PROG8300-22F – Malware Project – John White (6714158)

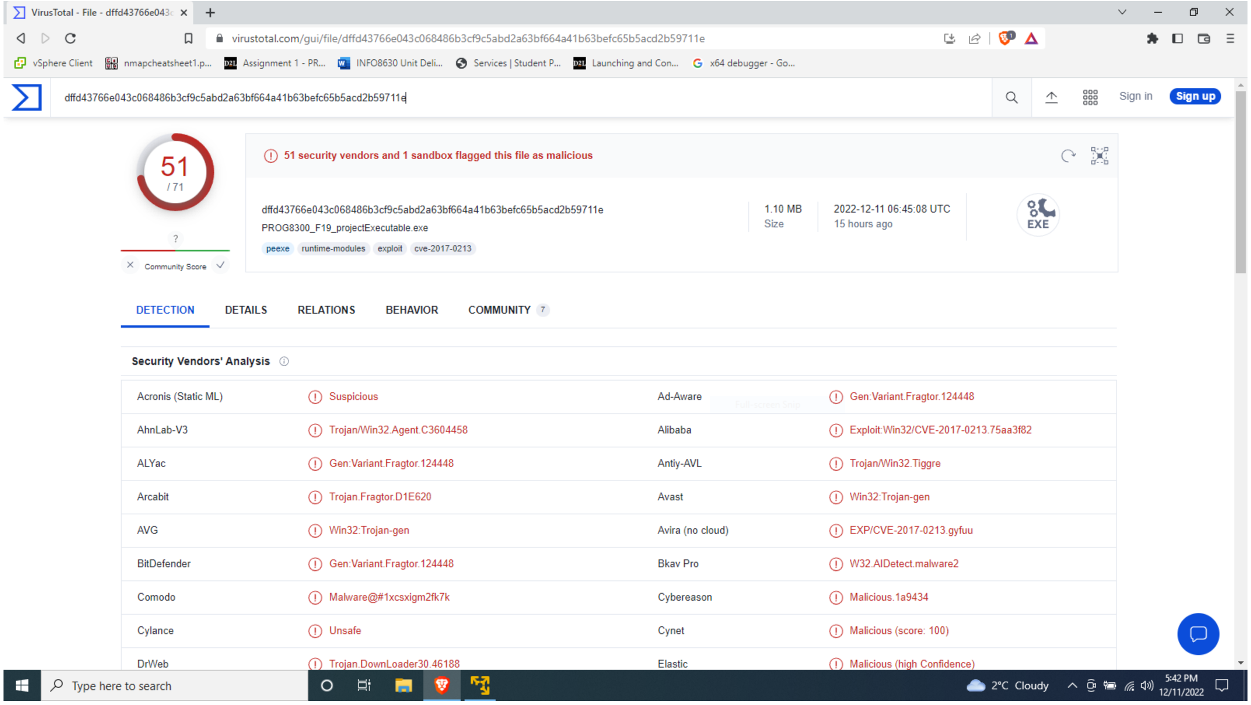
To begin the analysis, I uploaded the .exe file to VirusTotal.com to see if it matched any existing virus signatures (**Figure 1**). Many vendors did identify the .exe as malware and several of them suggested that the file could be a Trojan virus. I then continued with the static analysis using IDA. Based on the strings and imports, it seems like a large part of the program's functionality involves creating, opening, and modifying files (**Figure 2** and **Figure 3**). I also analyzed the file using PEid and OllyDBG (**Figure 4** and **Figure 5**) but I did not find anything that I thought was useful. Using DependancyWalker (**Figure 6**), we can verify many of the imports that we found using IDA.

For the dynamic analysis, I started with RegShot (**Figure 7**). RegShot did indeed find that multiple registries were edited by the program. Many of these registries were also listed in Process Monitor (**Figure 8**). It also seems to have made modifications so several other files as well. When I ran the executable and input the password 'PROG8300', it created a file on my desktop called 'AAAAAAAAAAA' and the terminal closed. I am not sure what the purpose of this file is as of right now.

I could not get a network connection to work on my sandbox VM without sharing direct access to my network card, so I could not perform this portion of the analysis effectively. However, based on some of the imports and strings from IDA, it seems that this executable does have networking capabilities, most likely for the purpose of downloading files from somewhere.

In conclusion, I believe that the purpose of this executable is to be a trojan virus downloader/installer. The program would be hidden in a seemingly-innocuous file and when run, it would install a virus on your computer that could log your keyboard activity or potentially act as a backdoor. It could also be very difficult to remove this virus once it's been installed, because the installer can change the registry as well to make it appear as though the virus is not present. It is highly advised to take the precautions necessary to avoid this malware in the first place.

Screenshots



dffd43766e043c068486b3cf9c5abd2a63bf664a41b63befc65b5acd2b59711e

51 / 71

? Community Score

51 security vendors and 1 sandbox flagged this file as malicious

dffd43766e043c068486b3cf9c5abd2a63bf664a41b63befc65b5acd2b59711e
PROG8300_F19_projectExecutable.exe
peexe runtime-modules exploit cve-2017-0213

