IT3564

Eden's Malware Analysis Adventures

Practical Assignment

Contents

Introduction

In this report…….. static and dynamic analysis will be conducted to understand how the programs will work and interact with the system…….

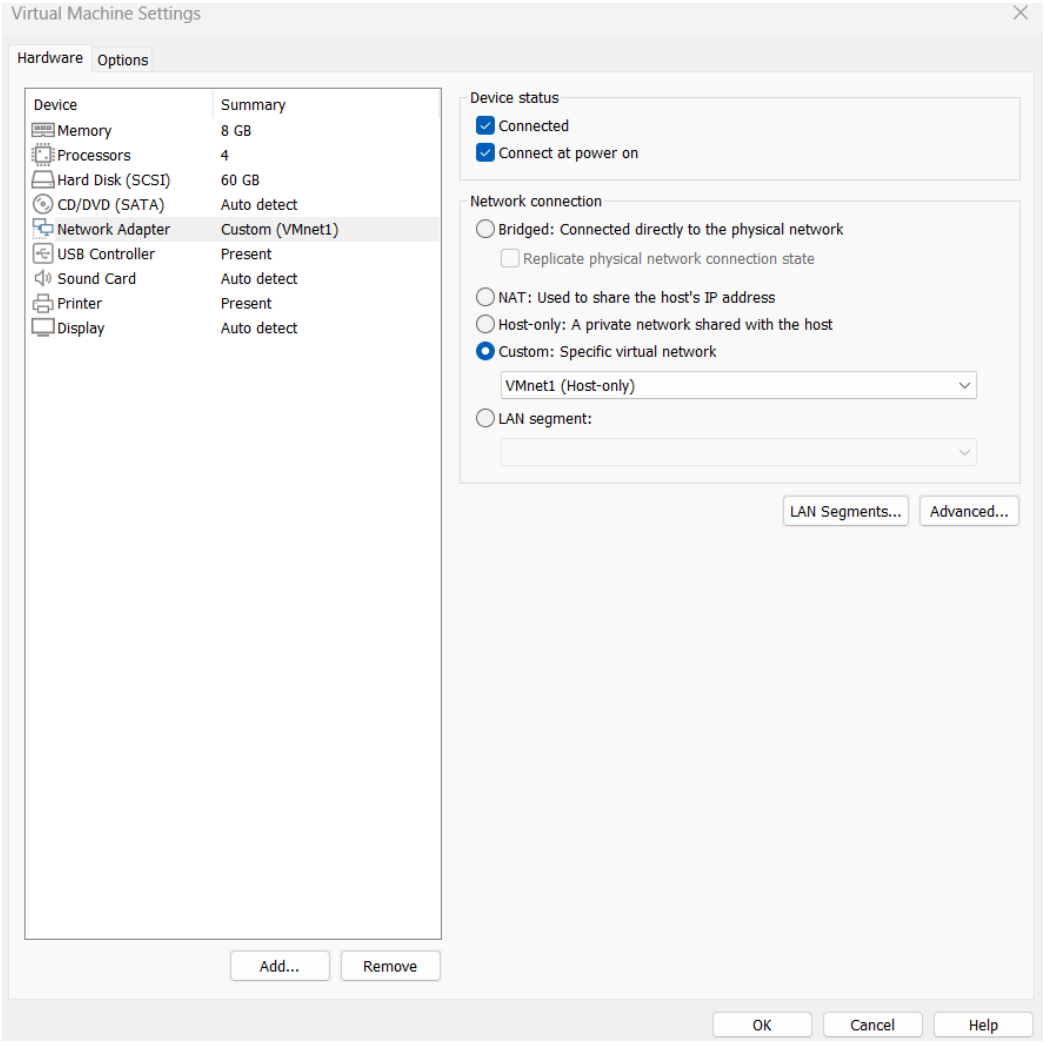
The malware will be simulated and tested through various means

Tools Used

Virtualization

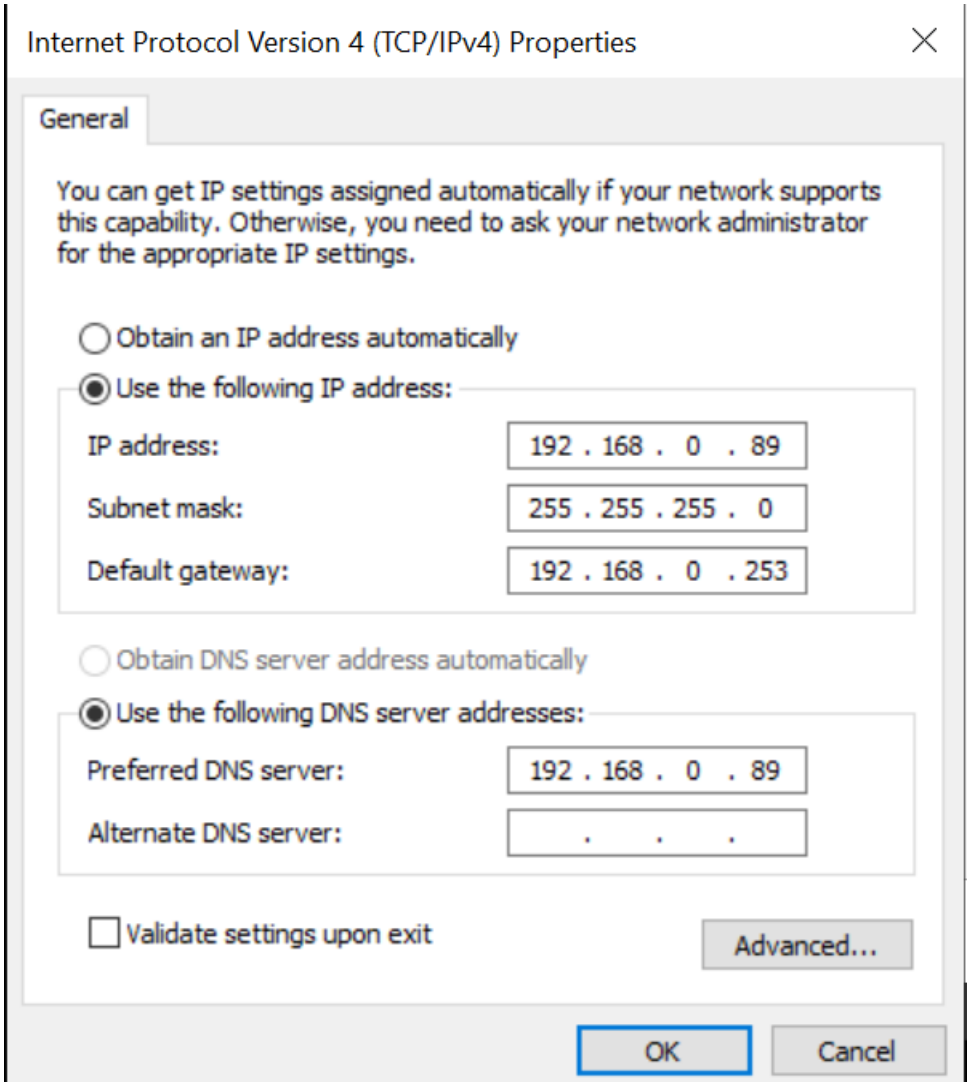
VMware Workstation 17 Pro is used to provide a virtual environment. The virtual machines used are as follows. All the virtual machines are in an isolated NAT Network with no access to the internet.

