SYNC 3.15.89

Date: October 19th, 2018.

Description

This a review of the CVE-2018-17538. This CVE identified some vulnerabilities in the software SYNC.3.15.89[1]. The main vulnerability of the software presented in the report was due to the possibility of a process injection which could cause opportunities to many different types of threats, accordingly to the payload used in each case. Up to this point, the initial presentation of this CVE identified the main vulnerable files, which could be then used to enumerate and target the processes of the software.

This review demonstrates how to get advantage of this vulnerability (process injection) by building an exploit and injecting the payload in one of the processes used by the software. Once the software is installed, the detection of the malicious file would be more difficult to be recognized, since the payload would be part of an authorized software. The payload created (Virus_Injection.dll) has a mechanism to reverse a session to a fictional IP address (192.168.1.99:1234) and would allow a remote code execution by an adversary.

The payload could be delivered by different means. For example, a dynamic-link library (*.dll) file could be embedded in the software prior to installation. And it also possible to inject the same *.dll file using a local access and a DLL injector to associate the malicious *.dll file to the main process (SYNC.exe).

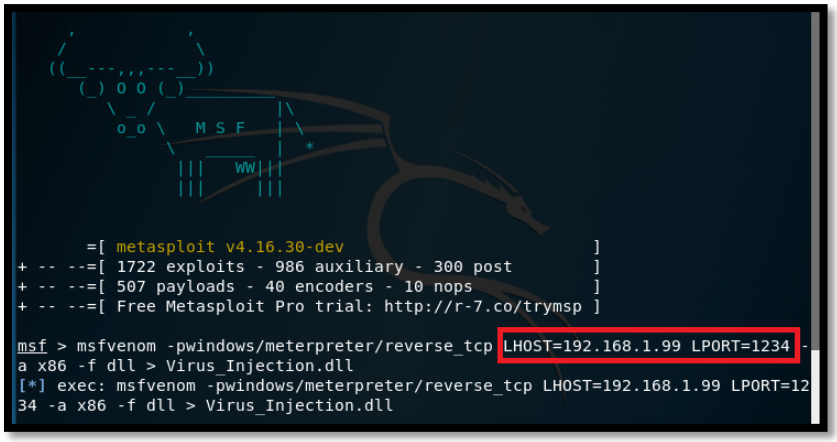
Table of Contents

[1] https://github.com/GitHubAssessments/CVE_Assessment_05_2018/blob/master/Evidence_Sync_Report.pdf

Executed Procedures

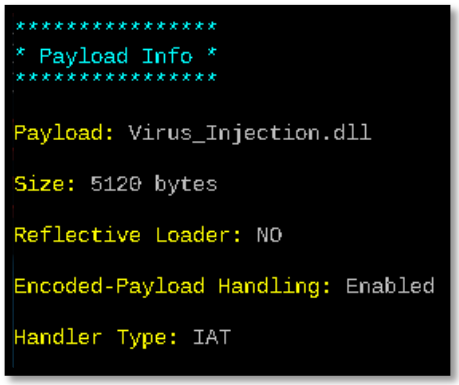
Payload Creation

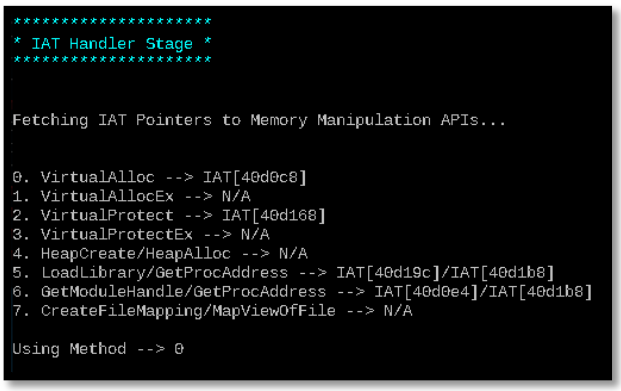
1. First it was created a payload[2] using Metasploit:



First Approach

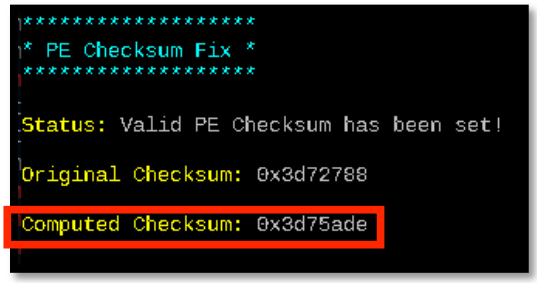
2. The first approach more efficient would be to modify the original file (Evidence_SYNC_Setup.exe[3]) before installation to add the payload created.



