MALWARE ANALYSIS PROJECT

AIM: Analyse the given malware and prepare a report on the same.

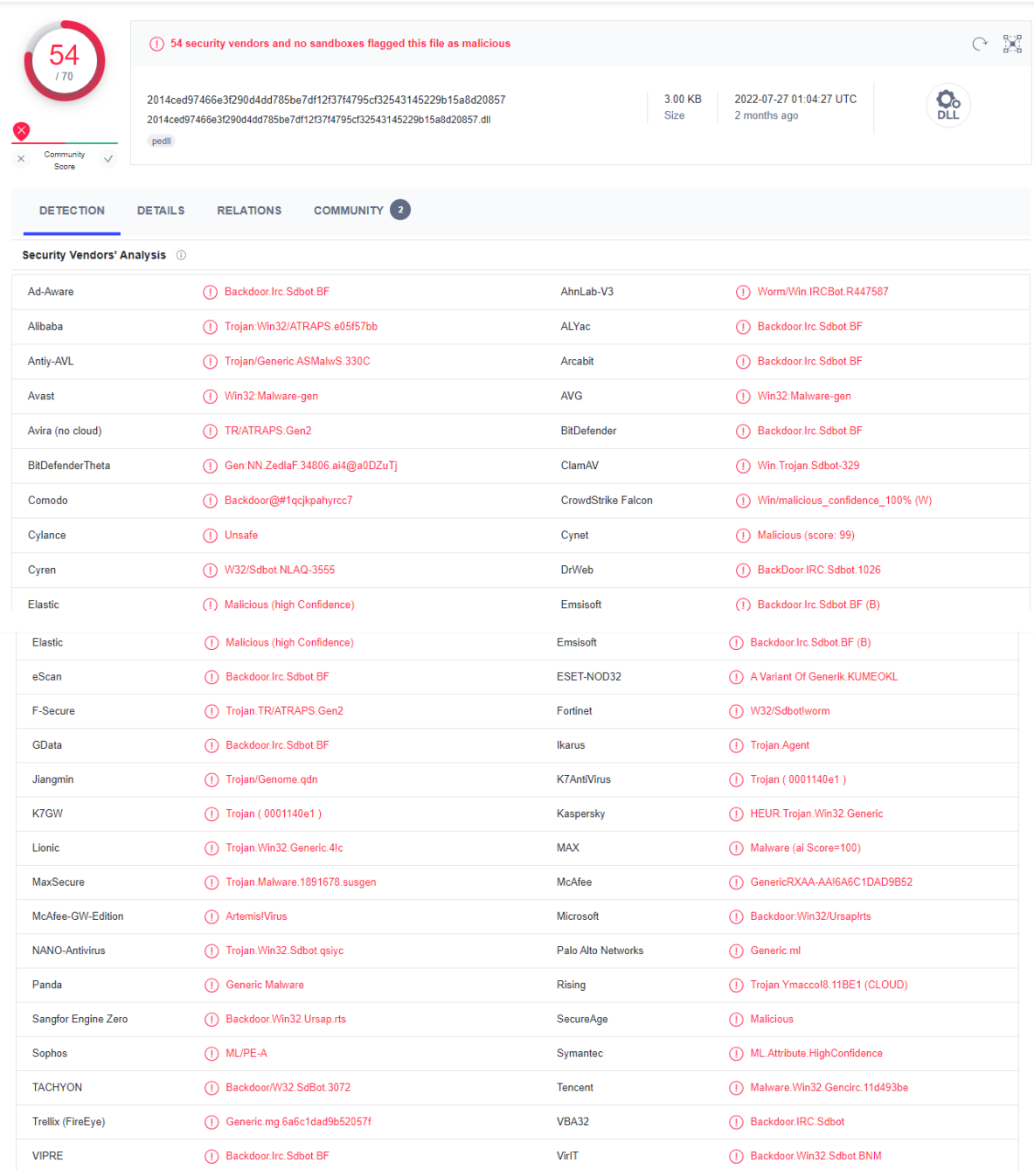
MALWARE SAMPLE: DopeBotv0.22_UnCrippled_Feb2007

Tools & Websites Used:

- Virus Total (website)
- PeStudio tool
- CFF Explorer tool
- Dependency Walker tool
- IDA Pro tool
- Process Explorer tool
- Process Monitor tool
- RegShot tool
- Hybrid Analysis (website)

Static Analysis:

Virus Total (website):



- Firstly, we are trying to fetch general information of the malware in the virus total. Here in the detection section most off the vendors have flagged this malware as backdoor.

Names

2014ced97466e3f290d4dd785be7df12f37f4795cf32543145229b15a8d20857.dll

6a6c1dad9b52057f815b9d4ca5e962cb_hook.dll

6a6c1dad9b52057f815b9d4ca5e962cb.dll

hook.dll

6a6c1dad9b52057f815b9d4ca5e962cb.vir

6A6C1DAD9B52057F815B9D4CA5E962CB

aa

vviVObsIM.dwg

pJh4hMJkFP.docx

Imports

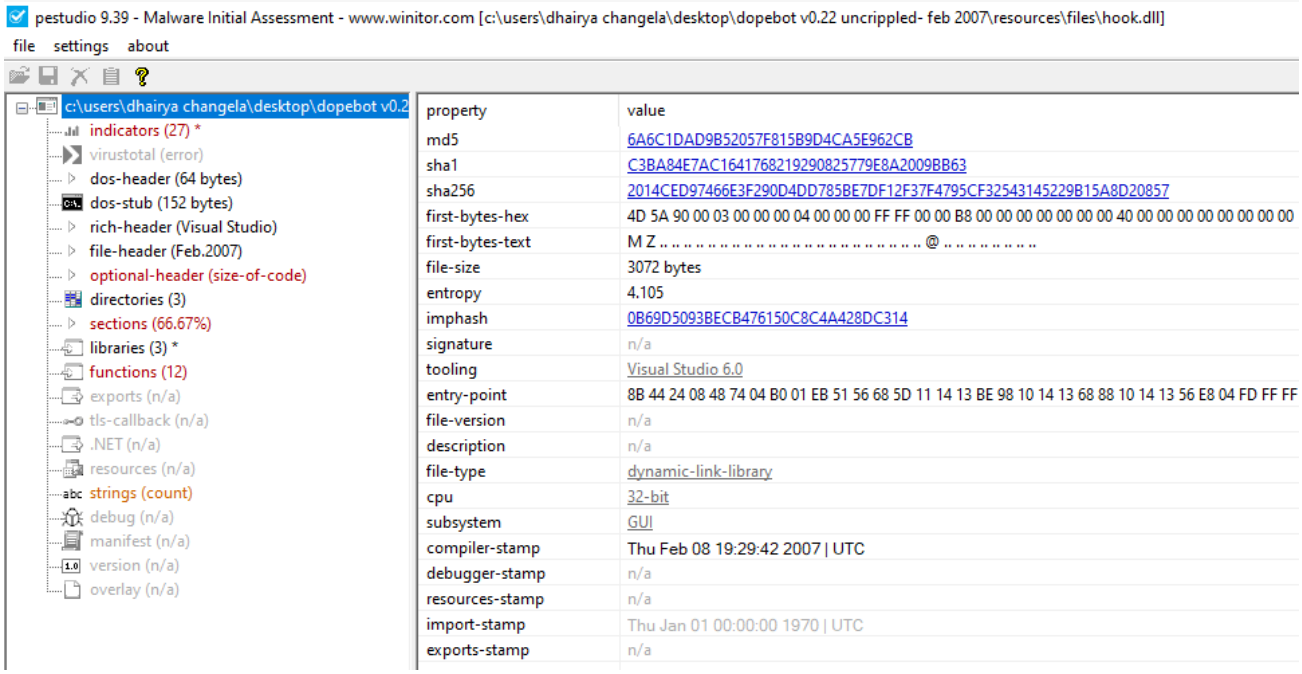
+ SHLWAPI.dll
+ KERNEL32.dll
+ MSVCRT.dll

PE Resource Parents (10)

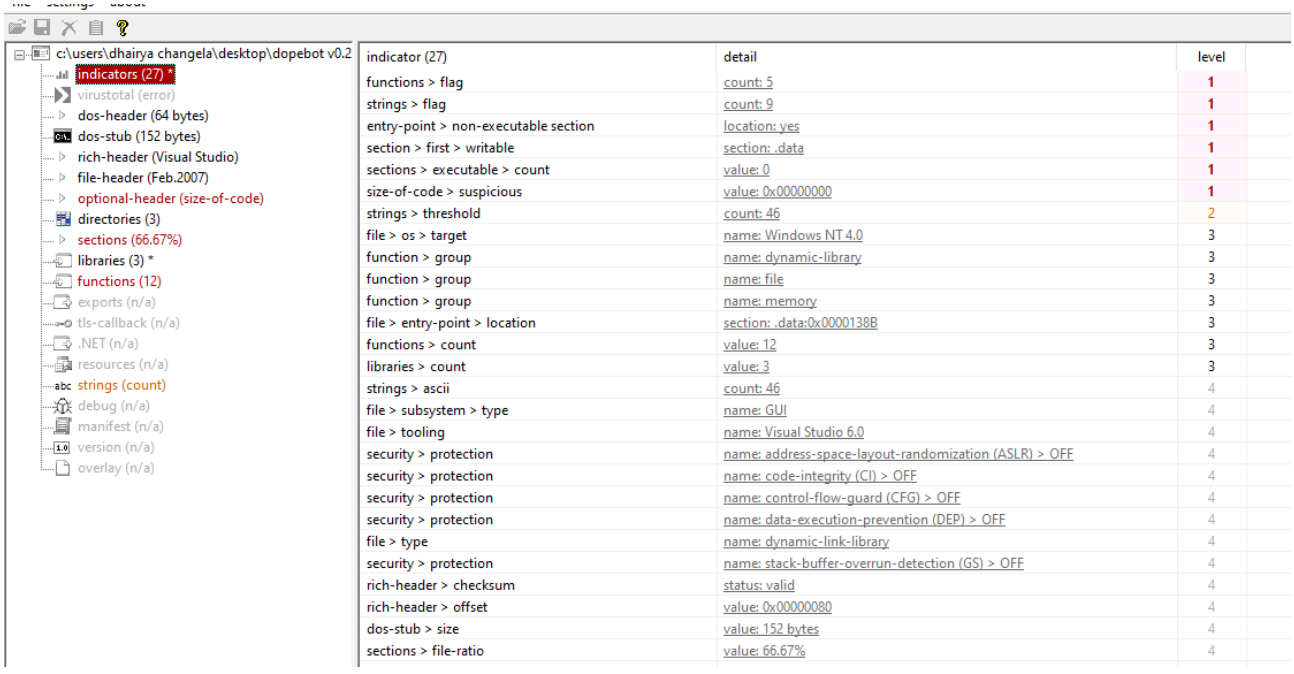
Scanned	Detections	Type	Name
2017-12-21	47 / 68	Win32 EXE	dopebot_debug.exe
2020-12-18	55 / 70	Win32 EXE	d10c1c49b63af1377f871c23c4faa5b3.virus
2013-04-23	35 / 46	Win32 EXE	VirusShare_84725461b4cbef09817a032d880be0c1
2021-01-04	51 / 70	Win32 EXE	VirusShare_02c487918b125f6ea612cca4196a86a4
2017-10-26	43 / 67	Win32 EXE	dopebot_debug.exe
2017-12-21	49 / 68	Win32 EXE	dopebot_debug.exe
2020-02-19	59 / 73	Win32 EXE	test.txt
2017-10-26	42 / 66	Win32 EXE	dopebot_debug.exe
2021-02-05	44 / 71	Win32 EXE	aa
2014-02-04	34 / 48	Win32 EXE	0e335fe3436b05d91194fdafe44def1113edc301-fdc96b777df8ec1e2eba9fdb6eada68d.01.exe1428.vir

- Additional information we've retrieved is the different names of the malware, importing dll files such as shlwapi.dll, kernale43.dll, msvcrt.dll etc.
- We also get it's relation with different malwares.