1. **Windows 10 64bit Service Pack 1**
    a. **8GB RAM**
    b. **HOST-ONLY networking.**
    c. **VMNET 1**



Isolate all Networks.

Verify that Networking is Host Only and isolated.



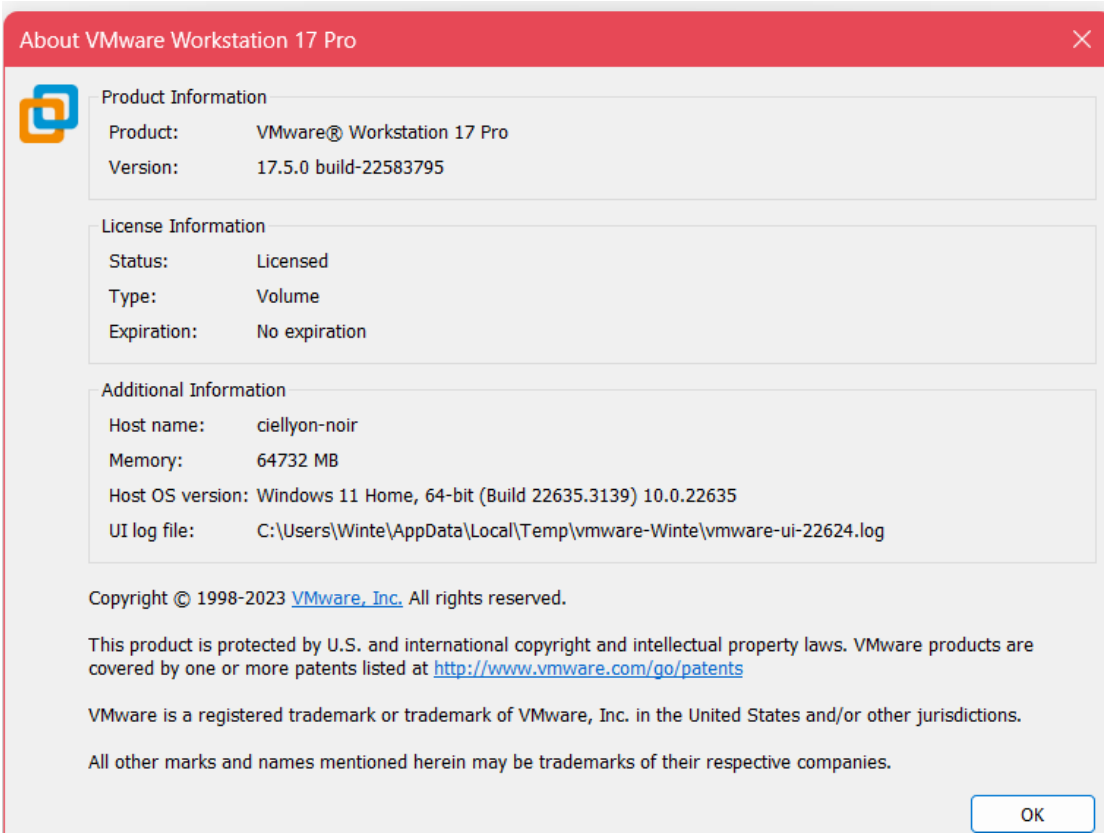
To do so complete the following steps

- **Run win + r**
- **ncpa.cpl**
- **Open the network adapter**
- **It should look like this**

Run FakeNET NG

This ensures that the malware think it is connected to the internet.

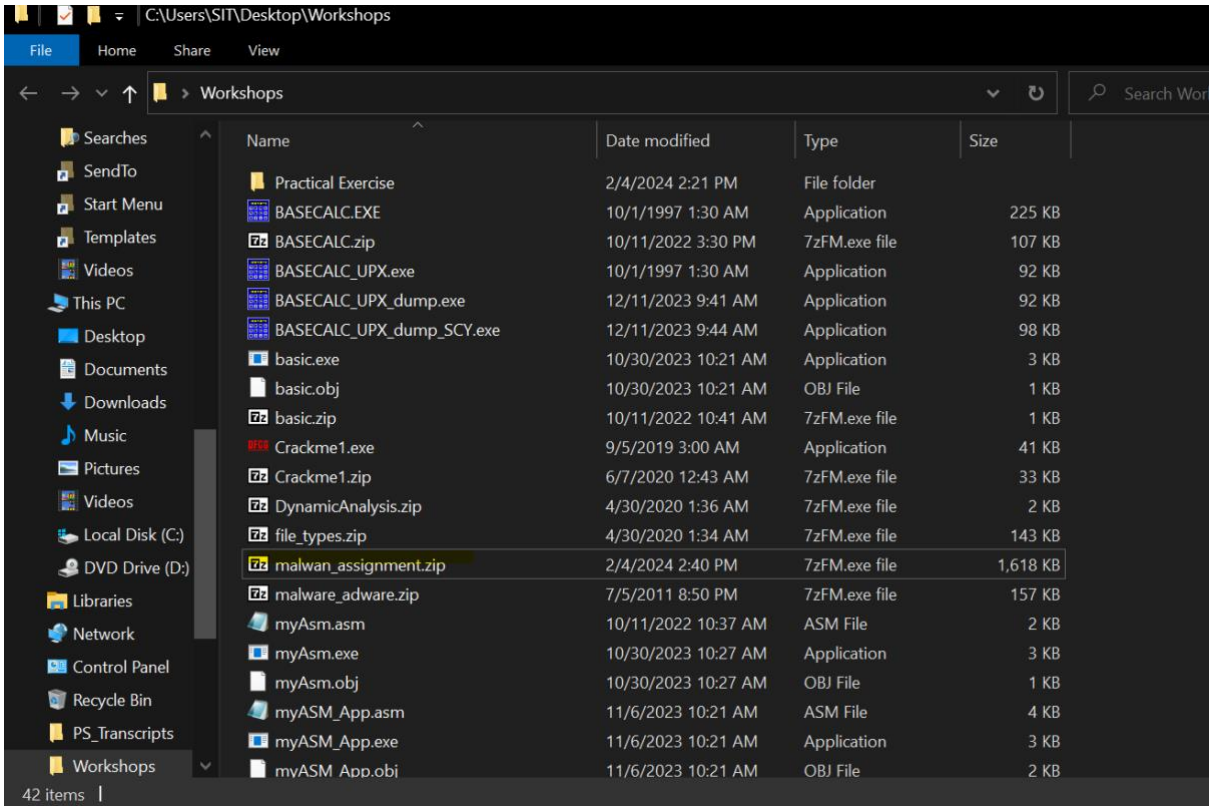
Ensure that VMWARE workstation pro is updated to latest patch



