47f7805733fae828a0cace9421d0bd83eaefa

process.0x89aab590.0x980000.dmp

pedll overlay checks-user-input corrupt detect-debug-environment

Size 36.00 KB

Last Analysis Date 2 months ago

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

Popular threat label trojan.fragtor/rootkit   Threat categories trojan   Family labels fragtor rootkit

Security vendors' analysis   Do you want to automate checks?

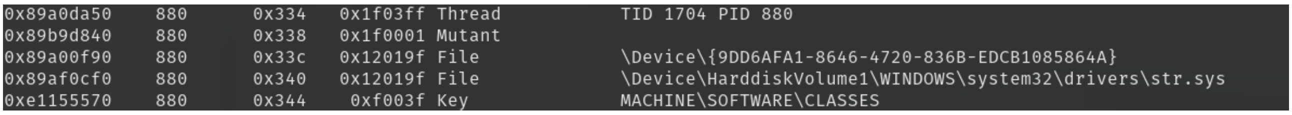
Alibaba	Trojan:Win32/Generic.3322a03b	AliCloud	Trojan:Win/Fragtor.Gen
ALYac	Gen:Variant.Fragtor.270264	Arcabit	Trojan.Fragtor.D41FB8
Arctic Wolf	Unsafe	Avast	Win32:Crypt-AUN [Trj]
AVG	Win32:Crypt-AUN [Trj]	BitDefender	Gen:Variant.Fragtor.270264
Bkav Pro	W32.AIDetectMalware	ClamAV	Win.Trojan.Kbot-10039012-0
CrowdStrike Falcon	Win/malicious_confidence_60% (W)	CTX	Dll.trojan.fragtor

Answer: svchost.exe

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

The file str.sys located in C:\WINDOWS\system32\drivers\ is referenced by a process. This is suspicious because it is not a standard Windows system file, and it may have been introduced by malware to further compromise the system. The location within the system32\drivers folder is particularly concerning, as this is where kernel-mode drivers typically reside, and a malicious driver can provide deep access to the system, allowing the malware to operate stealthily.

```
vol2 -f /work/CYBERDEF-567078-20230213-171333.raw --profile=WinXPSP2x86 -g 0x8054cde0
handles -p 880
```

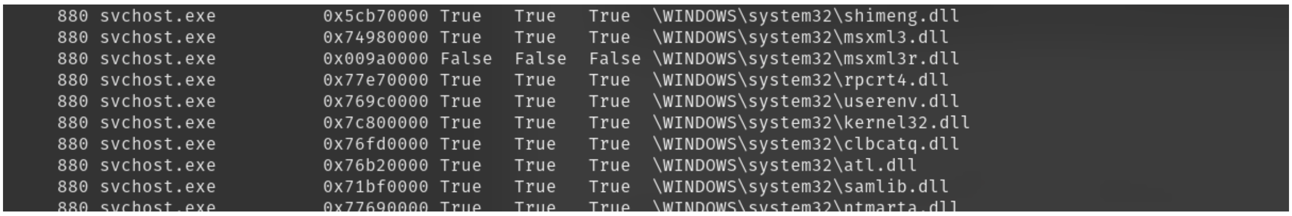


```
0x89a0da50     880       0x334   0x1f03ff Thread            TID 1704 PID 880
0x89b9d840     880       0x338   0x1f0001 Mutant
0x89a00f90     880       0x33c   0x12019f File              \Device\{9DD6AFA1-8646-4720-836B-EDCB1085864A}
0x89af0cf0     880       0x340   0x12019f File              \Device\HarddiskVolume1\WINDOWS\system32\drivers\str.sys
0xe1155570     880       0x344    0xf003f Key               MACHINE\SOFTWARE\CLASSES
```

Answer: C:\WINDOWS\system32\drivers\str.sys

7. What is the name of the injected DLL file loaded from the recent process?

```
vol2 -f /work/CYBERDEF-567078-20230213-171333.raw --profile=WinXPSP2x86 -g 0x8054cde0
ldrmodules -p 880
```



```
    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
    880 svchost.exe          0x77690000 True   True   True  \WINDOWS\system32\ntmarta.dll
```