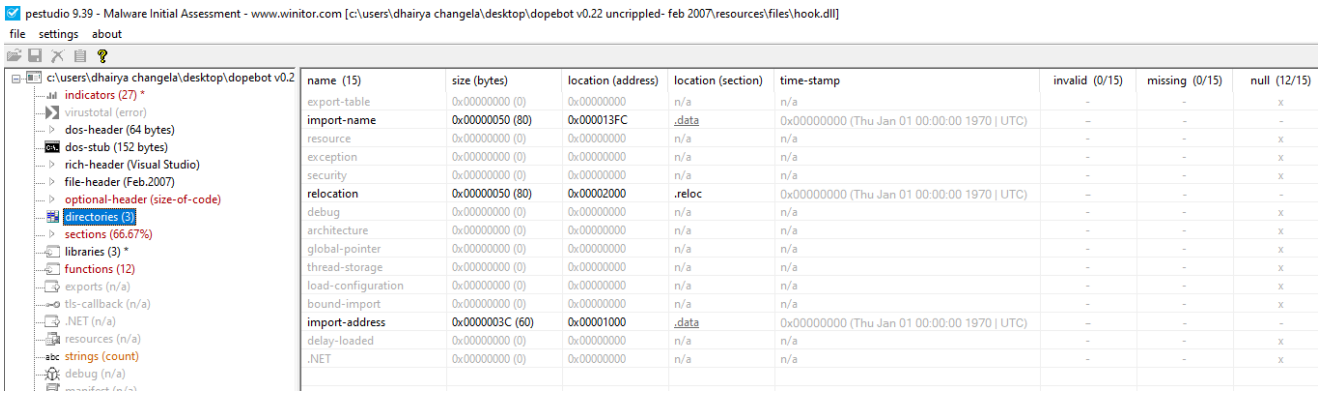
PeStudio tool:



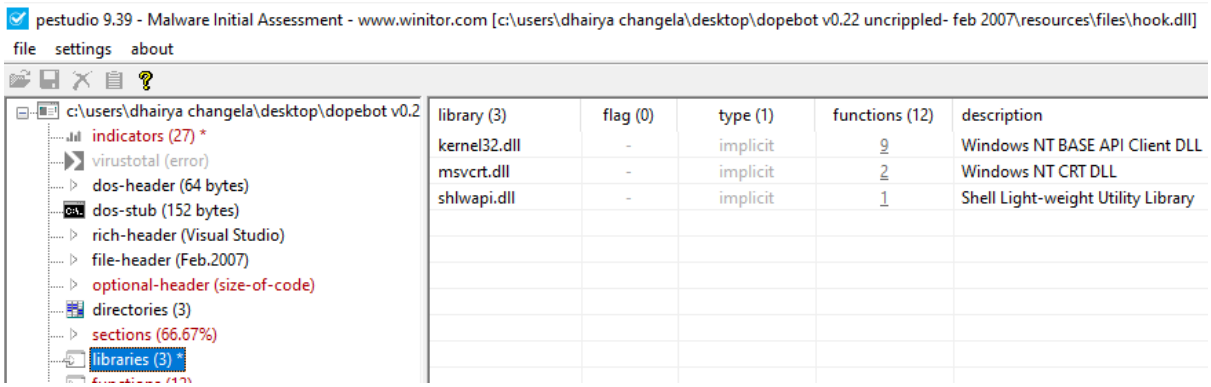
- After loading the file in Pestudio tool, we are getting general information such as md5, sha1, sha256 values, file type, subsystem etc. Also, first-byte-text is “M Z” hence we get to know that it is an executable file.

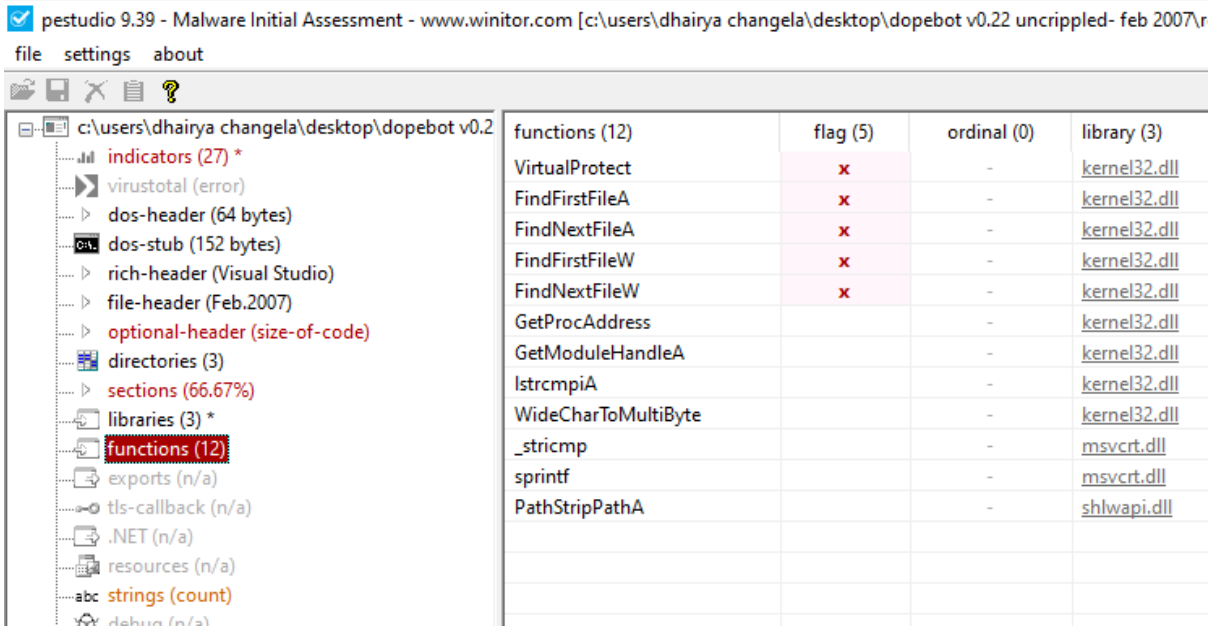


- We are getting 27 indicators as above.

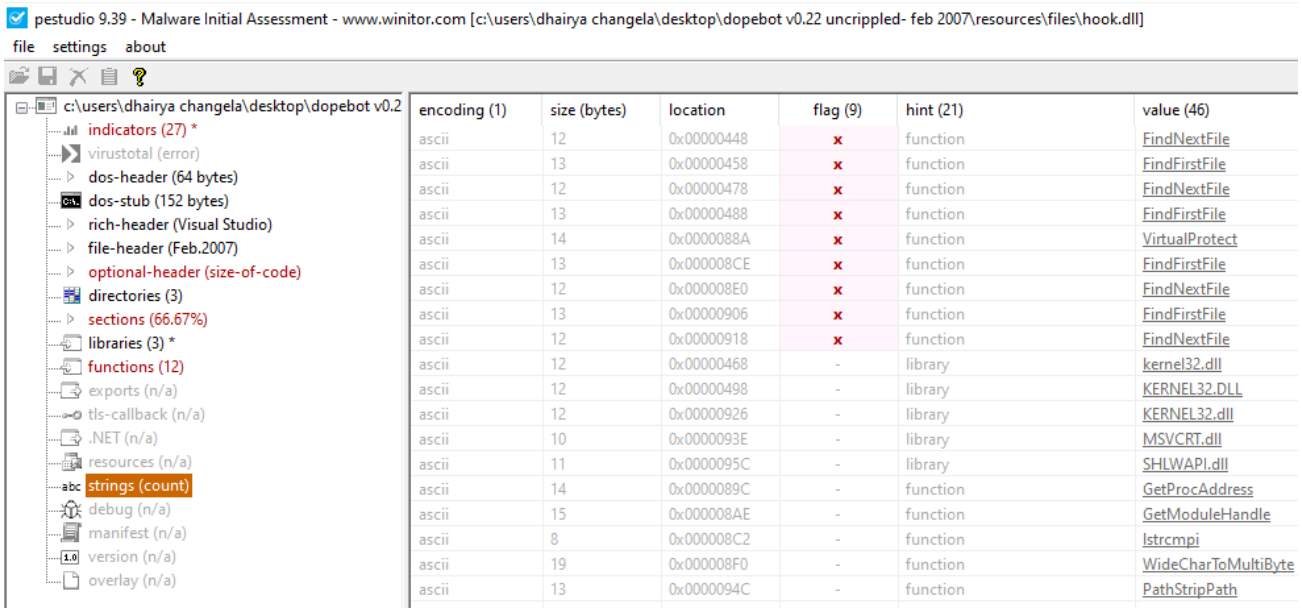


- We get 3 directories named import-name, relocation, import-address.



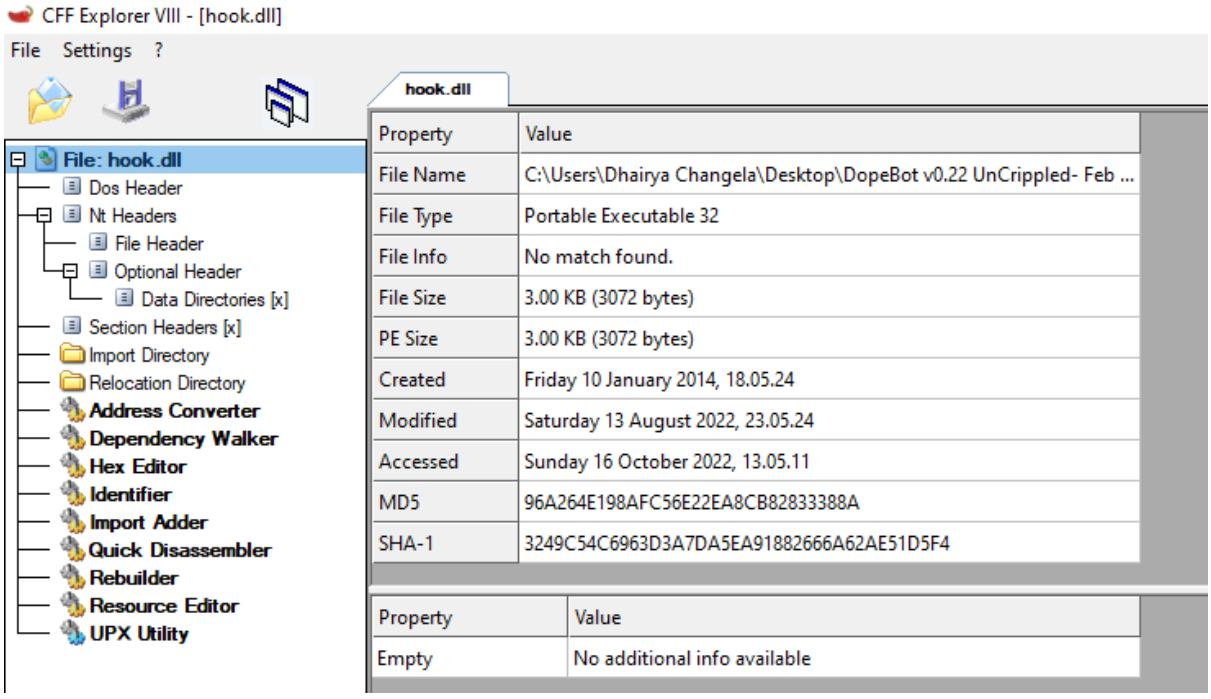


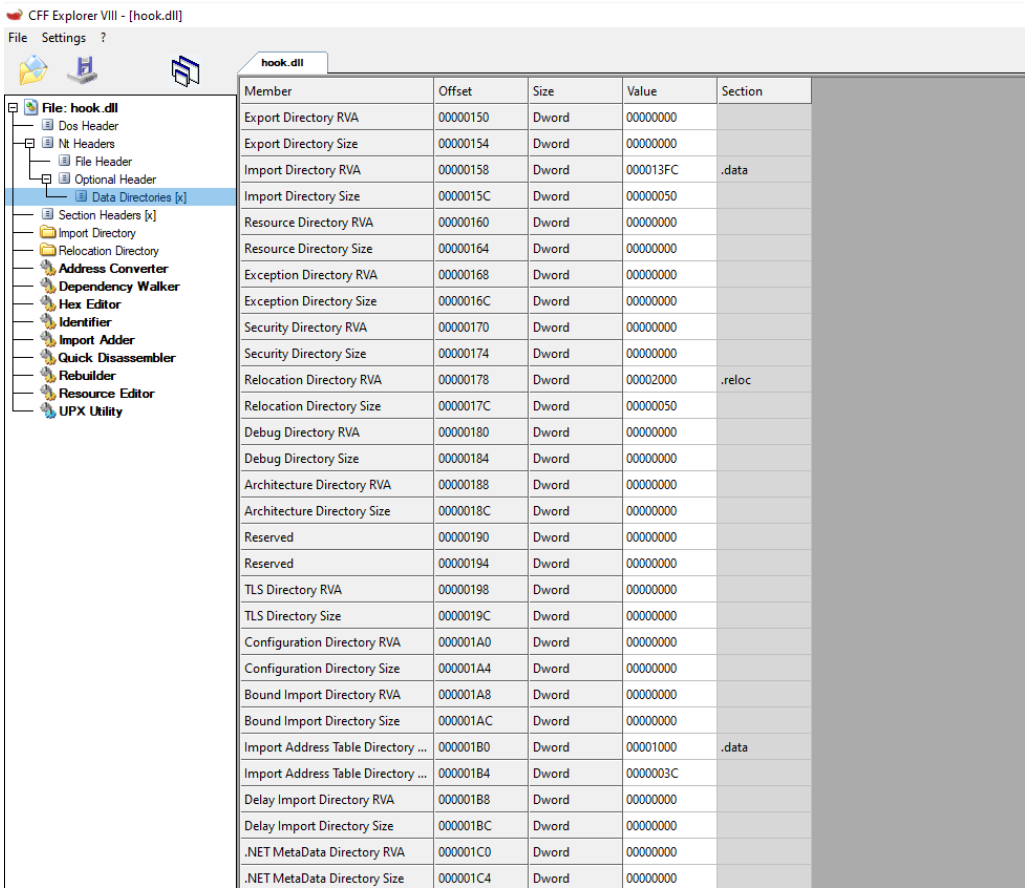
- It includes 3 libraries named kernel32.dll, msvcrt.dll, shlwapi.dll.
- Found various functions such as “VirtualProtect”, “FinadFirstFileA”, “GetProcAddress”, “GetModuleHadnleA” etc.