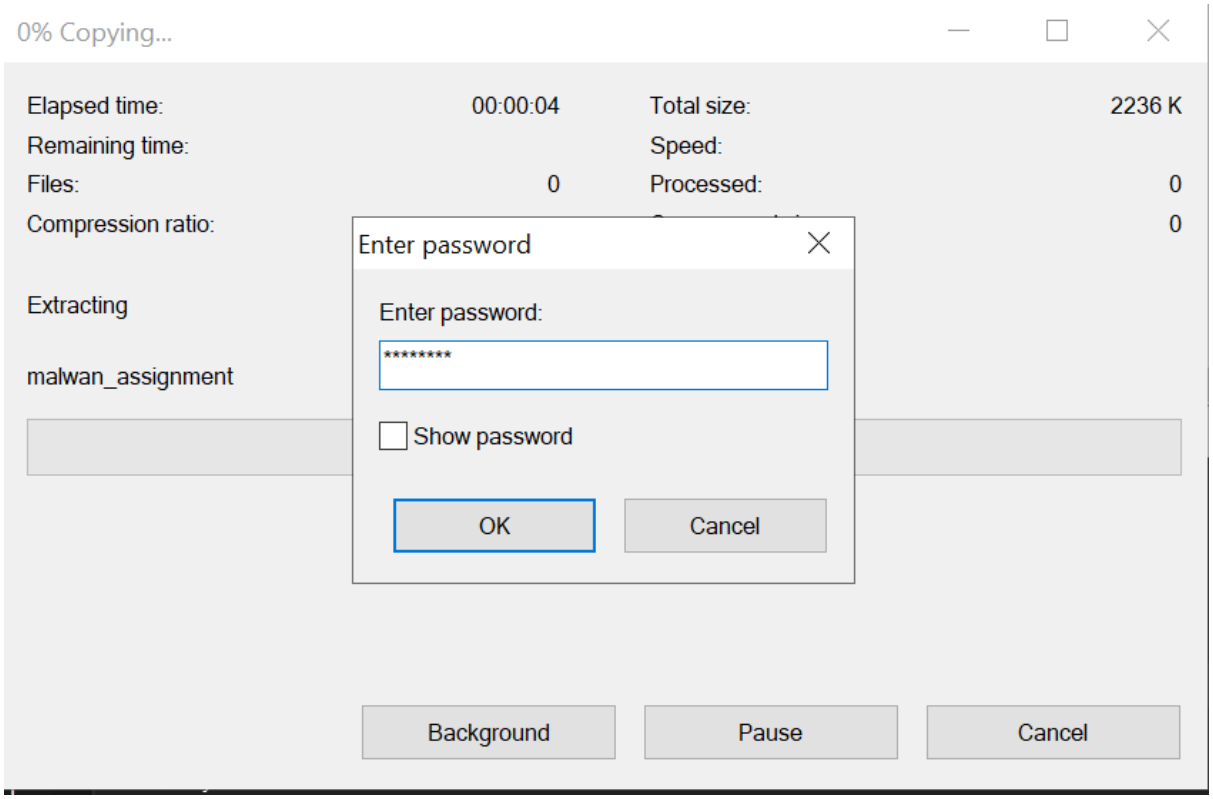
Static Properties Analysis (9 marks)

Place the file in Workshop for protected environment static properties.

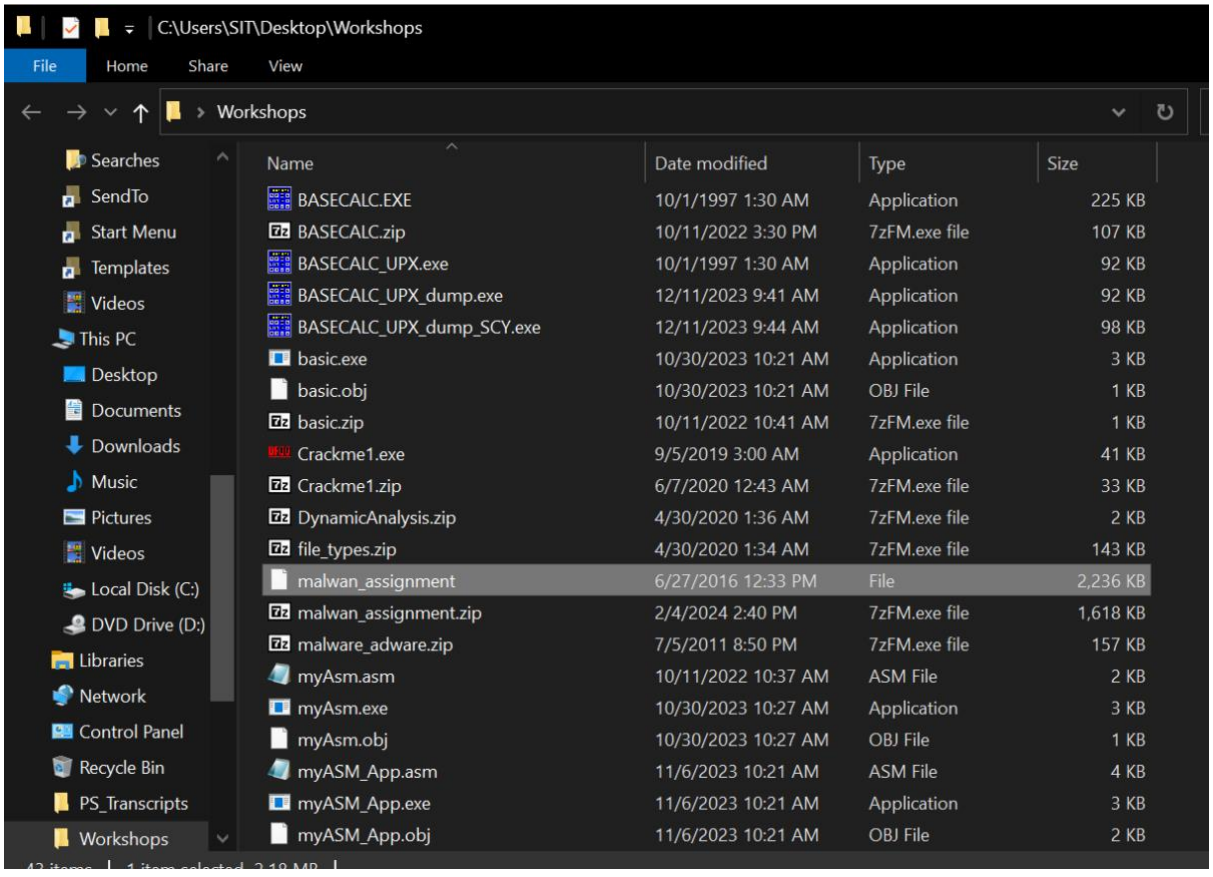
This ensure that if the malware is accidentally triggered it would not do much to the host machine.



Once done unzip the file for the malware.



Put malware as the password to unpack the malware.



Once unpacked, this would be the expected malware that will show.