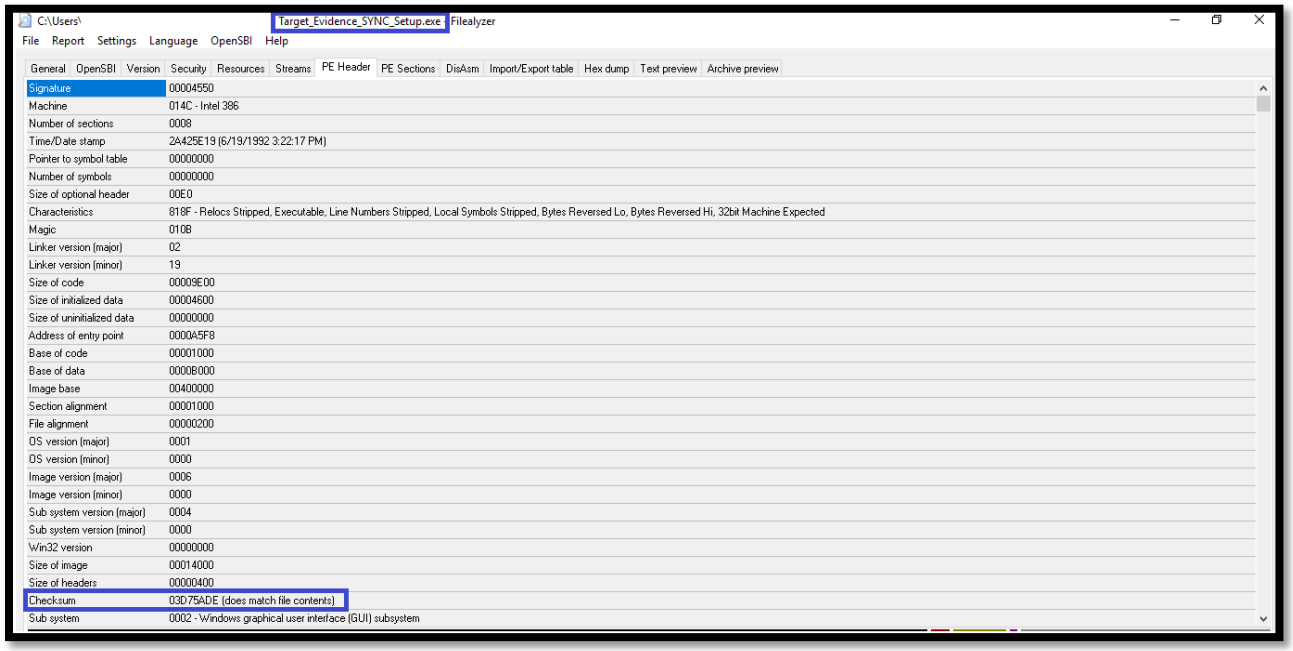


[2] https://www.virustotal.com/#/file/ceeca99cb1003008028fc07c76628b0383f27aa05116743bb3ea37160c552d11/detection

[3] https://www.hybrid-analysis.com/sample/fd574ef4edc93657dc9bdd5d132e3481eace05b5b336aecf7be29768ec51c54c?environmentId=100



3. Then, the new file (Target_Evidence_SYNC_Setup.exe[4]) including the payload[5] is created and will be deployed during the installation:

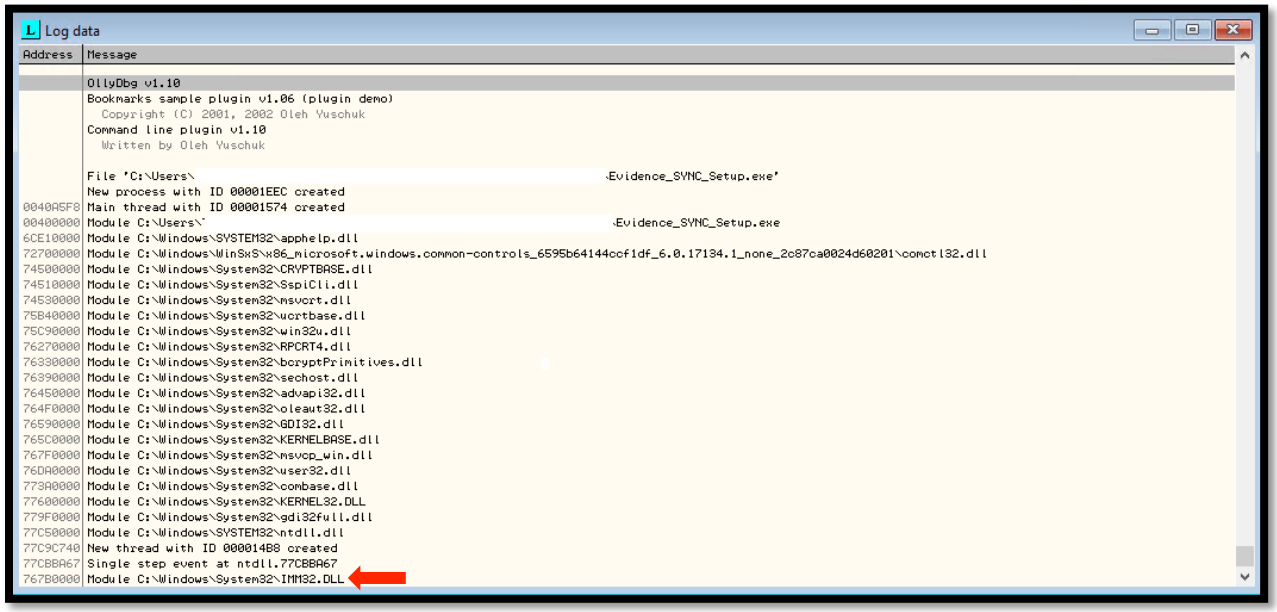


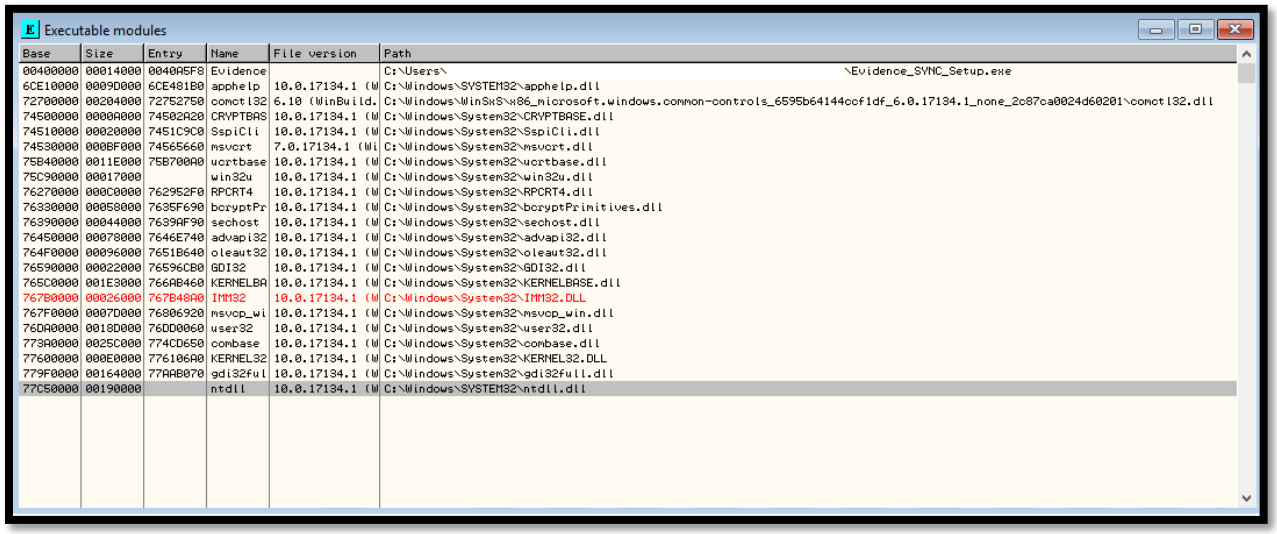
4. Once the software is installed the malicious *.dll file would work as intended.