- We are getting various flagged strings as above.

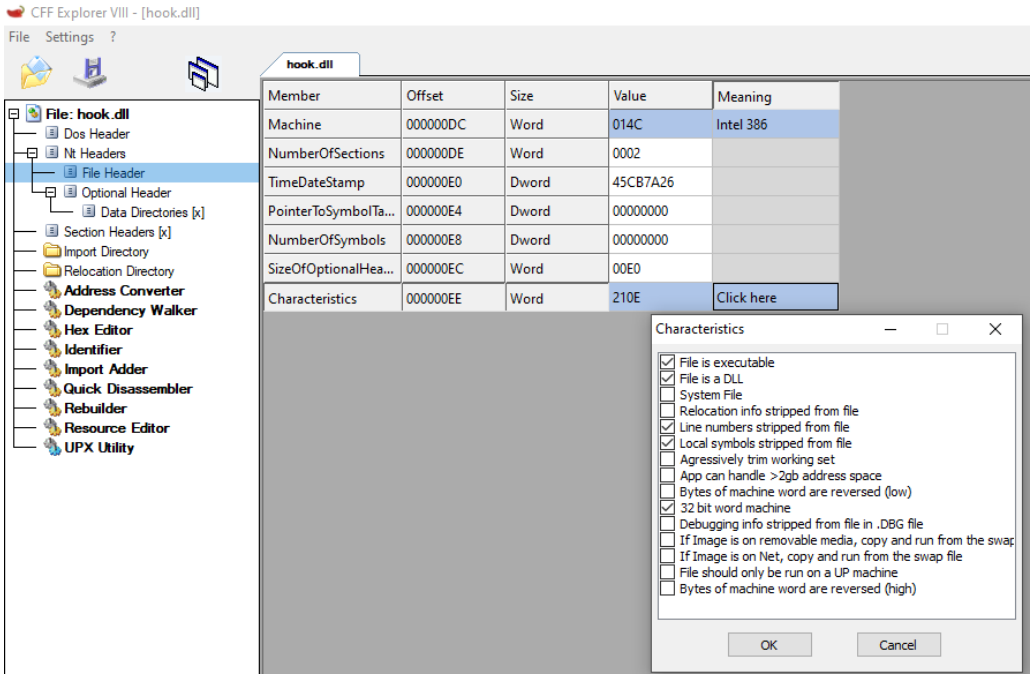
CFF Explorer tool:





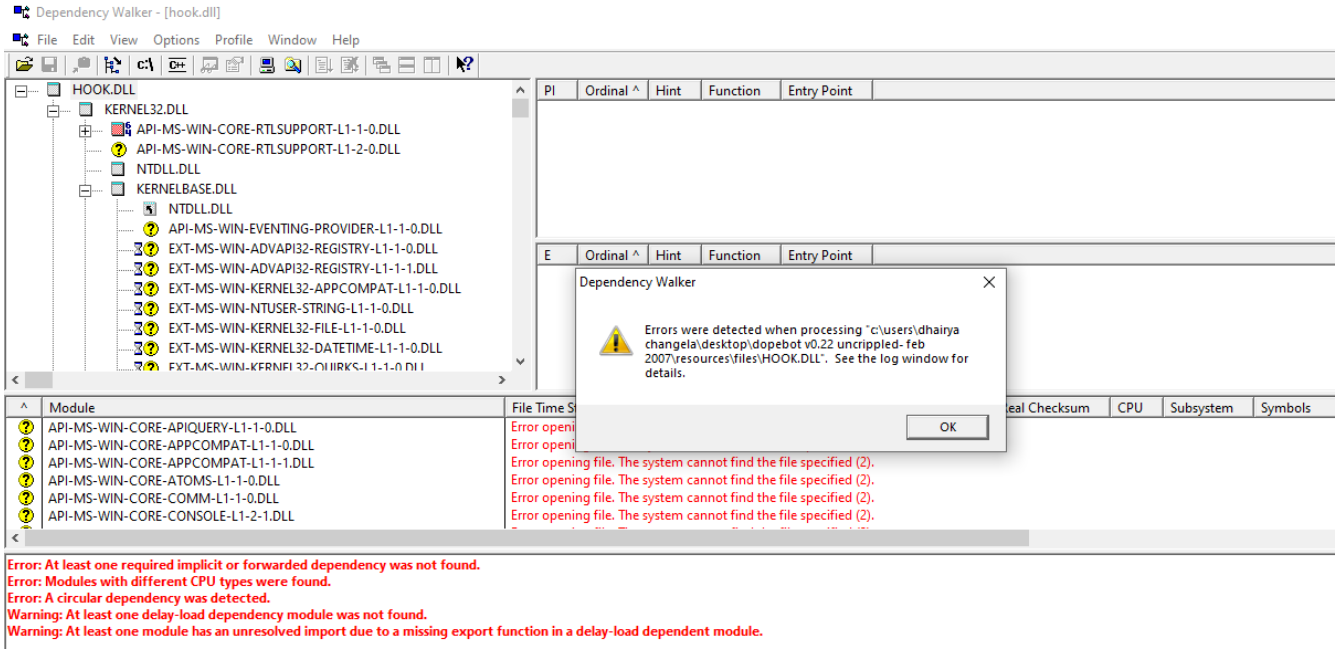
Member	Offset	Size	Value	Section
Export Directory RVA	00000150	Dword	00000000	
Export Directory Size	00000154	Dword	00000000	
Import Directory RVA	00000158	Dword	000013FC	.data
Import Directory Size	0000015C	Dword	00000050	
Resource Directory RVA	00000160	Dword	00000000	
Resource Directory Size	00000164	Dword	00000000	
Exception Directory RVA	00000168	Dword	00000000	
Exception Directory Size	0000016C	Dword	00000000	
Security Directory RVA	00000170	Dword	00000000	
Security Directory Size	00000174	Dword	00000000	
Relocation Directory RVA	00000178	Dword	00002000	.reloc
Relocation Directory Size	0000017C	Dword	00000050	
Debug Directory RVA	00000180	Dword	00000000	
Debug Directory Size	00000184	Dword	00000000	
Architecture Directory RVA	00000188	Dword	00000000	
Architecture Directory Size	0000018C	Dword	00000000	
Reserved	00000190	Dword	00000000	
Reserved	00000194	Dword	00000000	
TLS Directory RVA	00000198	Dword	00000000	
TLS Directory Size	0000019C	Dword	00000000	
Configuration Directory RVA	000001A0	Dword	00000000	
Configuration Directory Size	000001A4	Dword	00000000	
Bound Import Directory RVA	000001A8	Dword	00000000	
Bound Import Directory Size	000001AC	Dword	00000000	
Import Address Table Directory ...	000001B0	Dword	00001000	.data
Import Address Table Directory ...	000001B4	Dword	0000003C	
Delay Import Directory RVA	000001B8	Dword	00000000	
Delay Import Directory Size	000001BC	Dword	00000000	
.NET MetaData Directory RVA	000001C0	Dword	00000000	
.NET MetaData Directory Size	000001C4	Dword	00000000	

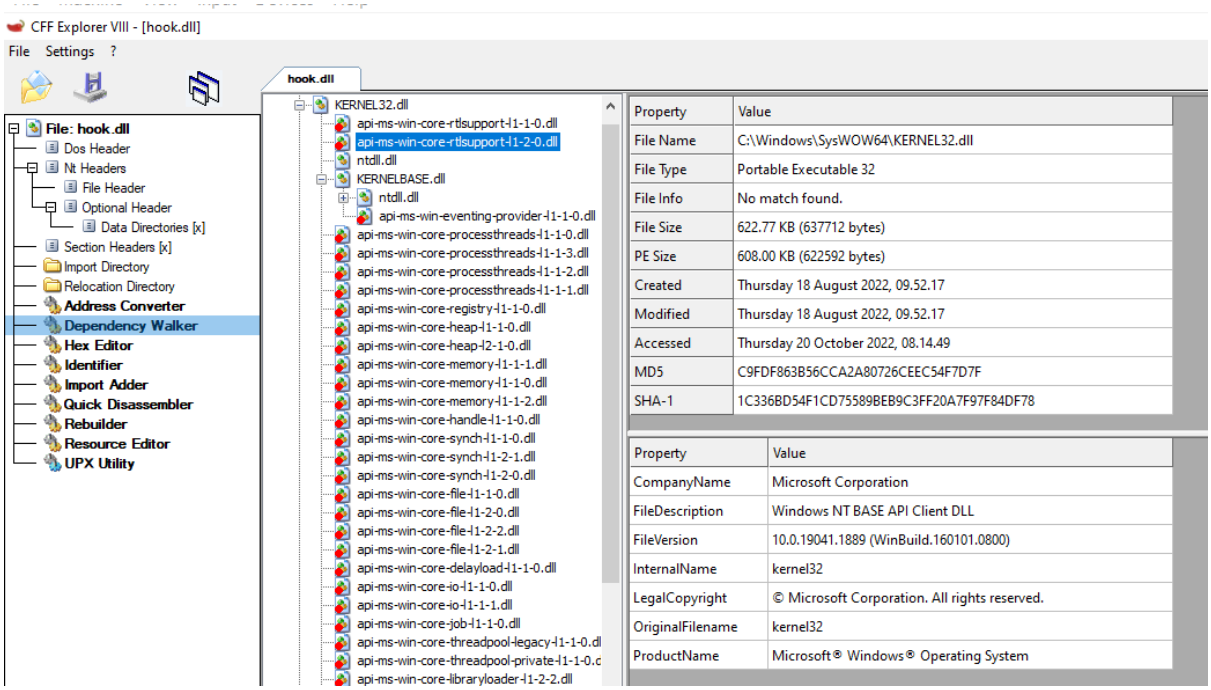
- Here we are not getting any additional information.
- But we have additional functionalities like we can check characteristics of the malware as below.