1.10 MB
Size

2022-12-11 06:45:08 UTC
15 hours ago

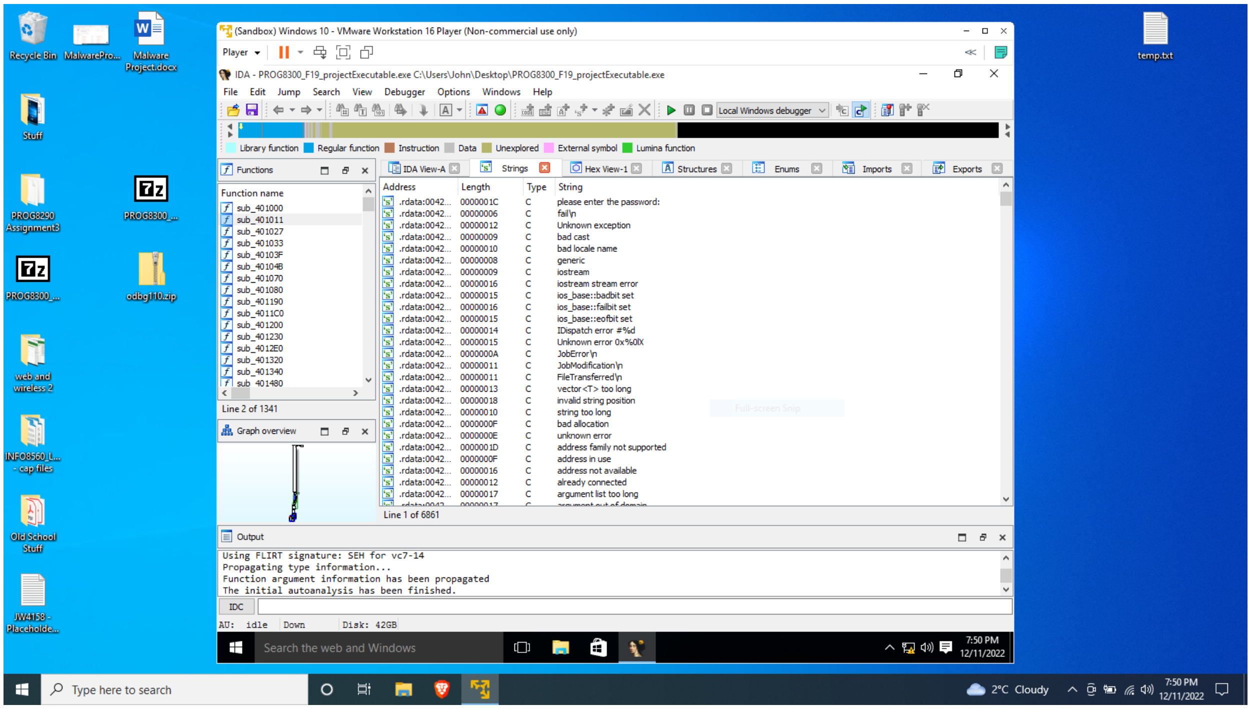
EXE

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 7

Security Vendors' Analysis

Acronis (Static ML)	Suspicious	Ad-Aware	Gen:Variant.Fragtor.124448
AhnLab-V3	Trojan/Win32.Agent.C3604458	Alibaba	Exploit:Win32/CVE-2017-0213.75aa3f82
ALYac	Gen:Variant.Fragtor.124448	Antiy-AVL	Trojan/Win32.Tiggre
Arcabit	Trojan.Fragtor.D1E620	Avast	Win32:Trojan-gen
AVG	Win32:Trojan-gen	Avira (no cloud)	EXP/CVE-2017-0213.gyfuu
BitDefender	Gen:Variant.Fragtor.124448	Bkav Pro	W32.AIDetect.malware2
Comodo	Malware@#1xcsxigm2fk7k	Cybereason	Malicious.1a9434
Cylance	Unsafe	Cynet	Malicious (score: 100)
DrWeb	Trojan.DownLoader30.46188	Elastic	Malicious (high Confidence)

Figure 1 – VirusTotal analysis



(Sandbox) Windows 10 - VMware Workstation 16 Player (Non-commercial use only)

IDA - PROG8300_F19_projectExecutable.exe C:\Users\John\Desktop\PROG8300_F19_projectExecutable.exe

```
Function name
sub_401000
sub_401011
sub_401027
sub_401033
sub_40103F
sub_40104B
sub_401070
sub_401080
sub_401190
sub_4011C0
sub_401200
sub_401230
sub_4012E0
sub_401320
sub_401340
sub_401480
```

Line 2 of 1341

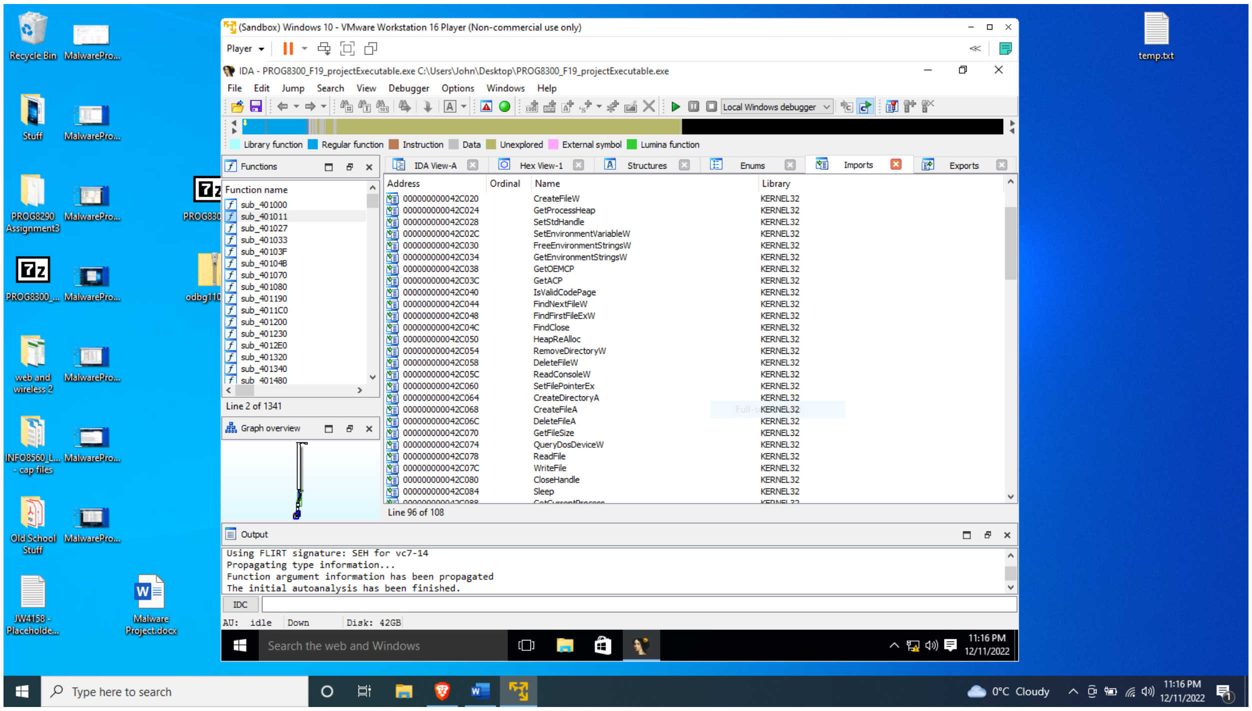
Address	Length	Type	String
.rdata:0042...	0000001C	C	please enter the password:
.rdata:0042...	00000006	C	fail\n
.rdata:0042...	00000012	C	Unknown exception
.rdata:0042...	00000009	C	bad cast
.rdata:0042...	00000010	C	bad locale name
.rdata:0042...	00000008	C	generic
.rdata:0042...	00000009	C	iostream
.rdata:0042...	00000016	C	iostream stream error
.rdata:0042...	00000015	C	ios_base::badbit set
.rdata:0042...	00000016	C	ios_base::failbit set
.rdata:0042...	00000015	C	ios_base::eofbit set
.rdata:0042...	00000014	C	IDispatch error #%d
.rdata:0042...	00000015	C	Unknown error 0x%0lX
.rdata:0042...	0000000A	C	JobError\n
.rdata:0042...	00000011	C	JobModification\n
.rdata:0042...	00000011	C	FileTransferred\n
.rdata:0042...	00000013	C	vector<T> too long
.rdata:0042...	00000018	C	invalid string position
.rdata:0042...	00000010	C	string too long
.rdata:0042...	0000000F	C	bad allocation
.rdata:0042...	0000000E	C	unknown error
.rdata:0042...	0000001D	C	address family not supported
.rdata:0042...	0000000F	C	address in use
.rdata:0042...	00000016	C	address not available
.rdata:0042...	00000012	C	already connected
.rdata:0042...	00000017	C	argument list too long
.rdata:0042...	00000017	C	argument out of domain