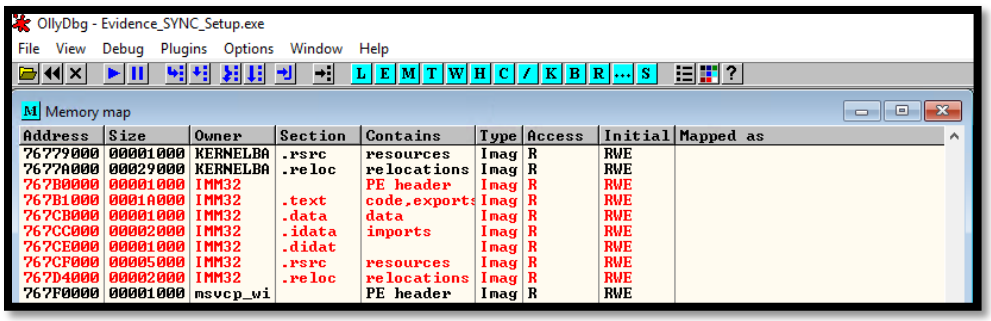
5. This approach took benefit of the process IMM32.dll. In the original version this *.dll file was flagged:

[4]https://www.virustotal.com/#/file/cbed5b25c72a5eefe978b72b22bb228b67c3ed80fd7205f0d8ee3d76eb4b5fc0/detection

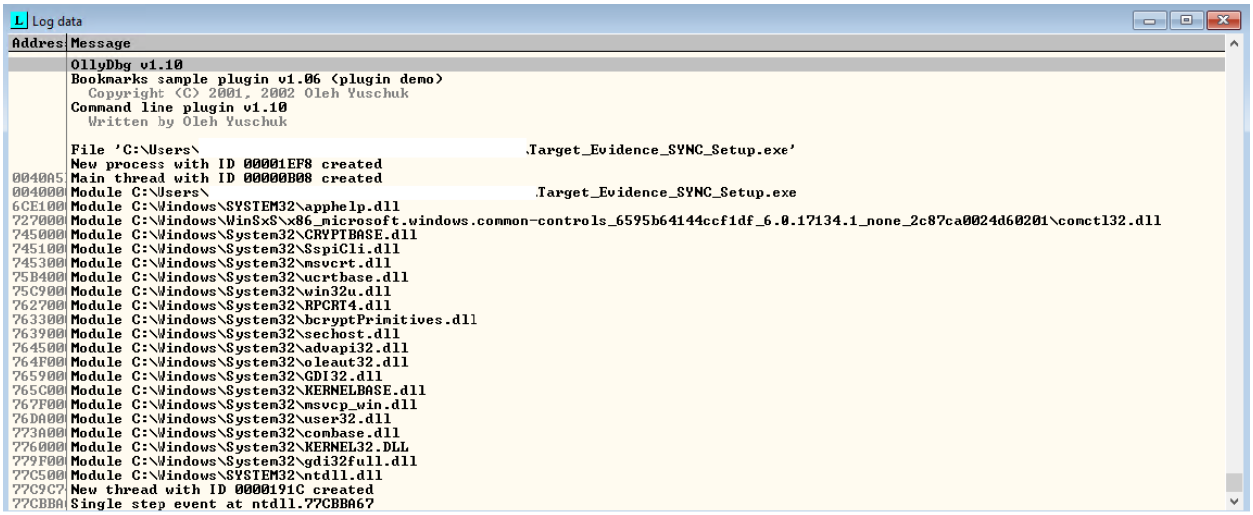
[5] https://www.hybrid-analysis.com/sample/cbed5b25c72a5eefe978b72b22bb228b67c3ed80fd7205f0d8ee3d76eb4b5fc0?environmentId=100