6

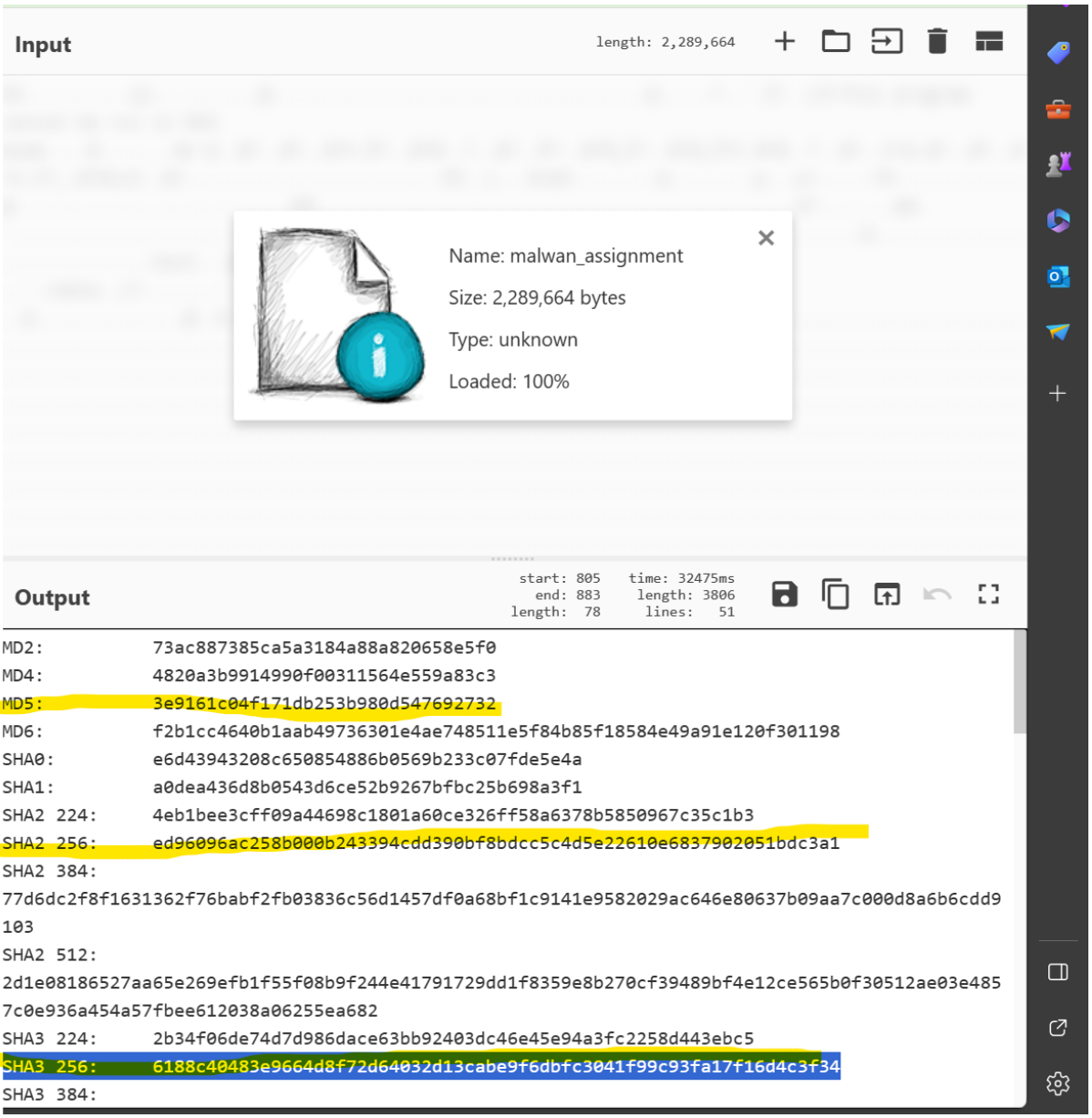
Hash (0.5 mark)

MD5	**MD5: 3e9161c04f171db253b980d547692732**
SHA1	**SHA1: a0dea436d8b0543d6ce52b9267bfbc25b698a3f1**
SHA256	**SHA2 256: ed96096ac258b000b243394cdd390bf8bdcc5c4d5e22610e6837902051bdc3a1** **SHA3 256: 6188c40483e9664d8f72d64032d13cabe9f6dbfc3041f99c93fa17f16d4c3f34**

Open cyberchef then do the hash calculations, cyberchef is a versatile tool that can be used to uncover information about the malware.

On the next page, I will show you the steps to generating the hashes for the malware analysis.

Steps to create the Hash output



1. Create recipe
2. Generate all hashes

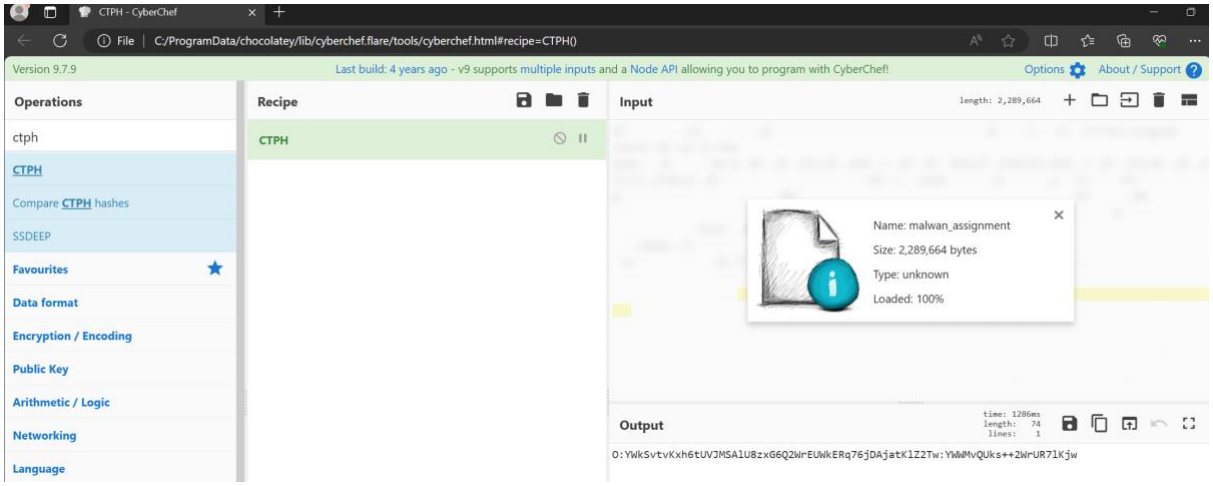
It would output the hash values of sha1, sha256 and md5

Compare (0.5 mark)

Fuzzy Hash	**CTPH:** **O:YWkSvtvKxh6tUVJMSAlU8zxG6Q2WrEUWkERq76jDAjatKlZ2Tw:YWWMvQUks++2WrUR7lKjw** **SSDEEP:** **49152:aKNosMNIVn1LsjETsYpeH0Lv7rLe491W5Jf0gFsIZrs8QKlwCo:aKu/NKsqKGvLe4cfm4Q6o**

To Obtain this findings, First open cyberchef.