Line 1 of 6861

```
Using FLIRT signature: SEH for vc7-14
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished.
```

```
AU:  idle   Down       Disk: 42GB
```

Figure 2 – IDA analysis (strings)



(Sandbox) Windows 10 - VMware Workstation 16 Player (Non-commercial use only)

IDA - PROG8300_F19_projectExecutable.exe C:\Users\John\Desktop\PROG8300_F19_projectExecutable.exe

File Edit Jump Search View Debugger Options Windows Help
Local Windows debugger
Library function Regular function Instruction Data Unexplored External symbol Lumina function
Functions IDA View-A Hex View-1 Structures Enums Imports Exports
Graph overview
Output
IDC
Recycle Bin
MalwarePro...
Stuff
PROG8290 Assignment3
PROG8300_...
web and wireless 2
INFO8560_L... - cap files
Old School Stuff
JW4158 - Placeholde...
Malware Project.docx
odbg110
temp.txt
Search the web and Windows
Type here to search
0°C Cloudy

```
Function name
sub_401000
sub_401011
sub_401027
sub_401033
sub_40103F
sub_40104B
sub_401070
sub_401080
sub_401190
sub_4011C0
sub_401200
sub_401230
sub_4012E0
sub_401320
sub_401340
sub_401480
Line 2 of 1341
```

Address	Ordinal	Name	Library
000000000042C020		CreateFileW	KERNEL32
000000000042C024		GetProcessHeap	KERNEL32
000000000042C028		SetStdHandle	KERNEL32
000000000042C02C		SetEnvironmentVariableW	KERNEL32
000000000042C030		FreeEnvironmentStringsW	KERNEL32
000000000042C034		GetEnvironmentStringsW	KERNEL32
000000000042C038		GetOEMCP	KERNEL32
000000000042C03C		GetACP	KERNEL32
000000000042C040		IsValidCodePage	KERNEL32
000000000042C044		FindNextFileW	KERNEL32
000000000042C048		FindFirstFileExW	KERNEL32
000000000042C04C		FindClose	KERNEL32
000000000042C050		HeapReAlloc	KERNEL32
000000000042C054		RemoveDirectoryW	KERNEL32
000000000042C058		DeleteFileW	KERNEL32
000000000042C05C		ReadConsoleW	KERNEL32
000000000042C060		SetFilePointerEx	KERNEL32
000000000042C064		CreateDirectoryA	KERNEL32
000000000042C068		CreateFileA	KERNEL32
000000000042C06C		DeleteFileA	KERNEL32
000000000042C070		GetFileSize	KERNEL32
000000000042C074		QueryDosDeviceW	KERNEL32
000000000042C078		ReadFile	KERNEL32
000000000042C07C		WriteFile	KERNEL32
000000000042C080		CloseHandle	KERNEL32
000000000042C084		Sleep	KERNEL32

Line 96 of 108

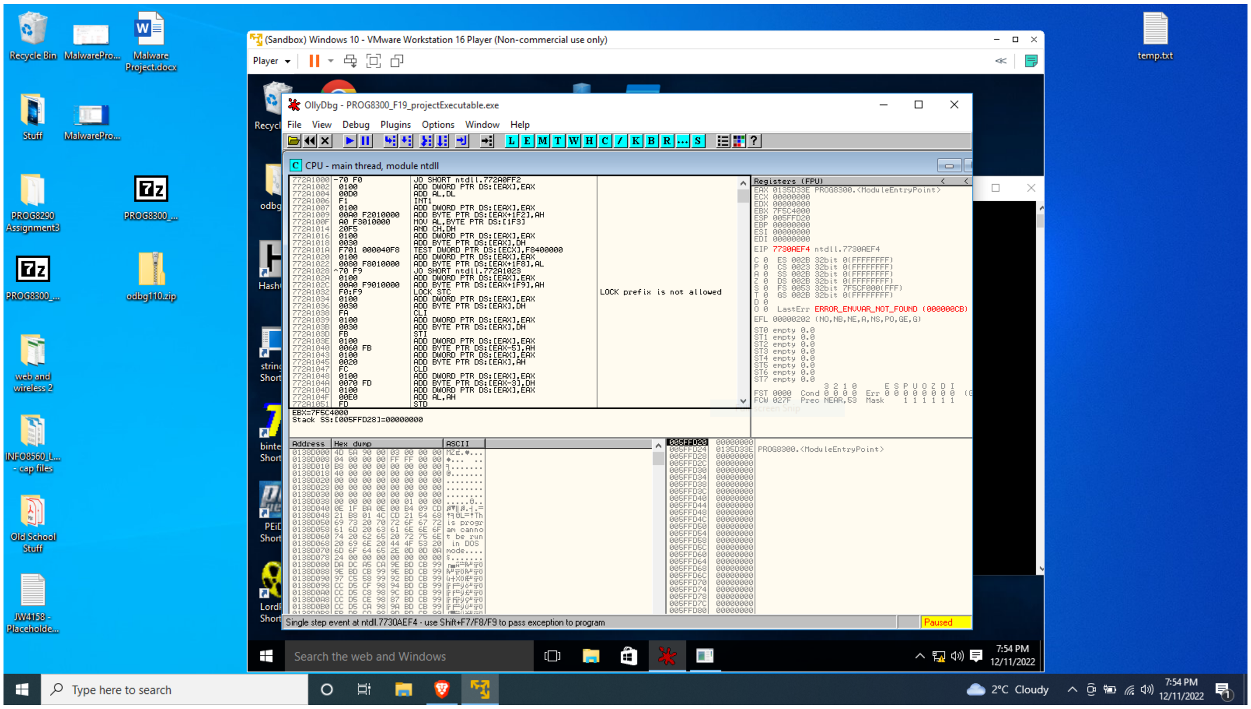
```
Using FLIRT signature: SEH for vc7-14
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished.
```

```
AU:  idle   Down   Disk: 42GB
```