Member	Offset	Size	Value	Meaning
Machine	000000DC	Word	014C	Intel 386
NumberOfSections	000000DE	Word	0002	
TimeDateStamp	000000E0	Dword	45CB7A26	
PointerToSymbolTa...	000000E4	Dword	00000000	
NumberOfSymbols	000000E8	Dword	00000000	
SizeOfOptionalHea...	000000EC	Word	00E0	
Characteristics	000000EE	Word	210E	Click here

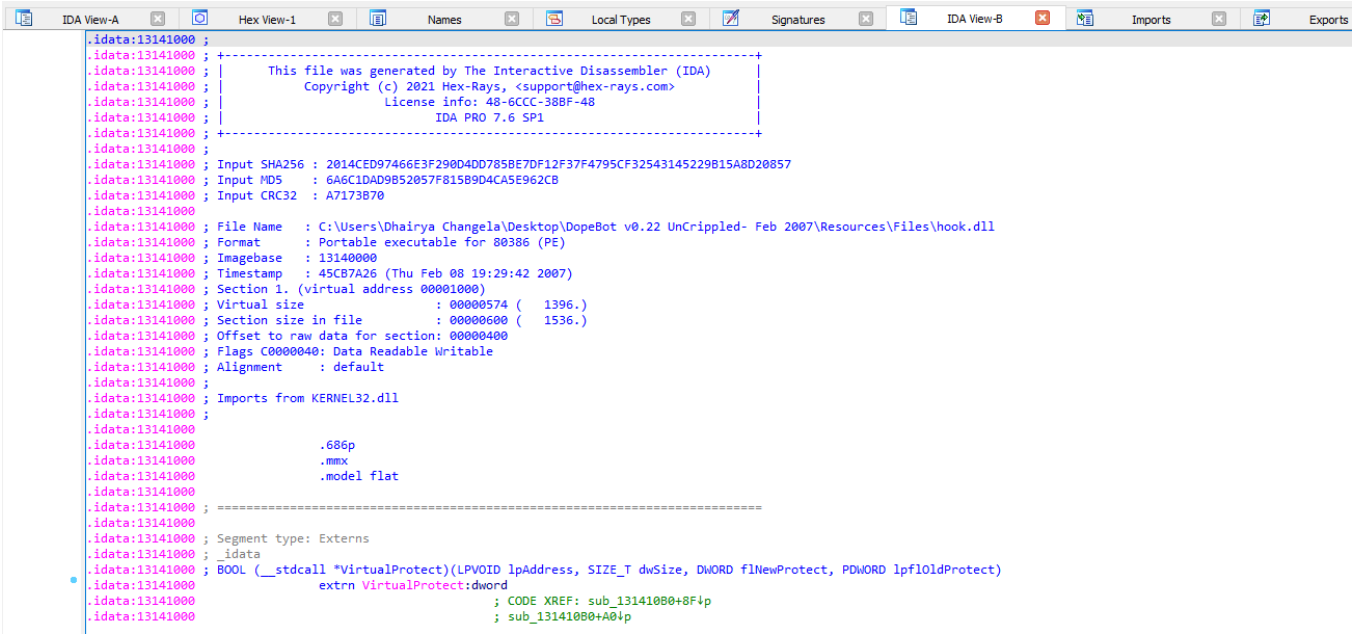
Dependency Walker tool:



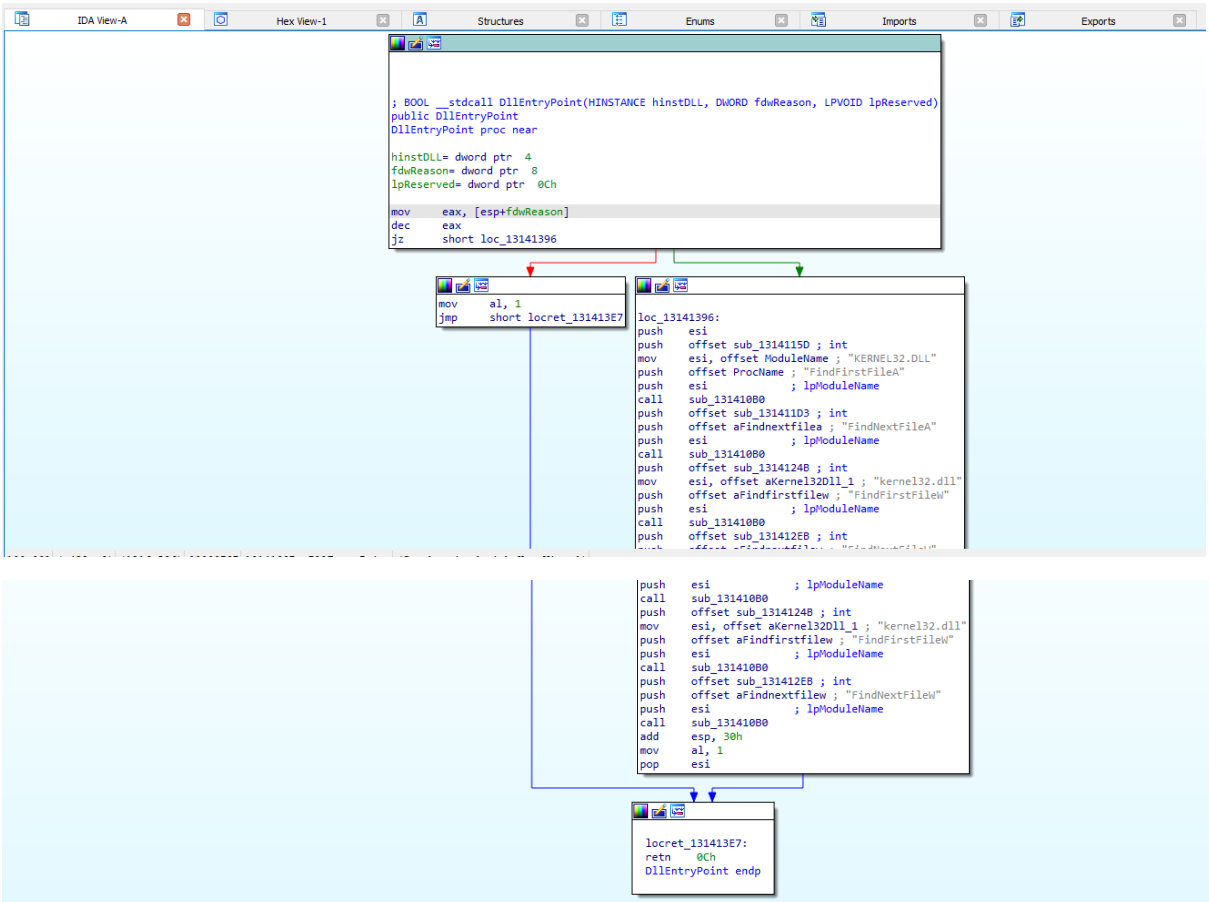


- As I was getting error while loading the file in dependency walker, I've gathered the information from cff explorer, here we can see the dependencies of the dll files.

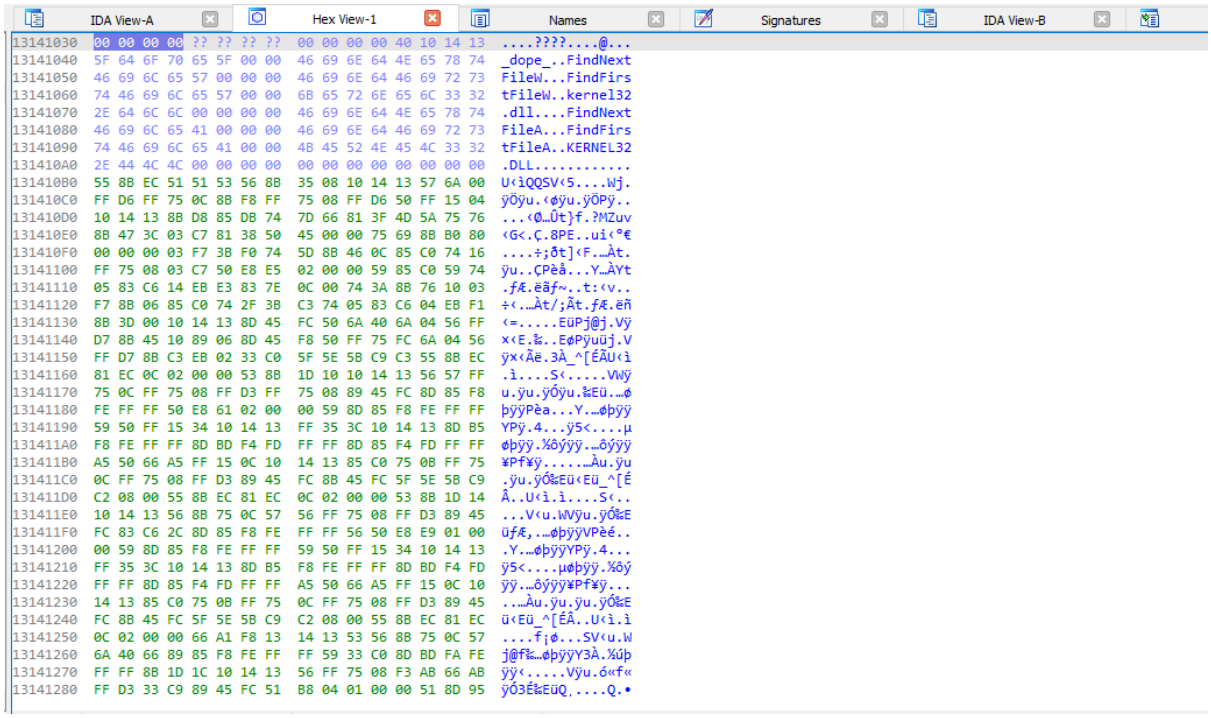
IDA Pro tool:

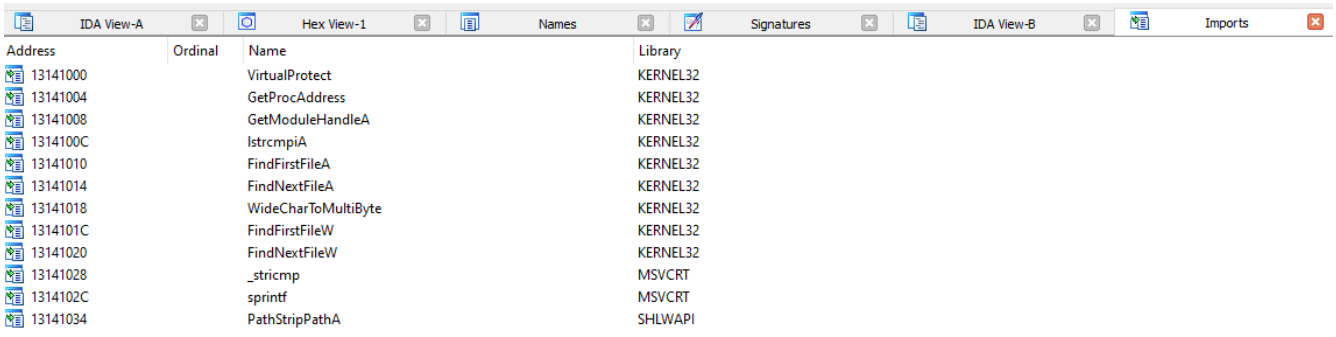


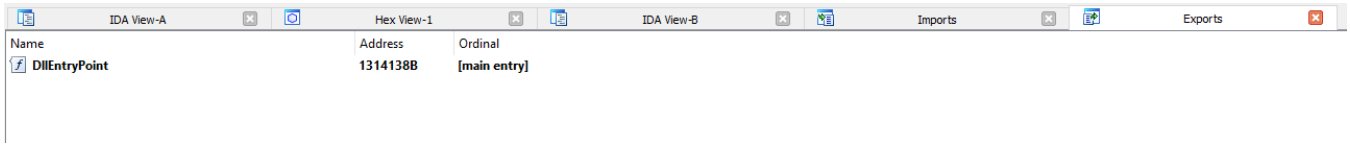
- Here we are retrieving general information including file name, format, sha, md5, crc32 hash values.



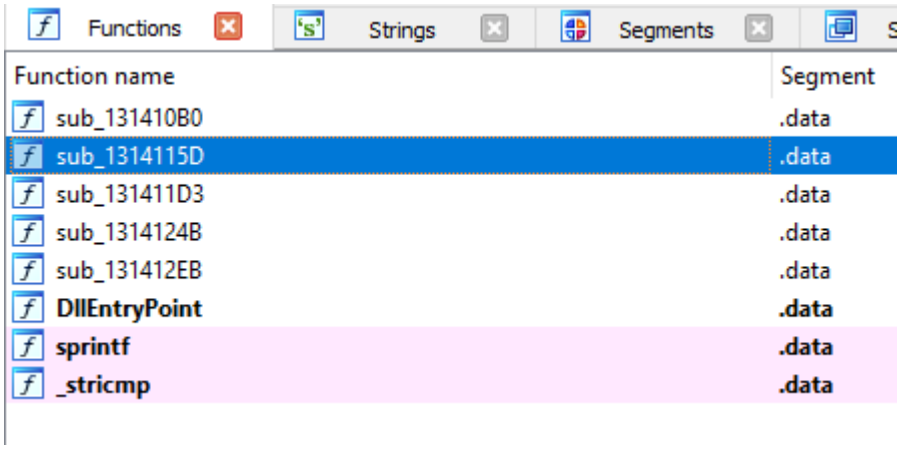
- We also get entire graph of the malware which uses different instructions.