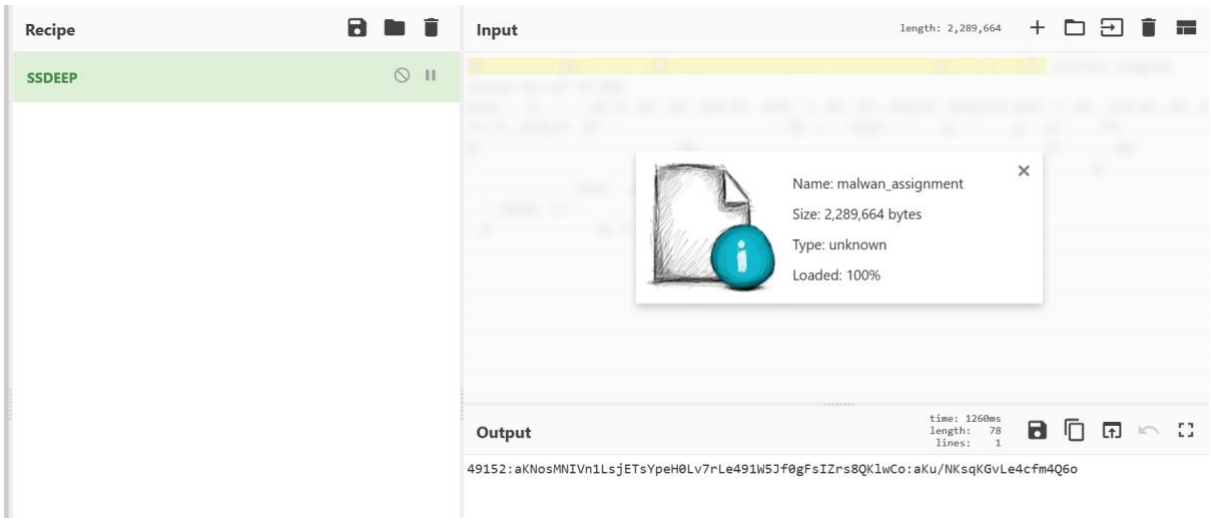
Then run Context Triggered Piecewise Hashes(CTPH) hash in the cyber chef this will show the fuzzy hash output generated.



Here shows the output of the CTPH hashes.

CTPH is a type of fuzzy hash that can be compared with other CTPH hash to generate a similarity report

Clear cyberchef and now run SSDEEP.



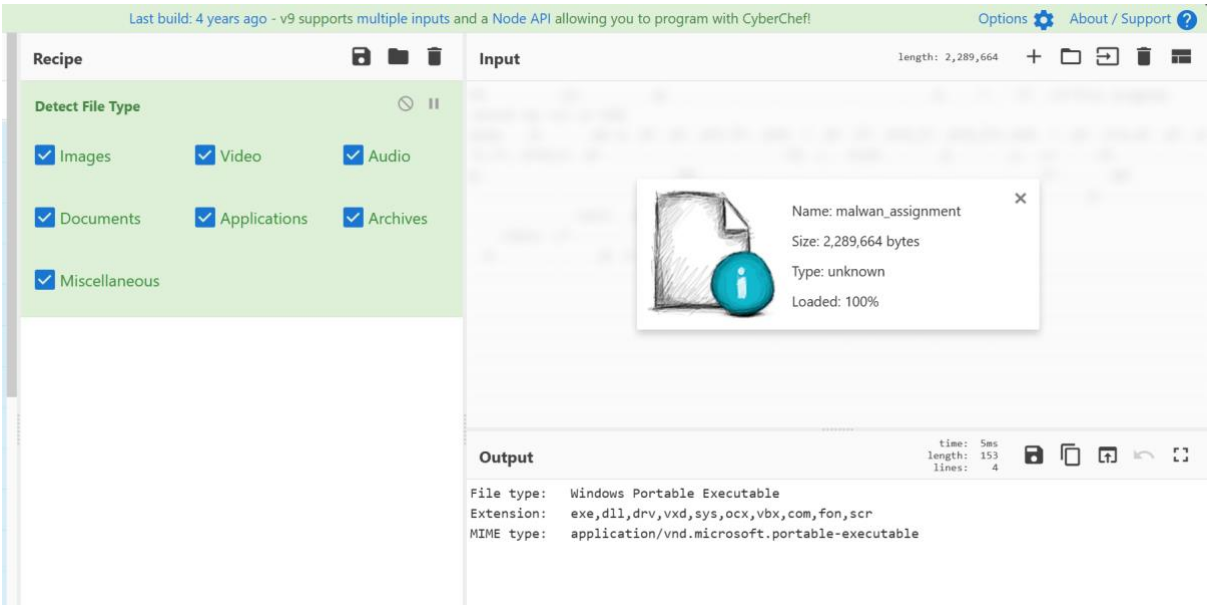
The Output of SSDeep hash is shown above.

SSDeep is another type of program to calculate the CTPH hash. It is used to compare file similarity based on the hash output.

Classify (1 mark)

File Type 1	Windows Portable Executable

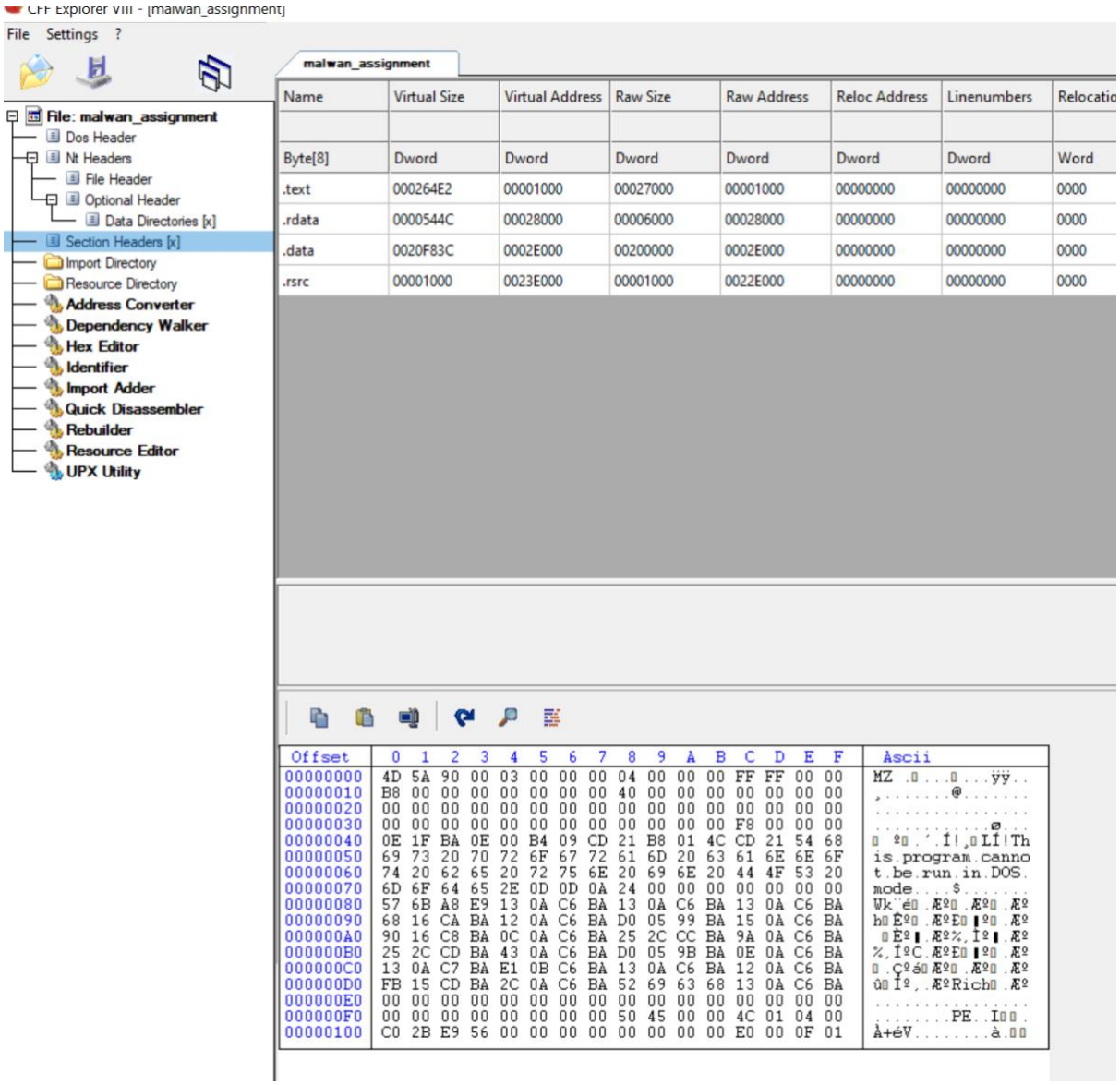
To deduce that it is a Windows Portable executable, lets open cyberchef