11:16 PM 12/11/2022

11:16 PM 12/11/2022

Figure 3 – IDA analysis (imports)



(Sandbox) Windows 10 - VMware Workstation 16 Player (Non-commercial use only)

OllyDbg - PROG8300_F19_projectExecutable.exe

CPU - main thread, module ntdll

```
772A1000 -70 F0            JO SHORT ntdll.772A0FF2
772A1002  0100             ADD DWORD PTR DS:[EAX],EAX
772A1004  00D0             ADD AL,DL
772A1006  F1               INT1
772A1007  0100             ADD DWORD PTR DS:[EAX],EAX
772A1009  00A0 F2010000    ADD BYTE PTR DS:[EAX+1F2],AH
772A100F  A0 F3010000      MOV AL,BYTE PTR DS:[1F3]
772A1014  20F5             AND CH,DH
772A1016  0100             ADD DWORD PTR DS:[EAX],EAX
772A1018  0030             ADD BYTE PTR DS:[EAX],DH
772A101A  F701 000040F8    TEST DWORD PTR DS:[ECX],F8400000
772A1020  0100             ADD DWORD PTR DS:[EAX],EAX
772A1022  0080 F8010000    ADD BYTE PTR DS:[EAX+1F8],AL
772A1028 ^70 F9            JO SHORT ntdll.772A1023
772A102A  0100             ADD DWORD PTR DS:[EAX],EAX
772A102C  00A0 F9010000    ADD BYTE PTR DS:[EAX+1F9],AH
772A1032  F0:F9            LOCK STC                             LOCK prefix is not allowed
772A1034  0100             ADD DWORD PTR DS:[EAX],EAX
772A1036  0030             ADD BYTE PTR DS:[EAX],DH
772A1038  FA               CLI
772A1039  0100             ADD DWORD PTR DS:[EAX],EAX
772A103B  0030             ADD BYTE PTR DS:[EAX],DH
772A103D  FB               STI
772A103E  0100             ADD DWORD PTR DS:[EAX],EAX
772A1040  0060 FB          ADD BYTE PTR DS:[EAX-5],AH
772A1043  0100             ADD DWORD PTR DS:[EAX],EAX
772A1045  0020             ADD BYTE PTR DS:[EAX],AH
772A1047  FC               CLD
772A1048  0100             ADD DWORD PTR DS:[EAX],EAX
772A104A  0070 FD          ADD BYTE PTR DS:[EAX-3],DH
772A104D  0100             ADD DWORD PTR DS:[EAX],EAX
772A104F  00E0             ADD AL,AH
772A1051  FD               STD
EBX=7F5C4000
Stack SS:[005FFD28]=00000000
```

```
Registers (FPU)
EAX 0135D33E PROG8300.<ModuleEntryPoint>
ECX 00000000
EDX 00000000
EBX 7F5C4000
ESP 005FFD20
EBP 00000000
ESI 00000000
EDI 00000000
EIP 7730AEF4 ntdll.7730AEF4
C 0  ES 002B 32bit 0(FFFFFFFF)
P 0  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 0  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 7F5CF000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_ENVVAR_NOT_FOUND (000000CB)
EFL 00000202 (NO,NB,NE,A,NS,PO,GE,G)
ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

```
Address  Hex dump                 ASCII
0138D000 4D 5A 90 00 03 00 00 00  MZÉ.♥...
0138D008 04 00 00 00 FF FF 00 00  ♦...  ..
0138D010 B8 00 00 00 00 00 00 00  ╕.......
0138D018 40 00 00 00 00 00 00 00  @.......
0138D020 00 00 00 00 00 00 00 00  ........
0138D028 00 00 00 00 00 00 00 00  ........
0138D030 00 00 00 00 00 00 00 00  ........
0138D038 00 00 00 00 00 01 00 00  ......☺..
0138D040 0E 1F BA 0E 00 B4 09 CD  ♫▼║♫.┤.═
0138D048 21 B8 01 4C CD 21 54 68  !╕☺L═!Th
0138D050 69 73 20 70 72 6F 67 72  is progr
0138D058 61 6D 20 63 61 6E 6E 6F  am canno
0138D060 74 20 62 65 20 72 75 6E  t be run
0138D068 20 69 6E 20 44 4F 53 20   in DOS
0138D070 6D 6F 64 65 2E 0D 0D 0A  mode....
0138D078 24 00 00 00 00 00 00 00  $.......
0138D080 DA DC A5 CA 9E BD CB 99  ┌▄Ñ╩₧╜╦Ö
0138D088 9E BD CB 99 9E BD CB 99  ₧╜╦Ö₧╜╦Ö
0138D090 97 C5 58 99 92 BD CB 99  ù┼XÖÆ╜╦Ö
0138D098 CC D5 CF 98 94 BD CB 99  ╠╒╧ÿö╜╦Ö
0138D0A0 CC D5 C8 98 9C BD CB 99  ╠╒╚ÿ£╜╦Ö
0138D0A8 CC D5 CE 98 87 BD CB 99  ╠╒╬ÿç╜╦Ö
0138D0B0 CC D5 CA 98 9A BD CB 99  ╠╒╩ÿÜ╜╦Ö
```