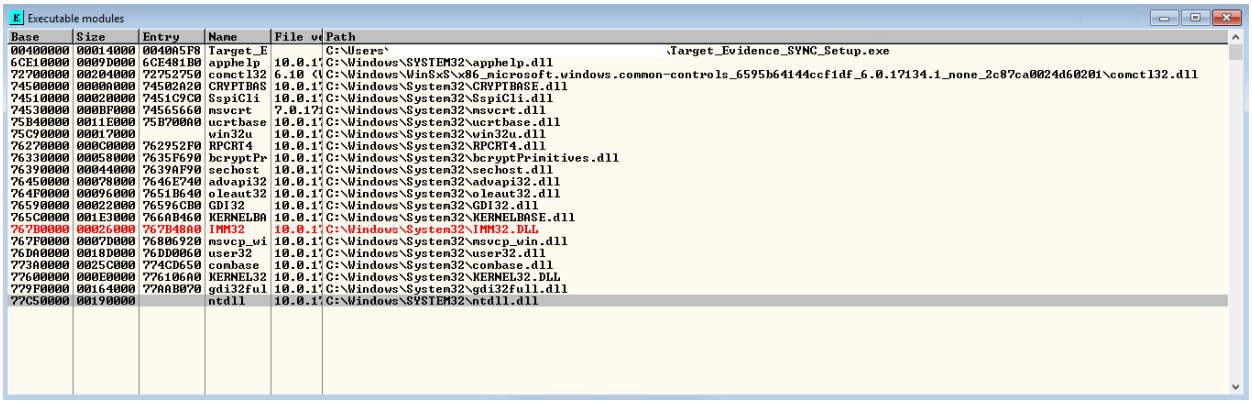

Log data
Address
Message
OllyDbg v1.10
Bookmarks sample plugin v1.06 (plugin demo)
Copyright (C) 2001, 2002 Oleh Yuschuk
Command line plugin v1.10
Written by Oleh Yuschuk
File 'C:\Users\ Evidence_SYNC_Setup.exe'
New process with ID 00001EEC created
0040A5F8 Main thread with ID 00001574 created
00400000 Module C:\Users\ Evidence_SYNC_Setup.exe
6CE10000 Module C:\Windows\SYSTEM32\apphelp.dll
72700000 Module C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.17134.1_none_2c87ca0024d60201\comctl32.dll
74500000 Module C:\Windows\System32\CRYPTBASE.dll
74510000 Module C:\Windows\System32\SspiCli.dll
74530000 Module C:\Windows\System32\msvcrt.dll
75B40000 Module C:\Windows\System32\ucrtbase.dll
75C90000 Module C:\Windows\System32\win32u.dll
76270000 Module C:\Windows\System32\RPCRT4.dll
76330000 Module C:\Windows\System32\bcryptPrimitives.dll
76390000 Module C:\Windows\System32\sechost.dll
76450000 Module C:\Windows\System32\advapi32.dll
764F0000 Module C:\Windows\System32\oleaut32.dll
76590000 Module C:\Windows\System32\GDI32.dll
765C0000 Module C:\Windows\System32\KERNELBASE.dll
767F0000 Module C:\Windows\System32\msvcp_win.dll
76DA0000 Module C:\Windows\System32\user32.dll
773A0000 Module C:\Windows\System32\combase.dll
77600000 Module C:\Windows\System32\KERNEL32.DLL
779F0000 Module C:\Windows\System32\gdi32full.dll
77C50000 Module C:\Windows\SYSTEM32\ntdll.dll
77C9C740 New thread with ID 000014B8 created
77CBBA67 Single step event at ntdll.77CBBA67
767B0000 Module C:\Windows\System32\IMM32.DLL