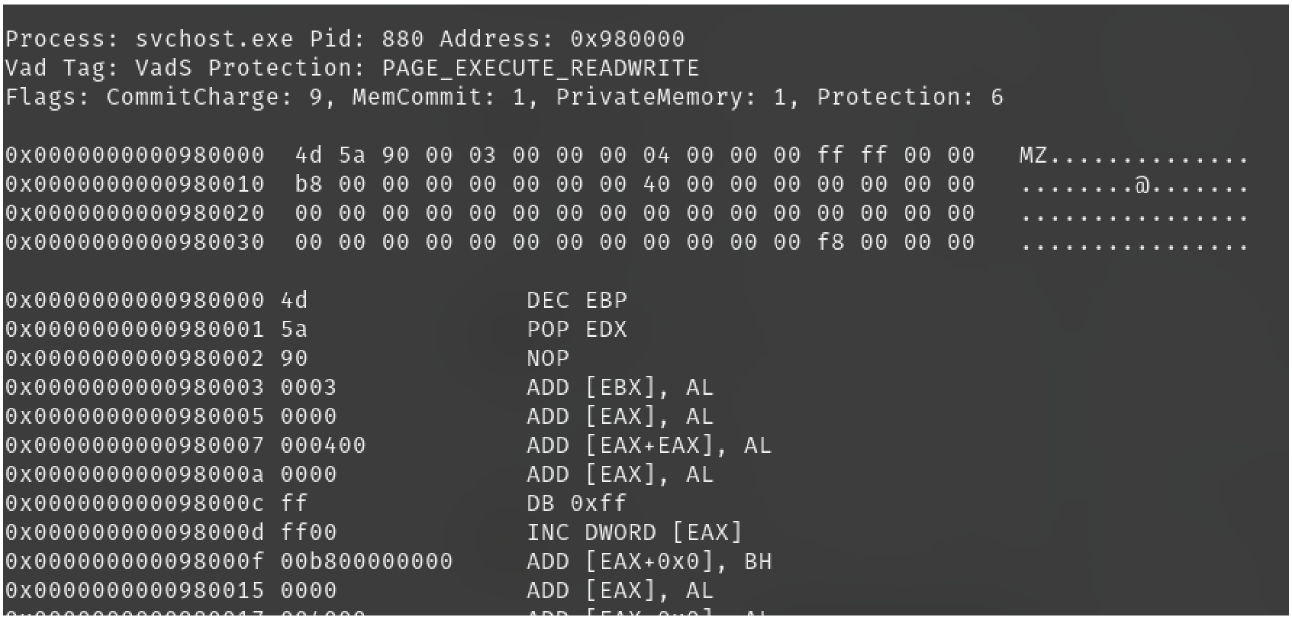
Answer: msxml3r.dll

The injected DLL file is msxml3r.dll. This file is not a standard system DLL, suggesting that it may have been placed by malware to enable its functionality. Injected DLLs are a common method for malware to alter the behavior of legitimate processes or to load additional malicious code. The presence of this DLL indicates an advanced form of malware that uses code injection to hide its presence and maintain control over the system.

8. What is the base address of the injected DLL?

The base address of the injected DLL is 0x980000. This is the location in memory where the injected DLL has been loaded. Knowing the base address is important for further analysis, as investigators can use it to locate the DLL in memory, extract it, and analyze its contents. This can help determine what the DLL does, how it interacts with other system components, and whether it is part of a larger malware payload.

vol2 -f /work/CYBERDEF-567078-20230213-171333.raw --profile=WinXPSP2x86 -g 0x8054cde0 malfind



```
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   ................

0x0000000000980000 4d               DEC EBP
0x0000000000980001 5a               POP EDX
0x0000000000980002 90               NOP
0x0000000000980003 0003             ADD [EBX], AL
0x0000000000980005 0000             ADD [EAX], AL
0x0000000000980007 000400           ADD [EAX+EAX], AL
0x000000000098000a 0000             ADD [EAX], AL
0x000000000098000c ff               DB 0xff
0x000000000098000d ff00             INC DWORD [EAX]
0x000000000098000f 00b800000000     ADD [EAX+0x0], BH
0x0000000000980015 0000             ADD [EAX], AL
0x0000000000980017 004000           ADD [EAX+0x0], AL
```

Answer: 0x980000