```
005FFD20  00000000
005FFD24  0135D33E  PROG8300.<ModuleEntryPoint>
005FFD28  00000000
005FFD2C  00000000
005FFD30  00000000
005FFD34  00000000
005FFD38  00000000
005FFD3C  00000000
005FFD40  00000000
005FFD44  00000000
005FFD48  00000000
005FFD4C  00000000
005FFD50  00000000
005FFD54  00000000
005FFD58  00000000
005FFD5C  00000000
005FFD60  00000000
005FFD64  00000000
005FFD68  00000000
005FFD6C  00000000
005FFD70  00000000
005FFD74  00000000
005FFD78  00000000
005FFD7C  00000000
005FFD80  00000000
```

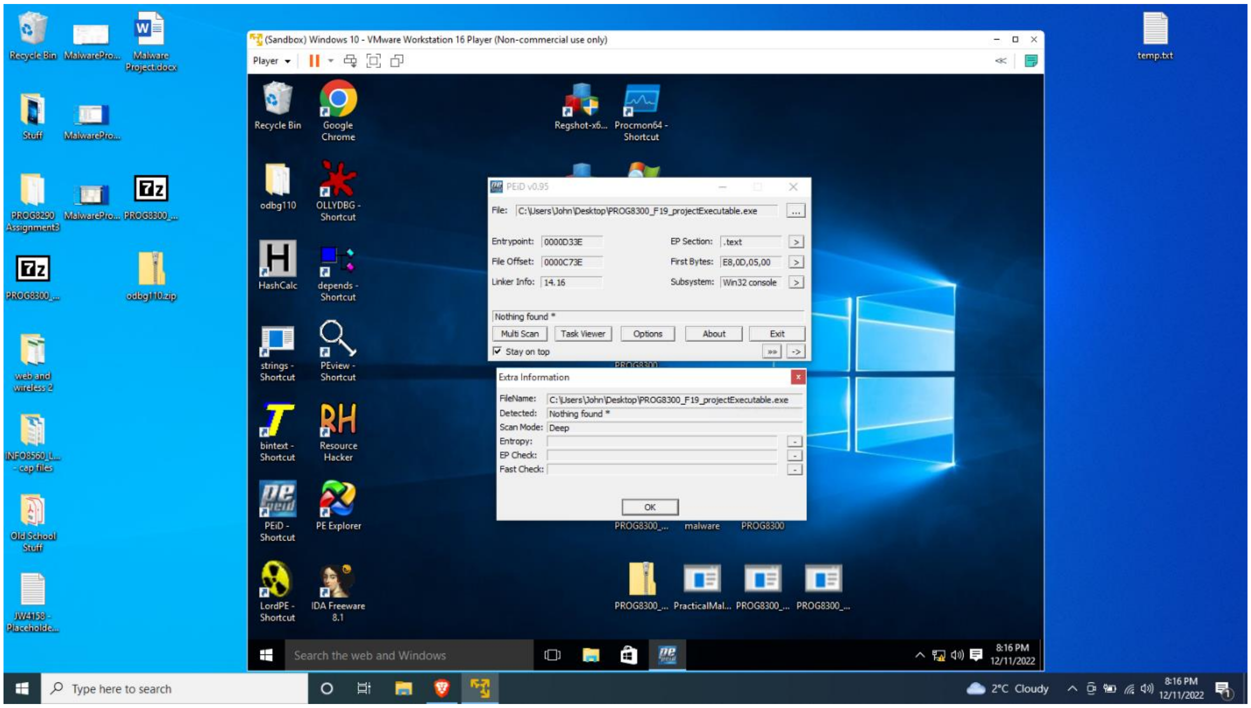
Single step event at ntdll.7730AEF4 - use Shift+F7/F8/F9 to pass exception to program

Paused

7:54 PM 12/11/2022

7:54 PM 12/11/2022

Figure 4 – OllyDBG analysis


(Sandbox) Windows 10 - VMware Workstation 16 Player (Non-commercial use only)
PEiD v0.95
Multi Scan
Task Viewer
Options
About
Exit
Extra Information
OK

File: C:\Users\John\Desktop\PROG8300_F19_projectExecutable.exe

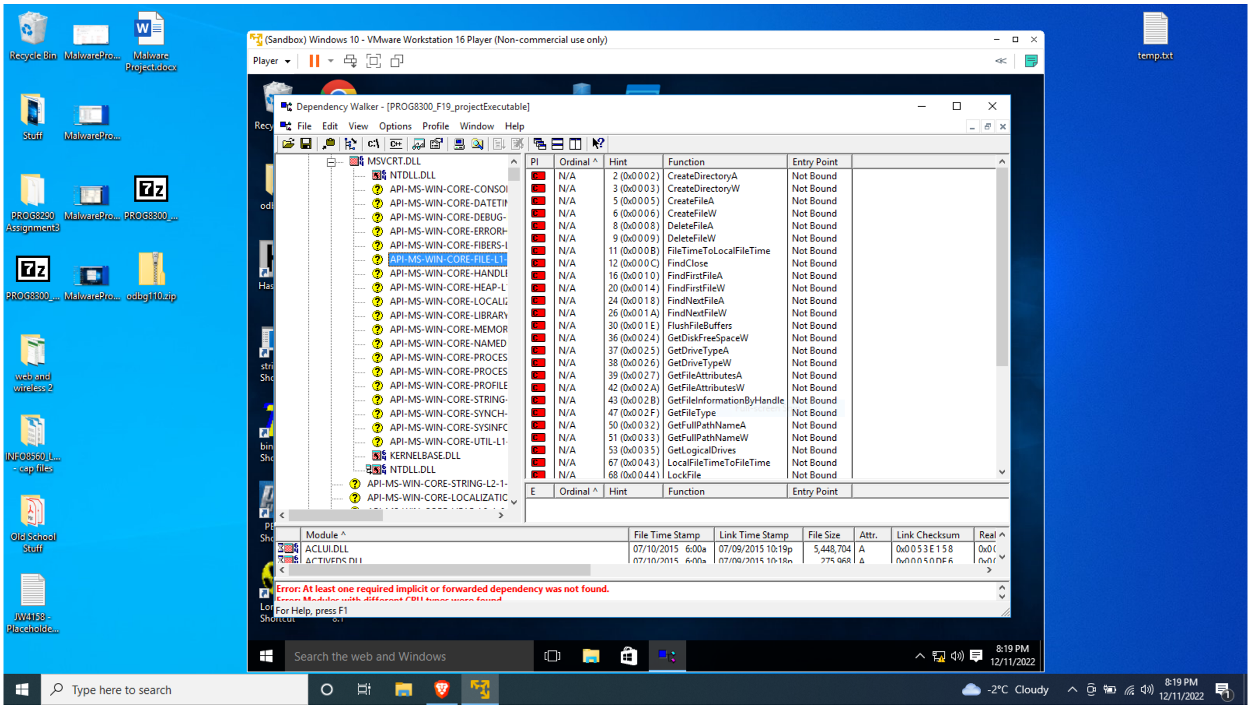
Entrypoint: 0000D33E
EP Section: .text
File Offset: 0000C73E
First Bytes: E8,0D,05,00
Linker Info: 14.16
Subsystem: Win32 console

Nothing found *

☑ Stay on top

FileName: C:\Users\John\Desktop\PROG8300_F19_projectExecutable.exe
Detected: Nothing found *
Scan Mode: Deep
Entropy:
EP Check:
Fast Check:

Figure 5 – PEiD analysis


(Sandbox) Windows 10 - VMware Workstation 16 Player (Non-commercial use only)
Dependency Walker - [PROG8300_F19_projectExecutable]
File
Edit
View
Options
Profile
Window
Help