Open the detect file type recipe. Here it shows Windows portable executable to be the file type.

On the next page, I used CFF Explorer to verify that the file type is a Portable Executable

Other ways of verifying the file type could be achieved using tools such as CFFexplorer.



Open cff explorer

Click section headers

On offset 000000 the first two letter is MZ this indicates that the file is a portable executable.

This confirms that the file type if a portable executable.

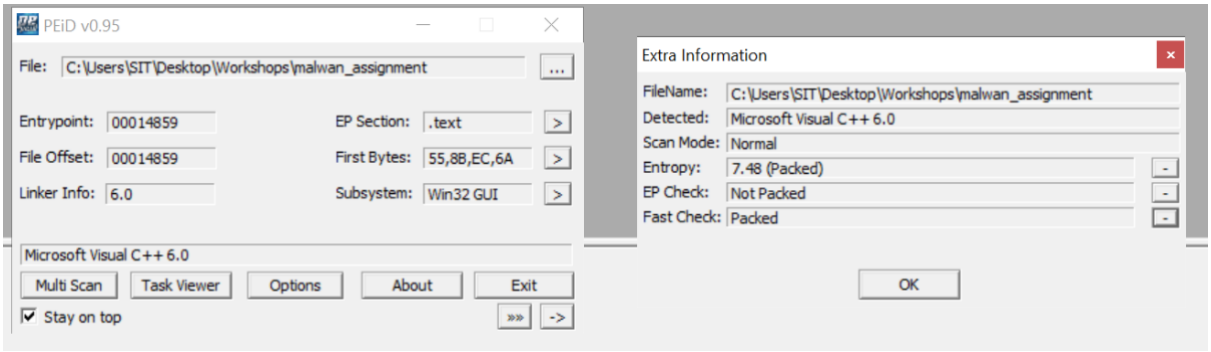
Examine (2 marks)

Identify at least 4 pieces of PE file information that is most relevant to its malicious properties/behaviours and explain why so.

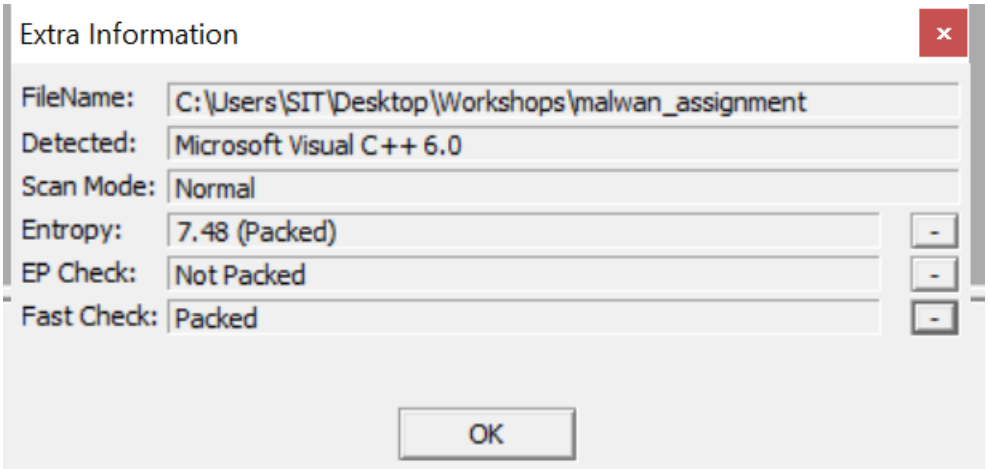
PE Information	**Entropy** **Score is 7.48** **This suggest the program is indeed packed. Entropy scores beyond 7 pts usually suggest the program is packed.** **However, during our file header analysis, it indicates that it is a portable executable.** **This may suggest that embedded files are attached within this portable executable that would be unpacked when the executable is run.** **We will need to verify this if it is true.**
PE Information	**Section Headers** **Only 4 Section Headers are Present.** • **.text** • **.rdata** • **Data** • **.rsrc** **Does not indicate that this has any malicious input yet. Moreover it does not suggest any packer used in the section header.**
PE Information	**Import Directory of cff viewer** **Modules such as kernel32 and user32 are capatilized.** **Suggesting that a packer was used to pack the module together.** **There are also many other dll being used. Suggesting that the malware has more complex behaviours than it seems. I will need to investigate further to see if there are any files that are of interest.**
PE Information File Name	**File Name is svchost disguised as a possible trojan; it is a file pretending to be a service host file**
PE Information File Header	**While detected as executable the file header in pestudio identifies the file as PE00 suggesting the file is a portable executable.**
PE Information Hex	**Using CFF explorer to check the address converter section. It was found that symbols resembling the present of a packer was seen when I scroll through the file contents using address converter.**

PEStudio Analysis	**Using PE studio, embedded files were detected in the portable executable. This suggest that the malware is a trojan that contains additional files within it to carry out its malicious tasks.**
Verification of embedded files with Cyber Chef	