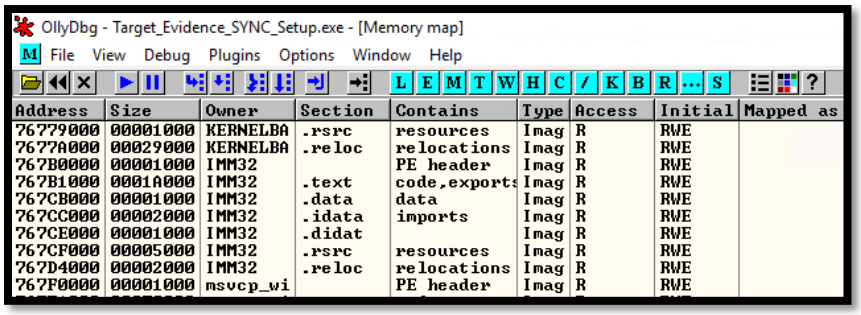

Executable modules
Base Size Entry Name File version Path
00400000 00014000 0040A5F8 Evidence C:\Users\ \Evidence_SYNC_Setup.exe
6CE10000 0009D000 6CE481B0 apphelp 10.0.17134.1 (W C:\Windows\SYSTEM32\apphelp.dll
72700000 00204000 72752750 comctl32 6.10 (WinBuild. C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.17134.1_none_2c87ca0024d60201\comctl32.dll
74500000 0000A000 74502A20 CRYPTBAS 10.0.17134.1 (W C:\Windows\System32\CRYPTBASE.dll
74510000 00020000 7451C9C0 SspiCli 10.0.17134.1 (W C:\Windows\System32\SspiCli.dll
74530000 000BF000 74565660 msvcrt 7.0.17134.1 (Wi C:\Windows\System32\msvcrt.dll
75B40000 0011E000 75B700A0 ucrtbase 10.0.17134.1 (W C:\Windows\System32\ucrtbase.dll
75C90000 00017000 win32u 10.0.17134.1 (W C:\Windows\System32\win32u.dll
76270000 000C0000 762952F0 RPCRT4 10.0.17134.1 (W C:\Windows\System32\RPCRT4.dll
76330000 00058000 7635F690 bcryptPr 10.0.17134.1 (W C:\Windows\System32\bcryptPrimitives.dll
76390000 00044000 7639AF90 sechost 10.0.17134.1 (W C:\Windows\System32\sechost.dll
76450000 00078000 7646E740 advapi32 10.0.17134.1 (W C:\Windows\System32\advapi32.dll
764F0000 00096000 7651B640 oleaut32 10.0.17134.1 (W C:\Windows\System32\oleaut32.dll
76590000 00022000 76596CB0 GDI32 10.0.17134.1 (W C:\Windows\System32\GDI32.dll
765C0000 001E3000 766AB460 KERNELBA 10.0.17134.1 (W C:\Windows\System32\KERNELBASE.dll
767B0000 00026000 767B48A0 IMM32 10.0.17134.1 (W C:\Windows\System32\IMM32.DLL
767F0000 0007D000 76806920 msvcp_wi 10.0.17134.1 (W C:\Windows\System32\msvcp_win.dll
76DA0000 0018D000 76DD0060 user32 10.0.17134.1 (W C:\Windows\System32\user32.dll
773A0000 0025C000 774CD650 combase 10.0.17134.1 (W C:\Windows\System32\combase.dll
77600000 000E0000 776106A0 KERNEL32 10.0.17134.1 (W C:\Windows\System32\KERNEL32.DLL
779F0000 00164000 77AAB070 gdi32ful 10.0.17134.1 (W C:\Windows\System32\gdi32full.dll
77C50000 00190000 ntdll 10.0.17134.1 (W C:\Windows\SYSTEM32\ntdll.dll


OllyDbg - Evidence_SYNC_Setup.exe
File View Debug Plugins Options Window Help
Memory map
Address Size Owner Section Contains Type Access Initial Mapped as
76779000 00001000 KERNELBA .rsrc resources Imag R RWE
7677A000 00029000 KERNELBA .reloc relocations Imag R RWE
767B0000 00001000 IMM32 PE header Imag R RWE
767B1000 0001A000 IMM32 .text code,exports Imag R RWE
767CB000 00001000 IMM32 .data data Imag R RWE
767CC000 00002000 IMM32 .idata imports Imag R RWE
767CE000 00001000 IMM32 .didat Imag R RWE
767CF000 00005000 IMM32 .rsrc resources Imag R RWE
767D4000 00002000 IMM32 .reloc relocations Imag R RWE
767F0000 00001000 msvcp_wi PE header Imag R RWE

6. In the modified version, the process IMM32.dll was removed and the ID of the processes changed. The process IMM32.dll is now integrated with the payload.