```
MSVCRT.DLL
    NTDLL.DLL
    API-MS-WIN-CORE-CONSOI
    API-MS-WIN-CORE-DATETII
    API-MS-WIN-CORE-DEBUG-
    API-MS-WIN-CORE-ERRORH
    API-MS-WIN-CORE-FIBERS-L
    API-MS-WIN-CORE-FILE-L1-
    API-MS-WIN-CORE-HANDLE
    API-MS-WIN-CORE-HEAP-L
    API-MS-WIN-CORE-LOCALIZ
    API-MS-WIN-CORE-LIBRARY
    API-MS-WIN-CORE-MEMOR
    API-MS-WIN-CORE-NAMED
    API-MS-WIN-CORE-PROCES
    API-MS-WIN-CORE-PROCES
    API-MS-WIN-CORE-PROFILE
    API-MS-WIN-CORE-STRING-
    API-MS-WIN-CORE-SYNCH-
    API-MS-WIN-CORE-SYSINFC
    API-MS-WIN-CORE-UTIL-L1-
    KERNELBASE.DLL
    NTDLL.DLL
API-MS-WIN-CORE-STRING-L2-1-
API-MS-WIN-CORE-LOCALIZATIC
```

PI	Ordinal ^	Hint	Function	Entry Point
C	N/A	2 (0x0002)	CreateDirectoryA	Not Bound
C	N/A	3 (0x0003)	CreateDirectoryW	Not Bound
C	N/A	5 (0x0005)	CreateFileA	Not Bound
C	N/A	6 (0x0006)	CreateFileW	Not Bound
C	N/A	8 (0x0008)	DeleteFileA	Not Bound
C	N/A	9 (0x0009)	DeleteFileW	Not Bound
C	N/A	11 (0x000B)	FileTimeToLocalFileTime	Not Bound
C	N/A	12 (0x000C)	FindClose	Not Bound
C	N/A	16 (0x0010)	FindFirstFileA	Not Bound
C	N/A	20 (0x0014)	FindFirstFileW	Not Bound
C	N/A	24 (0x0018)	FindNextFileA	Not Bound
C	N/A	26 (0x001A)	FindNextFileW	Not Bound
C	N/A	30 (0x001E)	FlushFileBuffers	Not Bound