PE Entropy Information

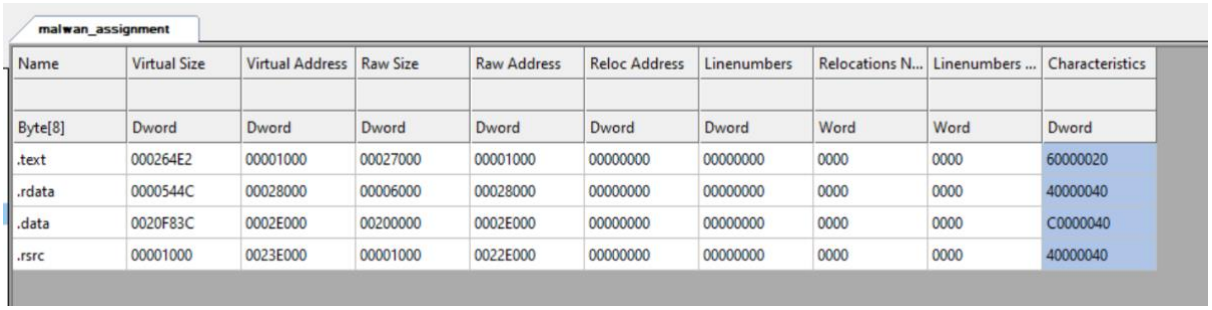


First I look at the entropy value, this will allow me to determine whether the program is packed. One of the best ways is to open PEID and to inspect the program entropy levels. If its high it will be regarded as packed. Here it shows the entropy level being 7.48, this suggest that the executable has packed contents



Since it indicates that the file is packed. My thought process would be to inspect the section headers. Usually packed files would have their section headers be different or packed with things such as UPX0 and UPX1

Section Headers

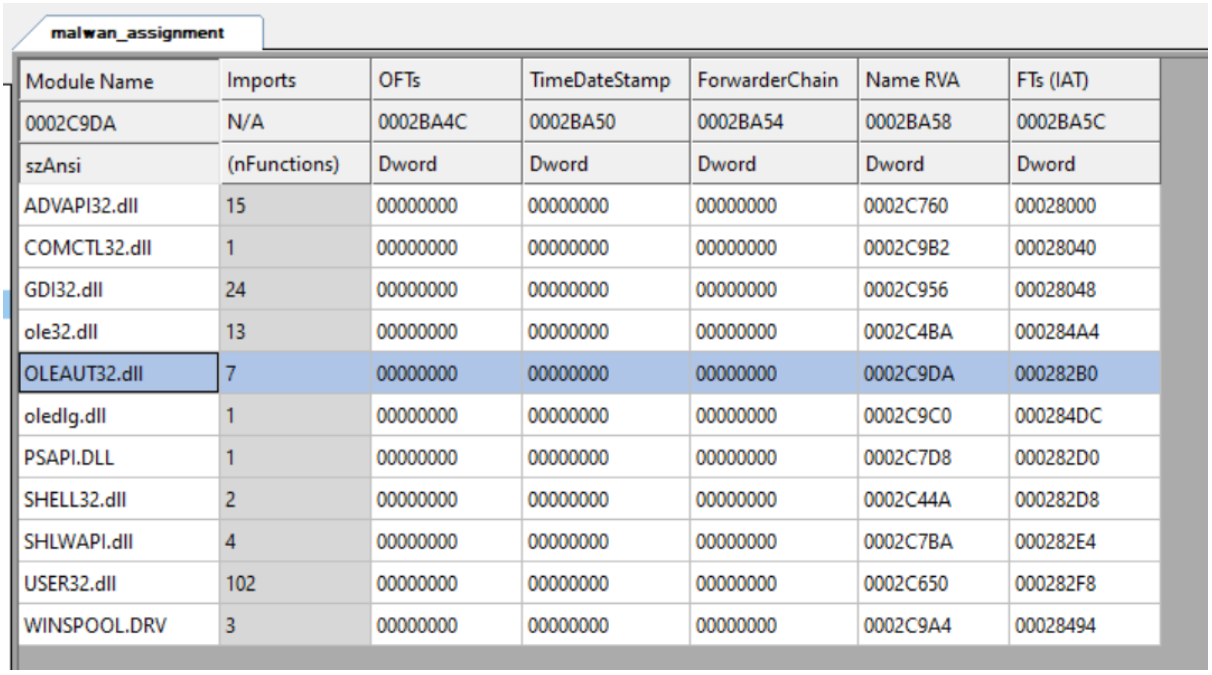


malwan_assignment

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	000264E2	00001000	00027000	00001000	00000000	00000000	0000	0000	60000020
.rdata	0000544C	00028000	00006000	00028000	00000000	00000000	0000	0000	40000040
.data	0020F83C	0002E000	00200000	0002E000	00000000	00000000	0000	0000	C0000040
.rsrc	00001000	0023E000	00001000	0022E000	00000000	00000000	0000	0000	40000040

During my inspection, no section headers were labelled as packed. However that does not rule out that this program is malicious.

Import directory of cff viewer


malwan_assignment

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
0002C9DA	N/A	0002BA4C	0002BA50	0002BA54	0002BA58	0002BA5C
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
ADVAPI32.dll	15	00000000	00000000	00000000	0002C760	00028000
COMCTL32.dll	1	00000000	00000000	00000000	0002C9B2	00028040
GDI32.dll	24	00000000	00000000	00000000	0002C956	00028048
ole32.dll	13	00000000	00000000	00000000	0002C4BA	000284A4
OLEAUT32.dll	7	00000000	00000000	00000000	0002C9DA	000282B0
oledlg.dll	1	00000000	00000000	00000000	0002C9C0	000284DC
PSAPI.DLL	1	00000000	00000000	00000000	0002C7D8	000282D0
SHELL32.dll	2	00000000	00000000	00000000	0002C44A	000282D8
SHLWAPI.dll	4	00000000	00000000	00000000	0002C7BA	000282E4
USER32.dll	102	00000000	00000000	00000000	0002C650	000282F8
WINSPOOL.DRV	3	00000000	00000000	00000000	0002C9A4	00028494

Using CFFExplorer, I will now check the import directory. Here it seems that there are many amount of libraries and modules imported. One thing that struck to me was how some of the modules in in capatilisation. This suggest that a packer was used earlier. For example in an non packed file kernel32 wouldn't be packed. While in a packed file kernel32 would look like KERNEL32 which is the same as the image above.