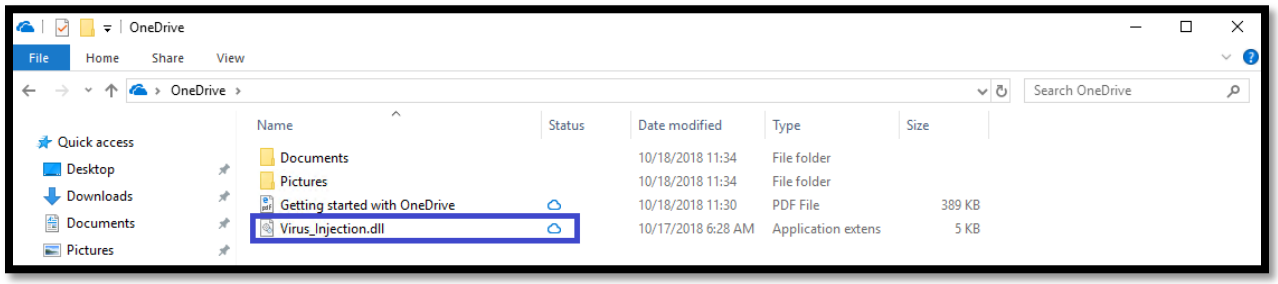




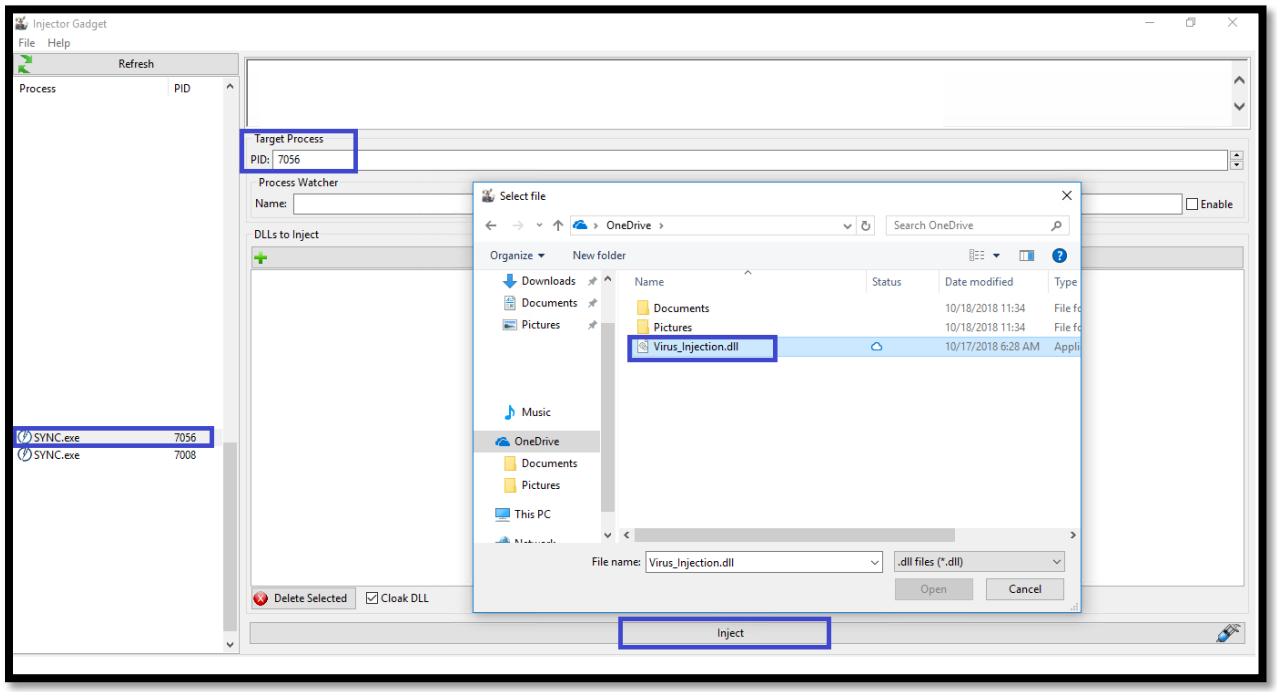
Second Approach

7. An alternative approach would be to inject the payload through a USB flash drive or accessing the file in the Cloud, and then directly associate the *.dll file to the Process ID (PID) of the software. This injection could be made by a DLL injector.

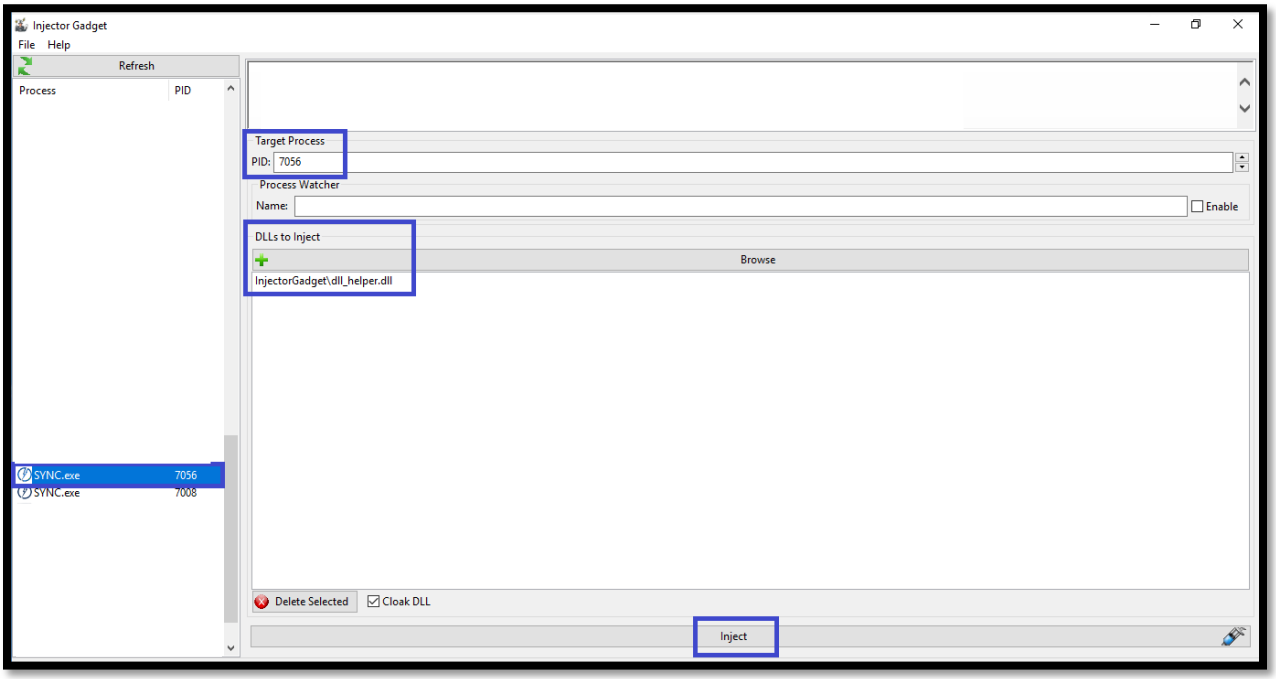
8. Access the file:



9. Locate the process (PID) and associate with the payload file, using a DLL injector:



10. The *.dll file will be added to the SYNC process. Note that any *.dll file could be added to the process, including a less offensive one.



11. By monitoring the specific process it is possible to confirm the injection to the assigned Process ID (PID):