C	N/A	36 (0x0024)	GetDiskFreeSpaceW	Not Bound
C	N/A	37 (0x0025)	GetDriveTypeA	Not Bound
C	N/A	38 (0x0026)	GetDriveTypeW	Not Bound
C	N/A	39 (0x0027)	GetFileAttributesA	Not Bound
C	N/A	42 (0x002A)	GetFileAttributesW	Not Bound
C	N/A	43 (0x002B)	GetFileInformationByHandle	Not Bound
C	N/A	47 (0x002F)	GetFileType	Not Bound
C	N/A	50 (0x0032)	GetFullPathNameA	Not Bound
C	N/A	51 (0x0033)	GetFullPathNameW	Not Bound
C	N/A	53 (0x0035)	GetLogicalDrives	Not Bound
C	N/A	67 (0x0043)	LocalFileTimeToFileTime	Not Bound
C	N/A	68 (0x0044)	LockFile	Not Bound

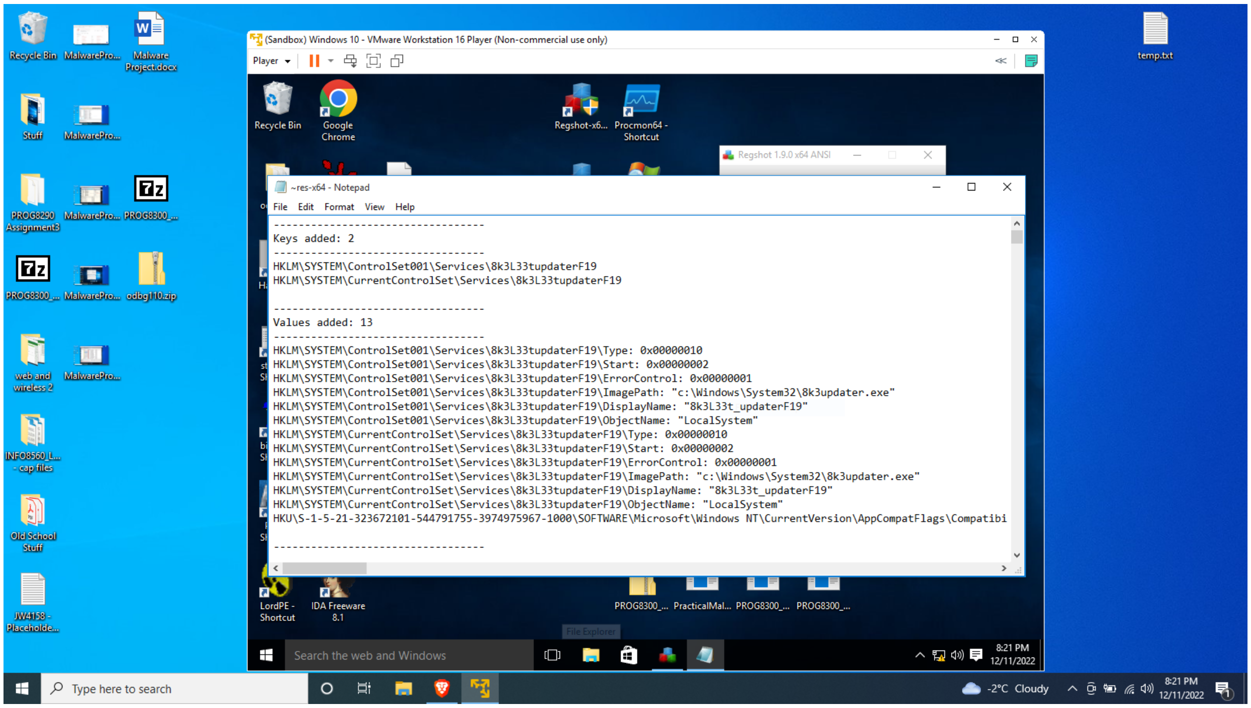
E	Ordinal ^	Hint	Function	Entry Point

Module ^	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real
ACLUI.DLL	07/10/2015 6:00a	07/09/2015 10:19p	5,448,704	A	0x0053E158	0x0(
ACTIVEDS.DLL	07/10/2015 6:00a	07/09/2015 10:18p	275,968	A	0x00050DE6	0x0(

Error: At least one required implicit or forwarded dependency was not found.
Error: Modules with different CPU types were found.

For Help, press F1

Figure 6 – Dependency Walker analysis

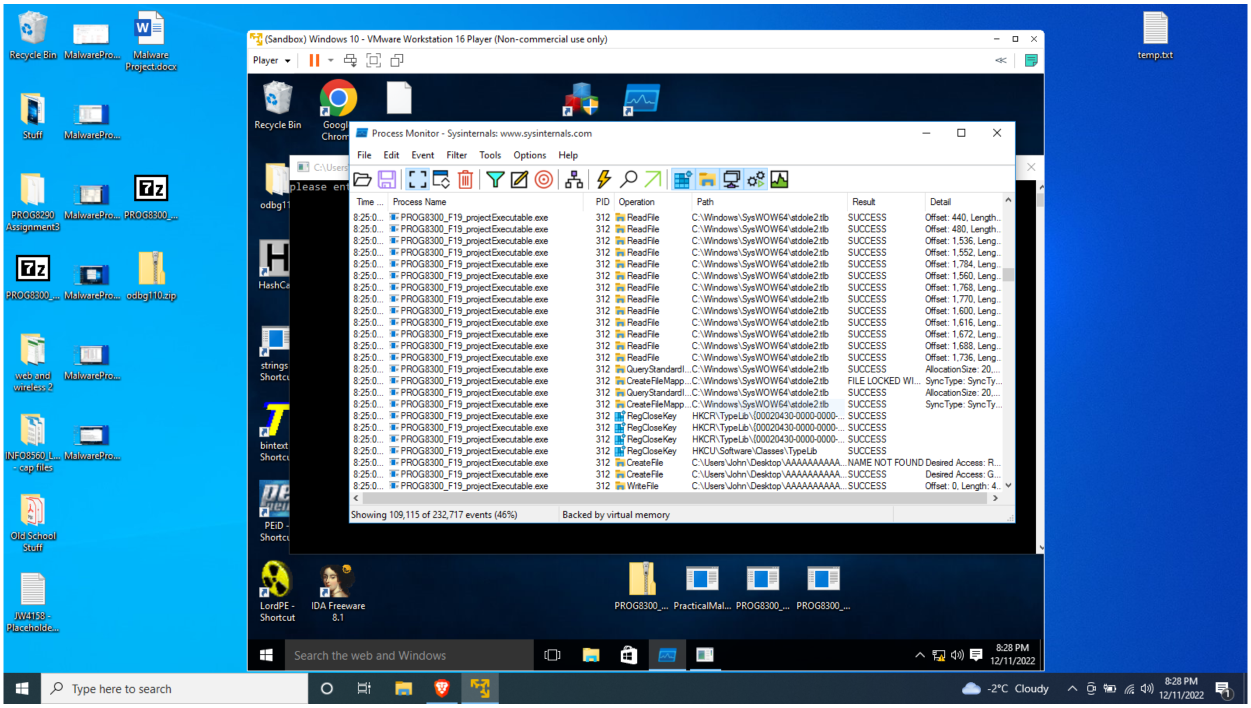

(Sandbox) Windows 10 - VMware Workstation 16 Player (Non-commercial use only)
Regshot 1.9.0 x64 ANSI
~res-x64 - Notepad
File Edit Format View Help