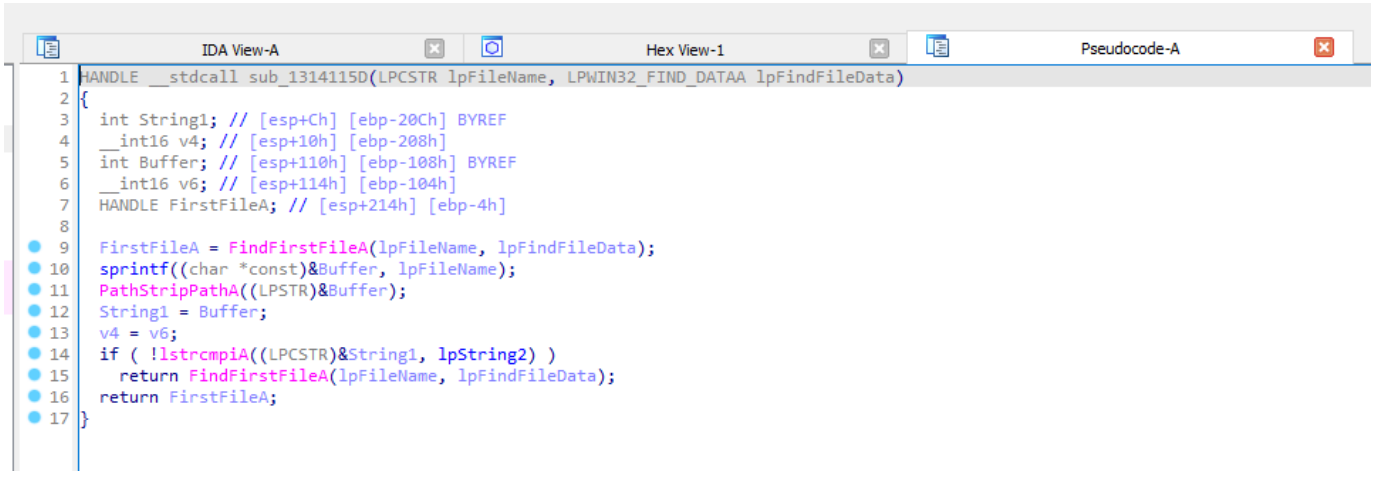


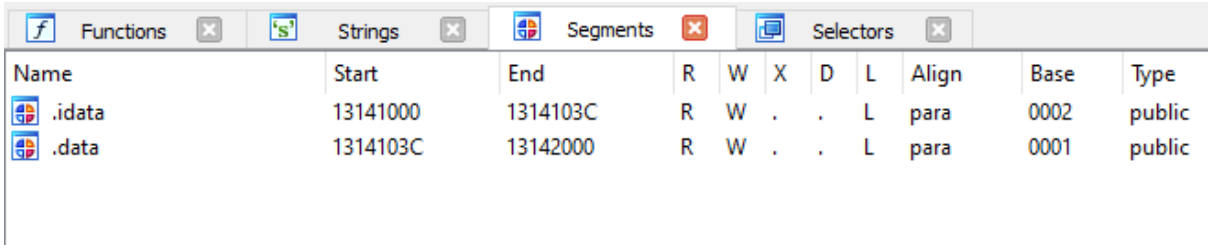


- We also get entire view of hex values, which file it is importing and which files it is exporting.

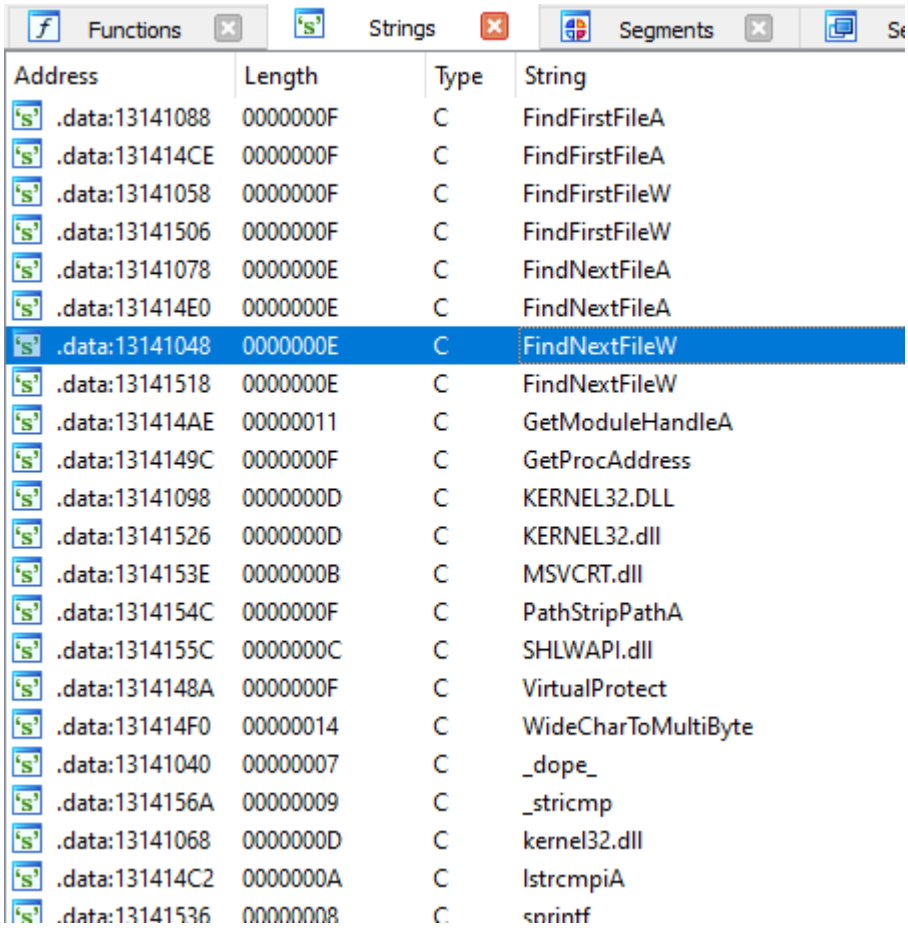


- We can see the various functions and pseudo code of any particular function as below.





- Two segments were found in the malware named “.idata” and “.data”.



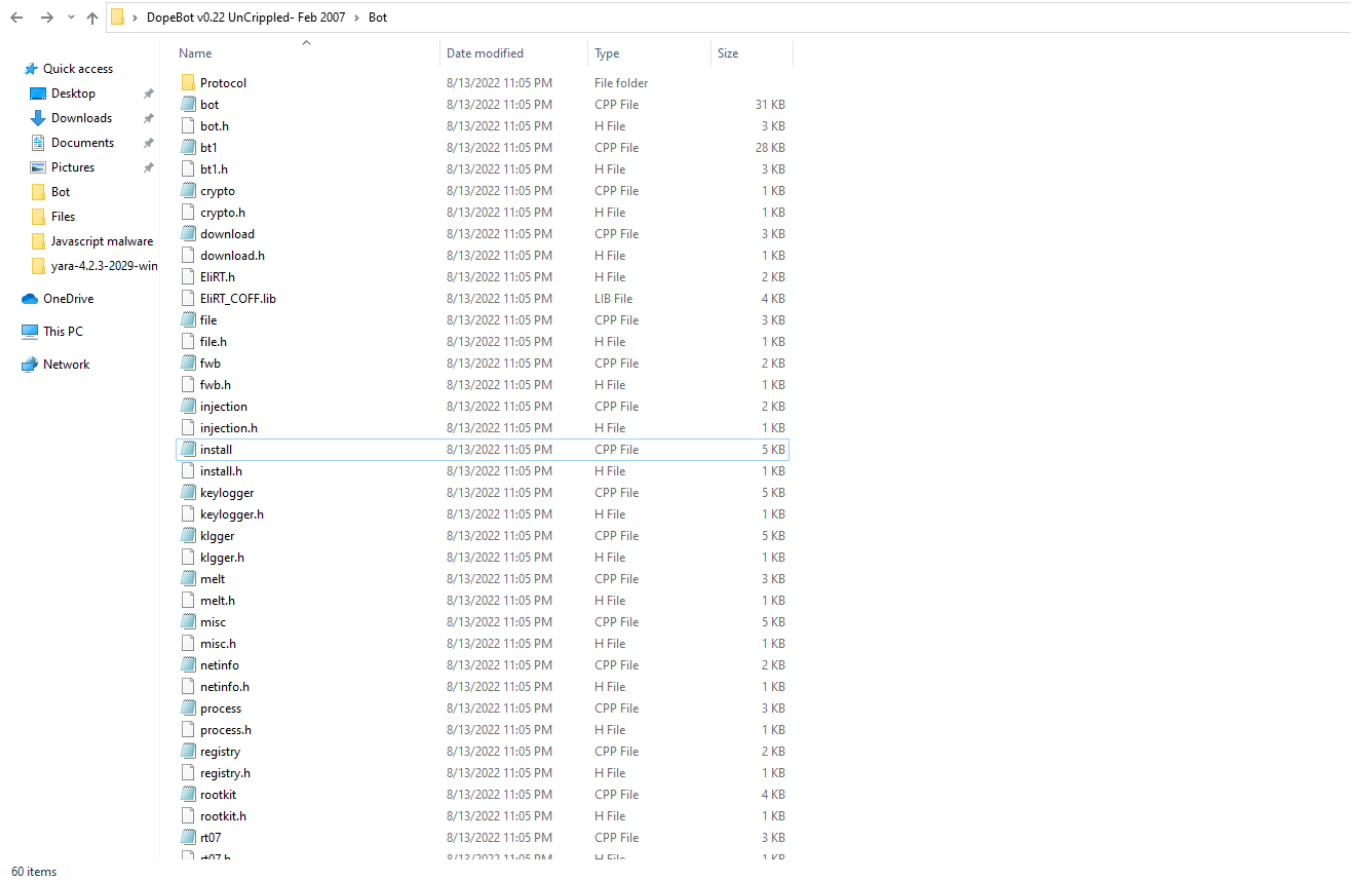
Functions | Strings | Segments

Address	Length	Type	String
.data:13141088	0000000F	C	FindFirstFileA
.data:131414CE	0000000F	C	FindFirstFileA
.data:13141058	0000000F	C	FindFirstFileW
.data:13141506	0000000F	C	FindFirstFileW
.data:13141078	0000000E	C	FindNextFileA
.data:131414E0	0000000E	C	FindNextFileA
.data:13141048	0000000E	C	FindNextFileW
.data:13141518	0000000E	C	FindNextFileW
.data:131414AE	00000011	C	GetModuleHandleA
.data:1314149C	0000000F	C	GetProcAddress
.data:13141098	0000000D	C	KERNEL32.DLL
.data:13141526	0000000D	C	KERNEL32.dll
.data:1314153E	0000000B	C	MSVCRT.dll
.data:1314154C	0000000F	C	PathStripPathA
.data:1314155C	0000000C	C	SHLWAPI.dll
.data:1314148A	0000000F	C	VirtualProtect
.data:131414F0	00000014	C	WideCharToMultiByte
.data:13141040	00000007	C	_dope_
.data:1314156A	00000009	C	_stricmp
.data:13141068	0000000D	C	kernel32.dll
.data:131414C2	0000000A	C	lstrcmpiA
.data:13141536	00000008	C	sprintf

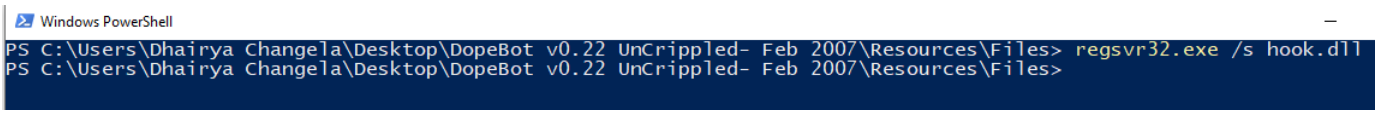
- We can also see what are the different strings are there with its address value.

Dynamic Analysis:

- There are various cpp files which are interconnected to other files

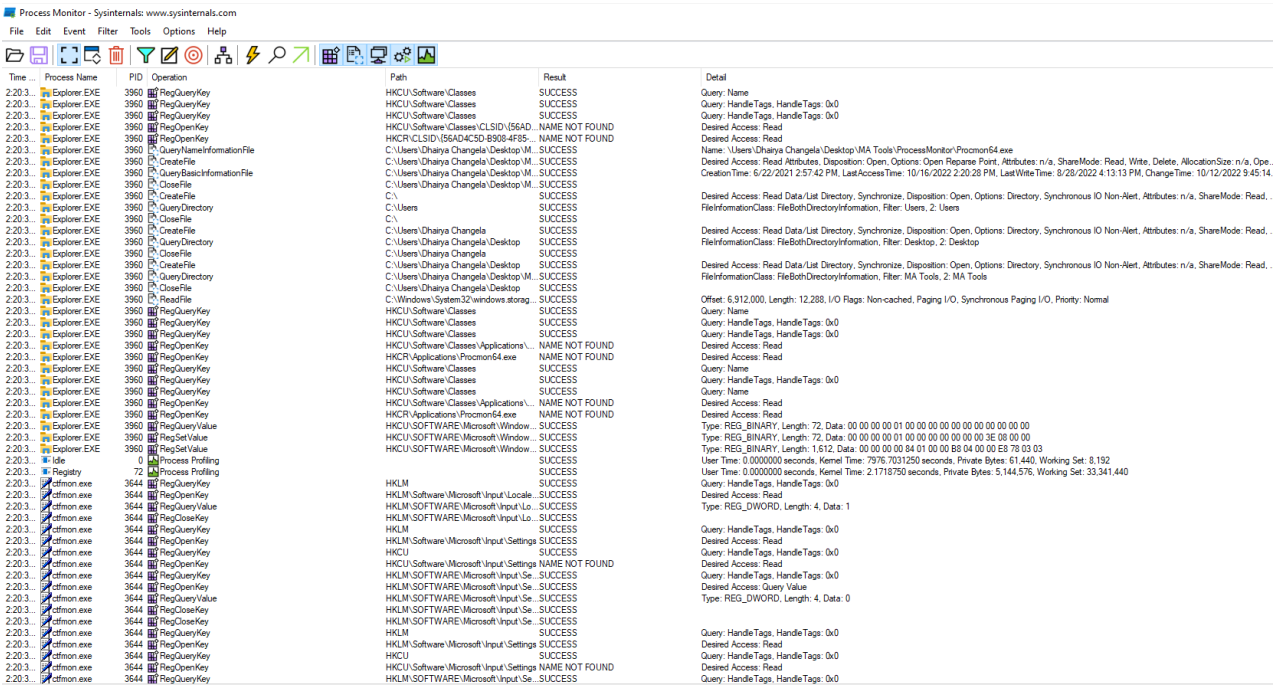


- Let’s execute the main .dll file.