```
----------------------------------
Keys added: 2
----------------------------------
HKLM\SYSTEM\ControlSet001\Services\8k3L33tupdaterF19
HKLM\SYSTEM\CurrentControlSet\Services\8k3L33tupdaterF19

----------------------------------
Values added: 13
----------------------------------
HKLM\SYSTEM\ControlSet001\Services\8k3L33tupdaterF19\Type: 0x00000010
HKLM\SYSTEM\ControlSet001\Services\8k3L33tupdaterF19\Start: 0x00000002
HKLM\SYSTEM\ControlSet001\Services\8k3L33tupdaterF19\ErrorControl: 0x00000001
HKLM\SYSTEM\ControlSet001\Services\8k3L33tupdaterF19\ImagePath: "c:\Windows\System32\8k3updater.exe"
HKLM\SYSTEM\ControlSet001\Services\8k3L33tupdaterF19\DisplayName: "8k3L33t_updaterF19"
HKLM\SYSTEM\ControlSet001\Services\8k3L33tupdaterF19\ObjectName: "LocalSystem"
HKLM\SYSTEM\CurrentControlSet\Services\8k3L33tupdaterF19\Type: 0x00000010
HKLM\SYSTEM\CurrentControlSet\Services\8k3L33tupdaterF19\Start: 0x00000002
HKLM\SYSTEM\CurrentControlSet\Services\8k3L33tupdaterF19\ErrorControl: 0x00000001
HKLM\SYSTEM\CurrentControlSet\Services\8k3L33tupdaterF19\ImagePath: "c:\Windows\System32\8k3updater.exe"
HKLM\SYSTEM\CurrentControlSet\Services\8k3L33tupdaterF19\DisplayName: "8k3L33t_updaterF19"
HKLM\SYSTEM\CurrentControlSet\Services\8k3L33tupdaterF19\ObjectName: "LocalSystem"
HKU\S-1-5-21-323672101-544791755-3974975967-1000\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibi

----------------------------------
```

Figure 7 – Regshot analysis


(Sandbox) Windows 10 - VMware Workstation 16 Player (Non-commercial use only)
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail
8:25:0...	PROG8300_F19_projectExecutable.exe	312	ReadFile	C:\Windows\SysWOW64\stdole2.tlb	SUCCESS	Offset: 440, Length...
8:25:0...	PROG8300_F19_projectExecutable.exe	312	ReadFile	C:\Windows\SysWOW64\stdole2.tlb	SUCCESS	Offset: 480, Length...
8:25:0...	PROG8300_F19_projectExecutable.exe	312	ReadFile	C:\Windows\SysWOW64\stdole2.tlb	SUCCESS	Offset: 1,536, Leng...
8:25:0...	PROG8300_F19_projectExecutable.exe	312	ReadFile	C:\Windows\SysWOW64\stdole2.tlb	SUCCESS	Offset: 1,552, Leng...
8:25:0...	PROG8300_F19_projectExecutable.exe	312	ReadFile	C:\Windows\SysWOW64\stdole2.tlb	SUCCESS	Offset: 1,784, Leng...
8:25:0...	PROG8300_F19_projectExecutable.exe	312	ReadFile	C:\Windows\SysWOW64\stdole2.tlb	SUCCESS	Offset: 1,560, Leng...
8:25:0...	PROG8300_F19_projectExecutable.exe	312	ReadFile	C:\Windows\SysWOW64\stdole2.tlb	SUCCESS	Offset: 1,768, Leng...
8:25:0...	PROG8300_F19_projectExecutable.exe	312	ReadFile	C:\Windows\SysWOW64\stdole2.tlb	SUCCESS	Offset: 1,770, Leng...
8:25:0...	PROG8300_F19_projectExecutable.exe	312	ReadFile	C:\Windows\SysWOW64\stdole2.tlb	SUCCESS	Offset: 1,600, Leng...
8:25:0...	PROG8300_F19_projectExecutable.exe	312	ReadFile	C:\Windows\SysWOW64\stdole2.tlb	SUCCESS	Offset: 1,616, Leng...
8:25:0...	PROG8300_F19_projectExecutable.exe	312	ReadFile	C:\Windows\SysWOW64\stdole2.tlb	SUCCESS	Offset: 1,672, Leng...
8:25:0...	PROG8300_F19_projectExecutable.exe	312	ReadFile	C:\Windows\SysWOW64\stdole2.tlb	SUCCESS	Offset: 1,688, Leng...
8:25:0...	PROG8300_F19_projectExecutable.exe	312	ReadFile	C:\Windows\SysWOW64\stdole2.tlb	SUCCESS	Offset: 1,736, Leng...
8:25:0...	PROG8300_F19_projectExecutable.exe	312	QueryStandardI...	C:\Windows\SysWOW64\stdole2.tlb	SUCCESS	AllocationSize: 20,...
8:25:0...	PROG8300_F19_projectExecutable.exe	312	CreateFileMapp...	C:\Windows\SysWOW64\stdole2.tlb	FILE LOCKED WI...	SyncType: SyncTy...
8:25:0...	PROG8300_F19_projectExecutable.exe	312	QueryStandardI...	C:\Windows\SysWOW64\stdole2.tlb	SUCCESS	AllocationSize: 20,...
8:25:0...	PROG8300_F19_projectExecutable.exe	312	CreateFileMapp...	C:\Windows\SysWOW64\stdole2.tlb	SUCCESS	SyncType: SyncTy...
8:25:0...	PROG8300_F19_projectExecutable.exe	312	RegCloseKey	HKCR\TypeLib\{00020430-0000-0000-...	SUCCESS	
8:25:0...	PROG8300_F19_projectExecutable.exe	312	RegCloseKey	HKCR\TypeLib\{00020430-0000-0000-...	SUCCESS	
8:25:0...	PROG8300_F19_projectExecutable.exe	312	RegCloseKey	HKCR\TypeLib\{00020430-0000-0000-...	SUCCESS	
8:25:0...	PROG8300_F19_projectExecutable.exe	312	RegCloseKey	HKCU\Software\Classes\TypeLib	SUCCESS	
8:25:0...	PROG8300_F19_projectExecutable.exe	312	CreateFile	C:\Users\John\Desktop\AAAAAAAAAA...	NAME NOT FOUND	Desired Access: R...
8:25:0...	PROG8300_F19_projectExecutable.exe	312	CreateFile	C:\Users\John\Desktop\AAAAAAAAAA...	SUCCESS	Desired Access: G...
8:25:0...	PROG8300_F19_projectExecutable.exe	312	WriteFile	C:\Users\John\Desktop\AAAAAAAAAA...	SUCCESS	Offset: 0, Length: 4...

Showing 109,115 of 232,717 events (46%) Backed by virtual memory

Figure 8 – Process Monitor analysis