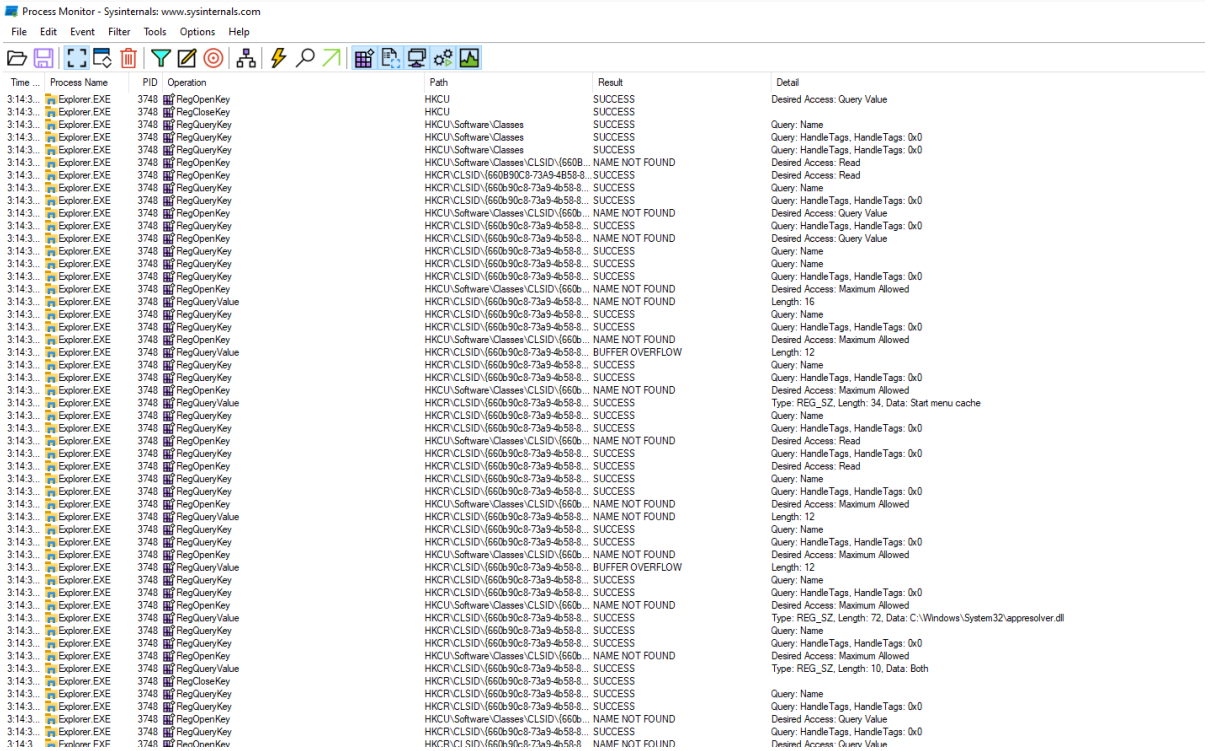
Process Explorer tool:

Before executing:



Time ...	Process Name	PID	Operation	Path	Result	Detail
2:20:3...	Explorer.EXE	3960	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
2:20:3...	Explorer.EXE	3960	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTags, HandleTags: 0x0
2:20:3...	Explorer.EXE	3960	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTags, HandleTags: 0x0
2:20:3...	Explorer.EXE	3960	RegOpenKey	HKCU\Software\Classes\CLSID\{56AD...	NAME NOT FOUND	Desired Access: Read
2:20:3...	Explorer.EXE	3960	RegOpenKey	HKCR\CLSID\{56AD4C5D-B908-4F85-...	NAME NOT FOUND	Desired Access: Read
2:20:3...	Explorer.EXE	3960	QueryNameInformationFile	C:\Users\Dhairya Changela\Desktop\M...	SUCCESS	Name: \Users\Dhairya Changela\Desktop\MA Tools\ProcessMonitor\Procmon64.exe
2:20:3...	Explorer.EXE	3960	CreateFile	C:\Users\Dhairya Changela\Desktop\M...	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, ShareMode: Read, Write, Delete, AllocationSize: n/a, Ope...
2:20:3...	Explorer.EXE	3960	QueryBasicInformationFile	C:\Users\Dhairya Changela\Desktop\M...	SUCCESS	CreationTime: 6/22/2021 2:57:42 PM, LastAccessTime: 10/16/2022 2:20:28 PM, LastWriteTime: 8/28/2022 4:13:13 PM, ChangeTime: 10/12/2022 9:45:14.
2:20:3...	Explorer.EXE	3960	CloseFile	C:\Users\Dhairya Changela\Desktop\M...	SUCCESS	
2:20:3...	Explorer.EXE	3960	CreateFile	C:\	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attributes: n/a, ShareMode: Read, .
2:20:3...	Explorer.EXE	3960	QueryDirectory	C:\Users	SUCCESS	FileInformationClass: FileBothDirectoryInformation, Filter: Users, 2: Users
2:20:3...	Explorer.EXE	3960	CloseFile	C:\	SUCCESS	
2:20:3...	Explorer.EXE	3960	CreateFile	C:\Users\Dhairya Changela	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attributes: n/a, ShareMode: Read, .
2:20:3...	Explorer.EXE	3960	QueryDirectory	C:\Users\Dhairya Changela\Desktop	SUCCESS	FileInformationClass: FileBothDirectoryInformation, Filter: Desktop, 2: Desktop
2:20:3...	Explorer.EXE	3960	CloseFile	C:\Users\Dhairya Changela	SUCCESS	
2:20:3...	Explorer.EXE	3960	CreateFile	C:\Users\Dhairya Changela\Desktop	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attributes: n/a, ShareMode: Read, .
2:20:3...	Explorer.EXE	3960	QueryDirectory	C:\Users\Dhairya Changela\Desktop\M...	SUCCESS	FileInformationClass: FileBothDirectoryInformation, Filter: MA Tools, 2: MA Tools
2:20:3...	Explorer.EXE	3960	CloseFile	C:\Users\Dhairya Changela\Desktop	SUCCESS	
2:20:3...	Explorer.EXE	3960	ReadFile	C:\Windows\System32\windows.storag...	SUCCESS	Offset: 6,912,000, Length: 12,288, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
2:20:3...	Explorer.EXE	3960	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
2:20:3...	Explorer.EXE	3960	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTags, HandleTags: 0x0
2:20:3...	Explorer.EXE	3960	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTags, HandleTags: 0x0
2:20:3...	Explorer.EXE	3960	RegOpenKey	HKCU\Software\Classes\Applications\...	NAME NOT FOUND	Desired Access: Read
2:20:3...	Explorer.EXE	3960	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: Read
2:20:3...	Explorer.EXE	3960	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
2:20:3...	Explorer.EXE	3960	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTags, HandleTags: 0x0
2:20:3...	Explorer.EXE	3960	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
2:20:3...	Explorer.EXE	3960	RegOpenKey	HKCU\Software\Classes\Applications\...	NAME NOT FOUND	Desired Access: Read
2:20:3...	Explorer.EXE	3960	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: Read
2:20:3...	Explorer.EXE	3960	RegQueryValue	HKCU\SOFTWARE\Microsoft\Window...	SUCCESS	Type: REG_BINARY, Length: 72, Data: 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00
2:20:3...	Explorer.EXE	3960	RegSetValue	HKCU\SOFTWARE\Microsoft\Window...	SUCCESS	Type: REG_BINARY, Length: 72, Data: 00 00 00 00 01 00 00 00 00 00 00 00 3E 08 00 00
2:20:3...	Explorer.EXE	3960	RegSetValue	HKCU\SOFTWARE\Microsoft\Window...	SUCCESS	Type: REG_BINARY, Length: 1,612, Data: 00 00 00 00 84 01 00 00 B8 04 00 00 E8 78 03 03
2:20:3...	Idle	0	Process Profiling		SUCCESS	User Time: 0.0000000 seconds, Kernel Time: 7976.7031250 seconds, Private Bytes: 61,440, Working Set: 8,192
2:20:3...	Registry	72	Process Profiling		SUCCESS	User Time: 0.0000000 seconds, Kernel Time: 2.1718750 seconds, Private Bytes: 5,144,576, Working Set: 33,341,440
2:20:3...	ctfmon.exe	3644	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
2:20:3...	ctfmon.exe	3644	RegOpenKey	HKLM\Software\Microsoft\Input\Locale...	SUCCESS	Desired Access: Read
2:20:3...	ctfmon.exe	3644	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Lo...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
2:20:3...	ctfmon.exe	3644	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Lo...	SUCCESS	
2:20:3...	ctfmon.exe	3644	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
2:20:3...	ctfmon.exe	3644	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Desired Access: Read
2:20:3...	ctfmon.exe	3644	RegQueryKey	HKCU	SUCCESS	Query: HandleTags, HandleTags: 0x0
2:20:3...	ctfmon.exe	3644	RegOpenKey	HKCU\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: Read
2:20:3...	ctfmon.exe	3644	RegQueryKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Query: HandleTags, HandleTags: 0x0
2:20:3...	ctfmon.exe	3644	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Desired Access: Query Value
2:20:3...	ctfmon.exe	3644	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
2:20:3...	ctfmon.exe	3644	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
2:20:3...	ctfmon.exe	3644	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
2:20:3...	ctfmon.exe	3644	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
2:20:3...	ctfmon.exe	3644	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Desired Access: Read
2:20:3...	ctfmon.exe	3644	RegQueryKey	HKCU	SUCCESS	Query: HandleTags, HandleTags: 0x0
2:20:3...	ctfmon.exe	3644	RegOpenKey	HKCU\Software\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: Read
2:20:3...	ctfmon.exe	3644	RegQueryKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Query: HandleTags, HandleTags: 0x0

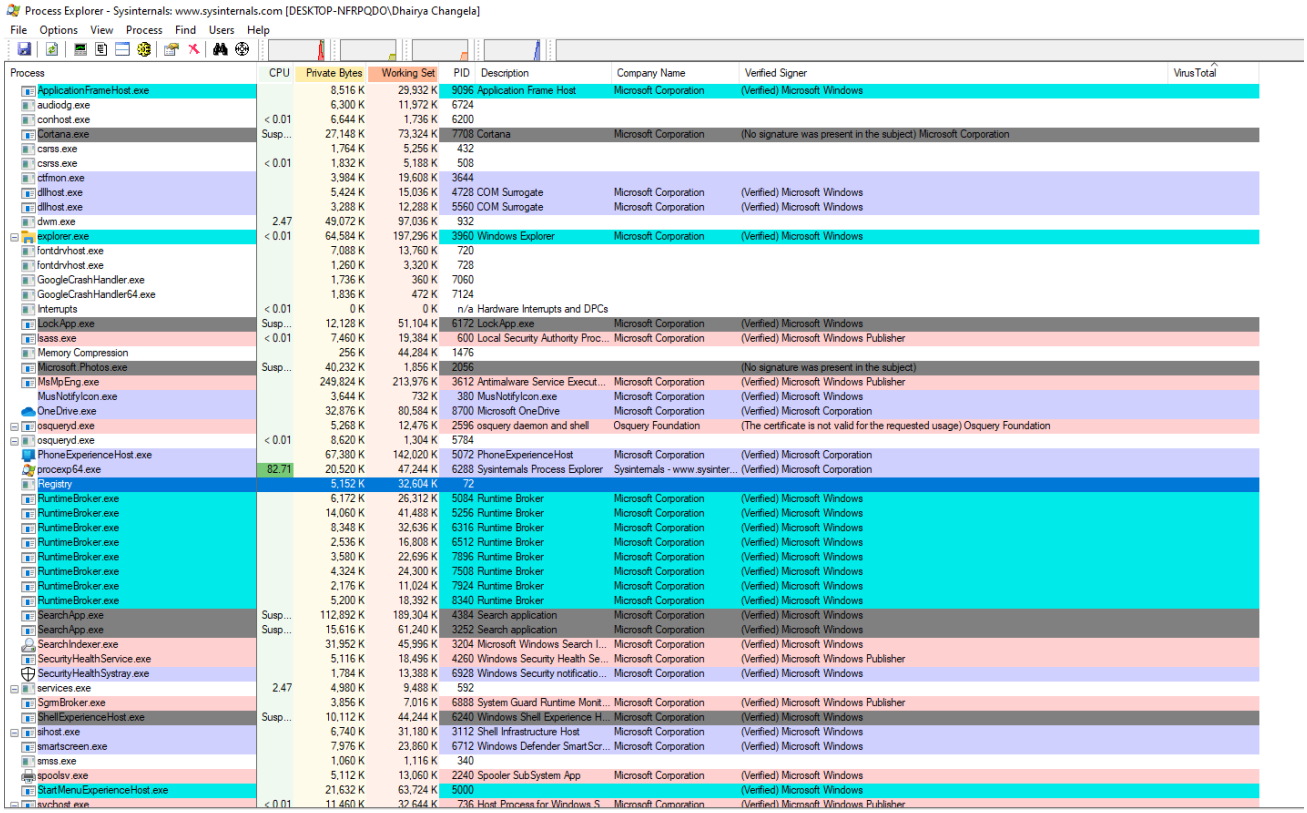
After executing:



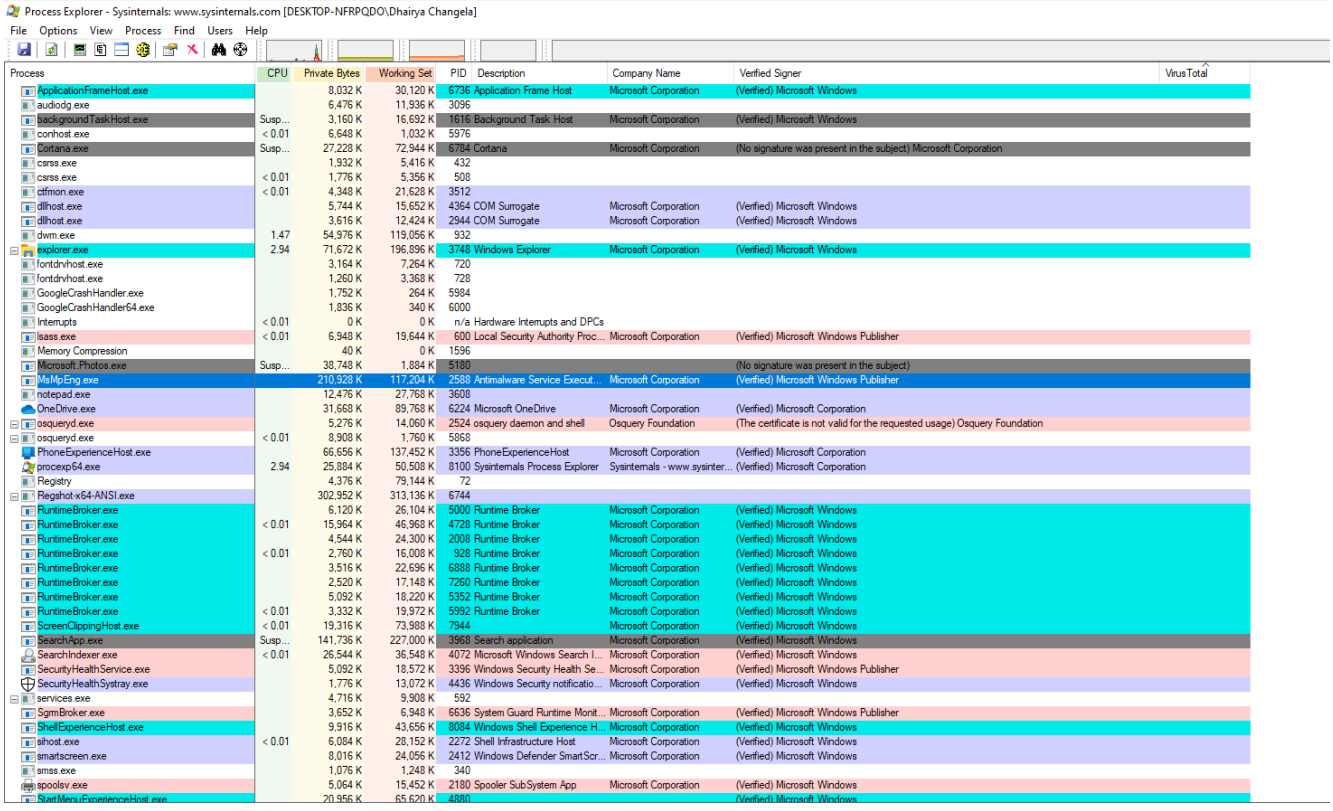
Time ...	Process Name	PID	Operation	Path	Result	Detail
3:14:3...	Explorer.EXE	3748	RegOpenKey	HKCU	SUCCESS	Desired Access: Query Value
3:14:3...	Explorer.EXE	3748	RegCloseKey	HKCU	SUCCESS	
3:14:3...	Explorer.EXE	3748	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
3:14:3...	Explorer.EXE	3748	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTags, HandleTags: 0x0
3:14:3...	Explorer.EXE	3748	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTags, HandleTags: 0x0
3:14:3...	Explorer.EXE	3748	RegOpenKey	HKCU\Software\Classes\CLSID\{660B...	NAME NOT FOUND	Desired Access: Read
3:14:3...	Explorer.EXE	3748	RegOpenKey	HKCR\CLSID\{660B90C8-73A9-4B58-8...	SUCCESS	Desired Access: Read
3:14:3...	Explorer.EXE	3748	RegQueryKey	HKCR\CLSID\{660b90c8-73a9-4b58-8...	SUCCESS	Query: Name
3:14:3...	Explorer.EXE	3748	RegQueryKey	HKCR\CLSID\{660b90c8-73a9-4b58-8...	SUCCESS	Query: HandleTags, HandleTags: 0x0
3:14:3...	Explorer.EXE	3748	RegOpenKey	HKCU\Software\Classes\CLSID\{660b...	NAME NOT FOUND	Desired Access: Query Value
3:14:3...	Explorer.EXE	3748	RegQueryKey	HKCR\CLSID\{660b90c8-73a9-4b58-8...	SUCCESS	Query: HandleTags, HandleTags: 0x0
3:14:3...	Explorer.EXE	3748	RegOpenKey	HKCR\CLSID\{660b90c8-73a9-4b58-8...	NAME NOT FOUND	Desired Access: Query Value
3:14:3...	Explorer.EXE	3748	RegQueryKey	HKCR\CLSID\{660b90c8-73a9-4b58-8...	SUCCESS	Query: Name
3:14:3...	Explorer.EXE	3748	RegQueryKey	HKCR\CLSID\{660b90c8-73a9-4b58-8...	SUCCESS	Query: Name
3:14:3...	Explorer.EXE	3748	RegQueryKey	HKCR\CLSID\{660b90c8-73a9-4b58-8...	SUCCESS	Query: HandleTags, HandleTags: 0x0
3:14:3...	Explorer.EXE	3748	RegOpenKey	HKCU\Software\Classes\CLSID\{660b...	NAME NOT FOUND	Desired Access: Maximum Allowed
3:14:3...	Explorer.EXE	3748	RegQueryValue	HKCR\CLSID\{660b90c8-73a9-4b58-8...	NAME NOT FOUND	Length: 16
3:14:3...	Explorer.EXE	3748	RegQueryKey	HKCR\CLSID\{660b90c8-73a9-4b58-8...	SUCCESS	Query: Name
3:14:3...	Explorer.EXE	3748	RegQueryKey	HKCR\CLSID\{660b90c8-73a9-4b58-8...	SUCCESS	Query: HandleTags, HandleTags: 0x0
3:14:3...	Explorer.EXE	3748	RegOpenKey	HKCU\Software\Classes\CLSID\{660b...	NAME NOT FOUND	Desired Access: Maximum Allowed
3:14:3...	Explorer.EXE	3748	RegQueryValue	HKCR\CLSID\{660b90c8-73a9-4b58-8...	BUFFER OVERFLOW	Length: 12
3:14:3...	Explorer.EXE	3748	RegQueryKey	HKCR\CLSID\{660b90c8-73a9-4b58-8...	SUCCESS	Query: Name
3:14:3...	Explorer.EXE	3748	RegQueryKey	HKCR\CLSID\{660b90c8-73a9-4b58-8...	SUCCESS	Query: HandleTags, HandleTags: 0x0
3:14:3...	Explorer.EXE	3748	RegOpenKey	HKCU\Software\Classes\CLSID\{660b...	NAME NOT FOUND	Desired Access: Maximum Allowed
3:14:3...	Explorer.EXE	3748	RegQueryValue	HKCR\CLSID\{660b90c8-73a9-4b58-8...	SUCCESS	Type: REG_SZ, Length: 34, Data: Start menu cache
3:14:3...	Explorer.EXE	3748	RegQueryKey	HKCR\CLSID\{660b90c8-73a9-4b58-8...	SUCCESS	Query: Name
3:14:3...	Explorer.EXE	3748	RegQueryKey	HKCR\CLSID\{660b90c8-73a9-4b58-8...	SUCCESS	Query: HandleTags, HandleTags: 0x0
3:14:3...	Explorer.EXE	3748	RegOpenKey	HKCU\Software\Classes\CLSID\{660b...	NAME NOT FOUND	Desired Access: Read
3:14:3...	Explorer.EXE	3748	RegQueryKey	HKCR\CLSID\{660b90c8-73a9-4b58-8...	SUCCESS	Query: HandleTags, HandleTags: 0x0
3:14:3...	Explorer.EXE	3748	RegOpenKey	HKCR\CLSID\{660b90c8-73a9-4b58-8...	SUCCESS	Desired Access: Read
3:14:3...	Explorer.EXE	3748	RegQueryKey	HKCR\CLSID\{660b90c8-73a9-4b58-8...	SUCCESS	Query: Name
3:14:3...	Explorer.EXE	3748	RegQueryKey	HKCR\CLSID\{660b90c8-73a9-4b58-8...	SUCCESS	Query: HandleTags, HandleTags: 0x0
3:14:3...	Explorer.EXE	3748	RegOpenKey	HKCU\Software\Classes\CLSID\{660b...	NAME NOT FOUND	Desired Access: Maximum Allowed
3:14:3...	Explorer.EXE	3748	RegQueryValue	HKCR\CLSID\{660b90c8-73a9-4b58-8...	NAME NOT FOUND	Length: 12
3:14:3...	Explorer.EXE	3748	RegQueryKey	HKCR\CLSID\{660b90c8-73a9-4b58-8...	SUCCESS	Query: Name
3:14:3...	Explorer.EXE	3748	RegQueryKey	HKCR\CLSID\{660b90c8-73a9-4b58-8...	SUCCESS	Query: HandleTags, HandleTags: 0x0
3:14:3...	Explorer.EXE	3748	RegOpenKey	HKCU\Software\Classes\CLSID\{660b...	NAME NOT FOUND	Desired Access: Maximum Allowed
3:14:3...	Explorer.EXE	3748	RegQueryValue	HKCR\CLSID\{660b90c8-73a9-4b58-8...	BUFFER OVERFLOW	Length: 12
3:14:3...	Explorer.EXE	3748	RegQueryKey	HKCR\CLSID\{660b90c8-73a9-4b58-8...	SUCCESS	Query: Name
3:14:3...	Explorer.EXE	3748	RegQueryKey	HKCR\CLSID\{660b90c8-73a9-4b58-8...	SUCCESS	Query: HandleTags, HandleTags: 0x0
3:14:3...	Explorer.EXE	3748	RegOpenKey	HKCU\Software\Classes\CLSID\{660b...	NAME NOT FOUND	Desired Access: Maximum Allowed
3:14:3...	Explorer.EXE	3748	RegQueryValue	HKCR\CLSID\{660b90c8-73a9-4b58-8...	SUCCESS	Type: REG_SZ, Length: 72, Data: C:\Windows\System32\appresolver.dll
3:14:3...	Explorer.EXE	3748	RegQueryKey	HKCR\CLSID\{660b90c8-73a9-4b58-8...	SUCCESS	Query: Name
3:14:3...	Explorer.EXE	3748	RegQueryKey	HKCR\CLSID\{660b90c8-73a9-4b58-8...	SUCCESS	Query: HandleTags, HandleTags: 0x0
3:14:3...	Explorer.EXE	3748	RegOpenKey	HKCU\Software\Classes\CLSID\{660b...	NAME NOT FOUND	Desired Access: Maximum Allowed
3:14:3...	Explorer.EXE	3748	RegQueryValue	HKCR\CLSID\{660b90c8-73a9-4b58-8...	SUCCESS	Type: REG_SZ, Length: 10, Data: Both
3:14:3...	Explorer.EXE	3748	RegCloseKey	HKCR\CLSID\{660b90c8-73a9-4b58-8...	SUCCESS	
3:14:3...	Explorer.EXE	3748	RegQueryKey	HKCR\CLSID\{660b90c8-73a9-4b58-8...	SUCCESS	Query: Name
3:14:3...	Explorer.EXE	3748	RegQueryKey	HKCR\CLSID\{660b90c8-73a9-4b58-8...	SUCCESS	Query: HandleTags, HandleTags: 0x0
3:14:3...	Explorer.EXE	3748	RegOpenKey	HKCU\Software\Classes\CLSID\{660b...	NAME NOT FOUND	Desired Access: Query Value
3:14:3...	Explorer.EXE	3748	RegQueryKey	HKCR\CLSID\{660b90c8-73a9-4b58-8...	SUCCESS	Query: HandleTags, HandleTags: 0x0

Process Monitor tool:

Before executing:



After executing:



RegShot tool:

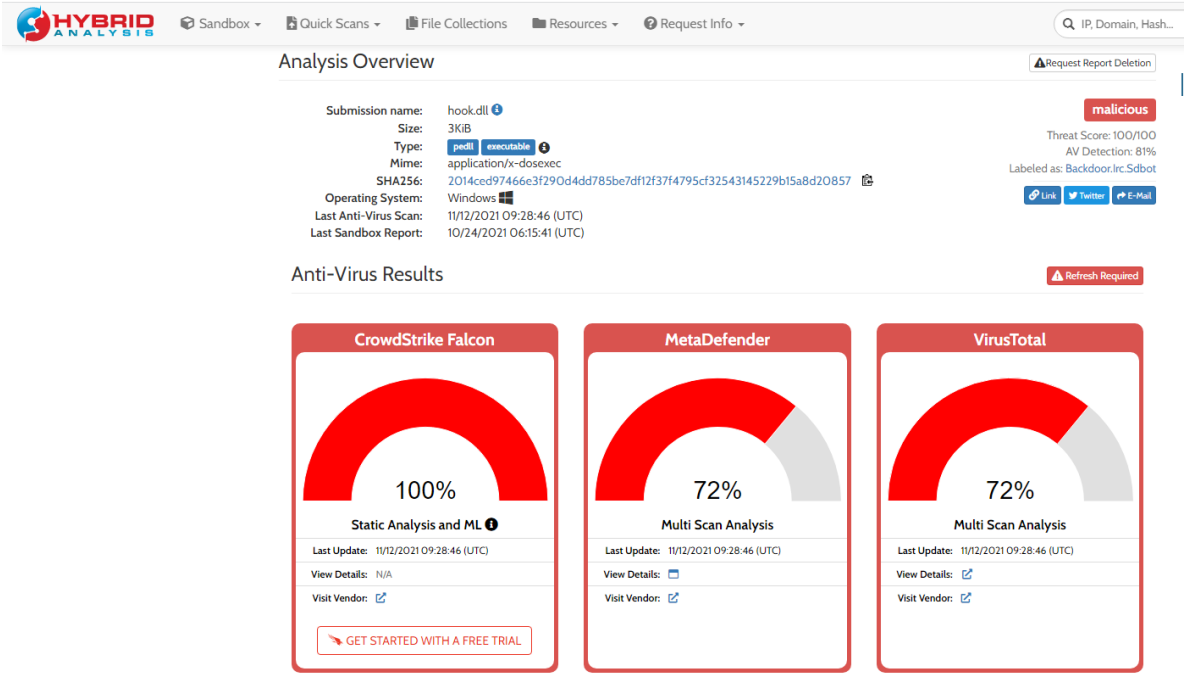
- After taking the 2nd shot in regshot tool, following registry keys changes have been made.

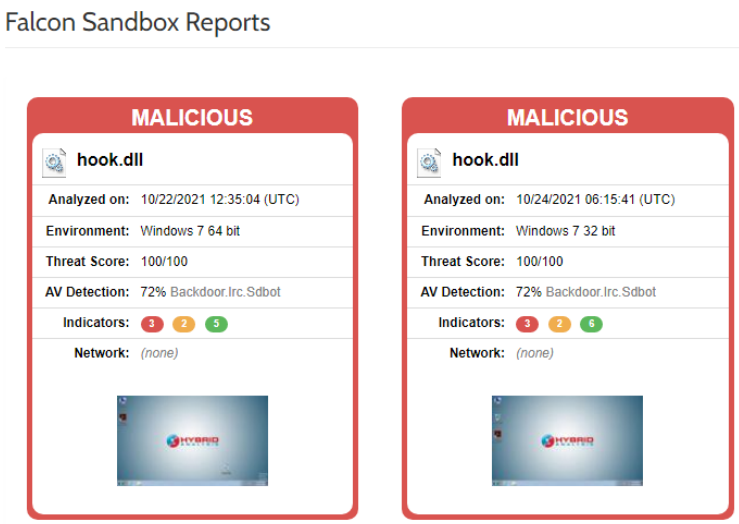
```
Regshot 1.9.0 x64 ANSI
Comments:
Datetime: 2022/10/16 08:55:16   ,   2022/10/16 09:19:42
Computer: DESKTOP-NFRPQDO , DESKTOP-NFRPQDO
Username: Dhairya Changela , Dhairya Changela

----------------------------------
Keys deleted: 20359
----------------------------------

----------------------------------
Keys added: 19
----------------------------------
HKLM\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\36B12B49F9819ED74C9EBC380FC6568F5DACB2F7
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1044
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\2840
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\4112
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\4736

----------------------------------
Values deleted: 24066
----------------------------------
HKLM\DRIVERS\DriverDatabase\Version: 0x0A000000
HKLM\DRIVERS\DriverDatabase\SchemaVersion: 0x00010000
HKLM\DRIVERS\DriverDatabase\UpdateDate:  60 59 85 E4 E5 DA D8 01
HKLM\DRIVERS\DriverDatabase\SetupStatus: 0x00000000
HKLM\DRIVERS\DriverDatabase\DeviceIds\*AEI0276\mdmmetri.inf:  01 FF 00 00
HKLM\DRIVERS\DriverDatabase\DeviceIds\*AEI9240\mdmti.inf:  01 FF 00 00

----------------------------------
Total changes: 44736
----------------------------------
```

HYBRID ANALYSIS:

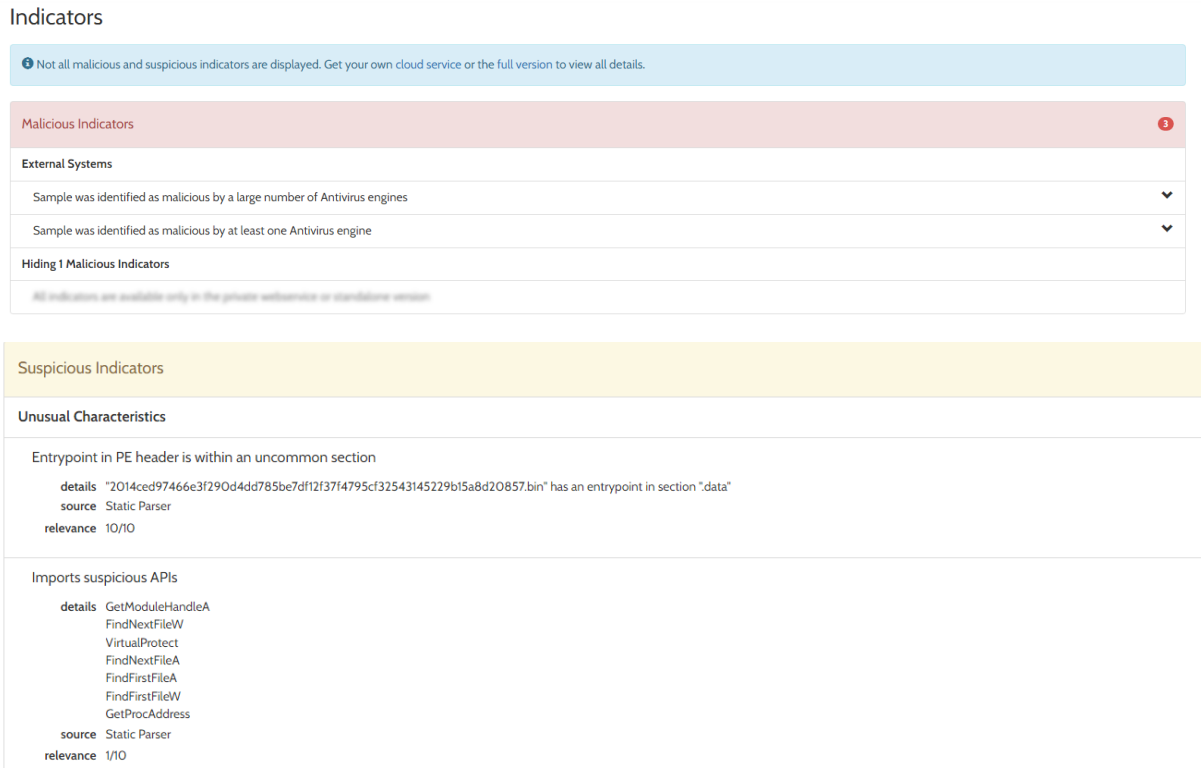
Sandbox analysis (website):

- Here we've done sandbox analysis of the malware on hybrid-analysis website and found General information as below.



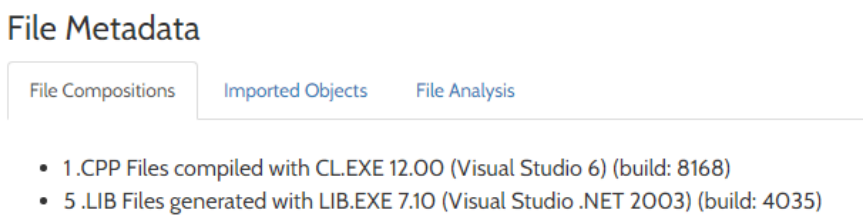


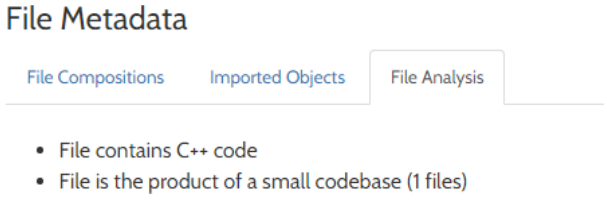
- Malicious and suspicious indicators were found in the file



- The malware imports following files.

- The metadata of the file.





Behaviour:

- After manually analysed the code, one of the file initiates a bot which then logs in to the host system, opening a socket.
- Further this bot downloads and activates multiple other bots through the internet.
- These multiple bots downloaded have various purposes such as listed below:
    - A bot is http downloader which downloads various files required by the boat to perform their respective tasks.
    - Another bot is programmed to open, execute and delete various files (majorly cpp & header files) as and when required by the bots.
    - Another bot is a network sniffer that sniffs the whole network of the target system.
    - Another bot is a key logger which records all the keystrokes of the target and sends them over the internet to the host system.
    - Another bot is a bandwidth flooder which floods the network of the target system disallowing it to perform any other activity over the internet.
    - Another bot is a system information stealer which grabs all the target system information and sends it over the internet.
    - Another bot's task is to update the registry keys in order to allow smooth functioning of the backdoor.
    - Another bot is programmed to list the current processes and kill the processes.
    - Another bot is a IP grabber, which scans the whole network to which the target is connected.
    - Another bot is programmed to send the files over the internet using ftp, tftp protocols.
    - Another bot is programmed as a rootkit to access all the files and data on the target system which are not allowed to normal users.
    - Another bot is programmed to shutdown all the other bots after the task is completed.

Conclusion:

- Seeing The files created by the malware when it was executed shows that the whole malware was designed using c++ as a base language and the malware was professionally developed to grab each and every vital information on the target system ranging from its IP Address, registry keys, current processes to the files not visible to normal users. This clearly shows that when the malware gets executed it will straight away have admin or root level privileges on the target system. It was also observed that the malware was self-capable of deleting the files it had create and killing the processes it starts in the backhand. Hence, giving the user no clue about the execution of the malware.