Property	Value
File Name	C:\Users\SIT\Desktop\Workshops\malwan_assignment
File Type	Portable Executable 32
File Info	Microsoft Visual C++ 6.0
File Size	2.18 MB (2289664 bytes)
PE Size	2.18 MB (2289664 bytes)
Created	Monday 12 December 2022, 10.26.26
Modified	Monday 27 June 2016, 12.33.24
Accessed	Sunday 04 February 2024, 18.59.37
MD5	145BC47EDEF11097AC970939D07A98FB
SHA-1	C5DD9D584A5EFAD6877FC067804A19E4CD6F4183

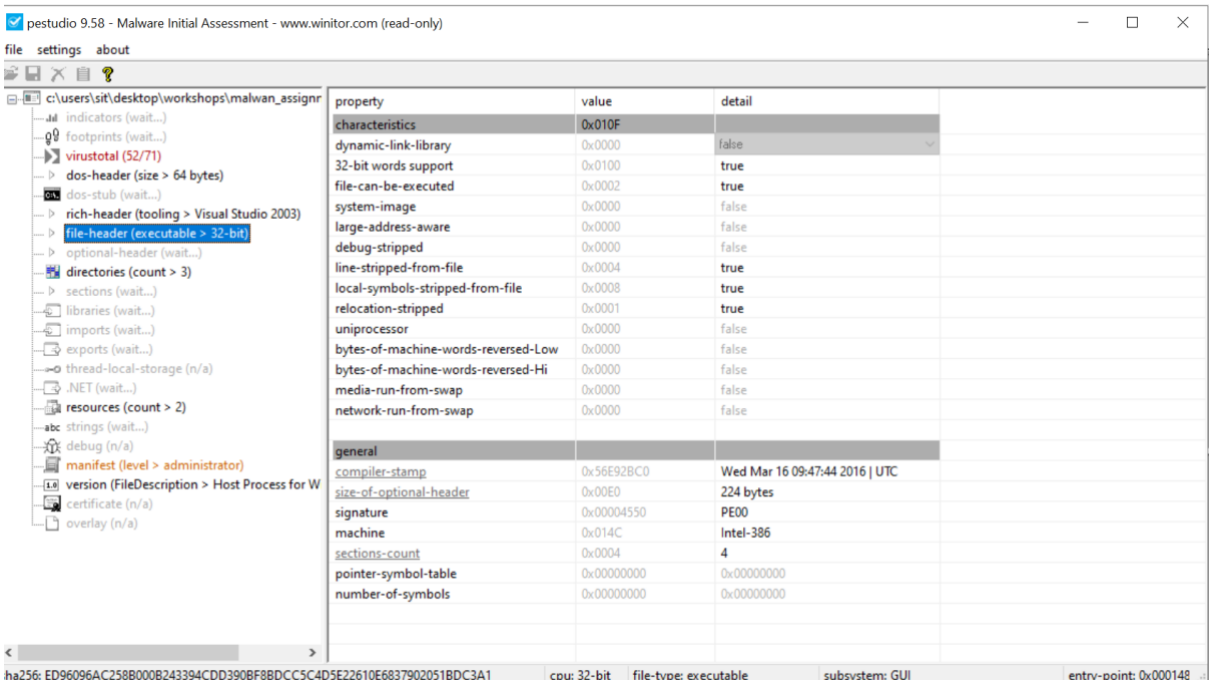
Property	Value
CompanyName	Microsoft Corporation
FileDescription	Host Process for Windows Services
FileVersion	6.1.7600.16385 (win7_rtm.090713-1255)
InternalName	svchost.exe
LegalCopyright	© Microsoft Corporation. All rights reserved.
OriginalFilename	svchost.exe
ProductName	Microsoft® Windows® Operating System

Using Cff explorer to now check the file itself.

File name is svchost, suggesting that it could be a trojan disguising as a legitimate file

I check the file name is gather further clues. Here the file name is shown to be as svchost this suggest that this programs is trying to masquerade as svchost file for the service host app on windows . It could imply that this program is a trojan meant to spoof users.

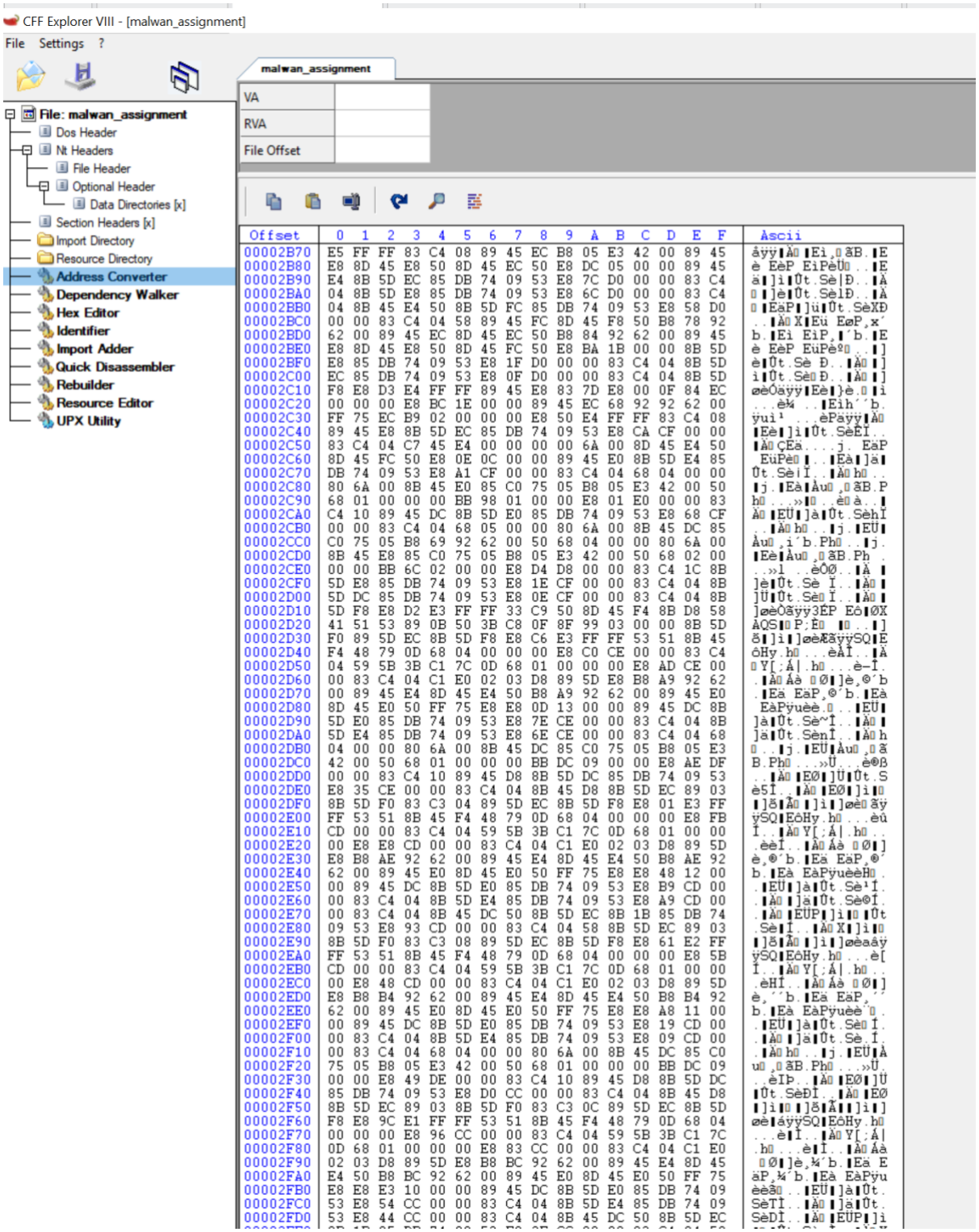
Results of PE Studio



Opening PE Studio led me to the file header. During the file header analysis, it has detected that the file header it uses is PE00 which suggest it is indeed an executable.

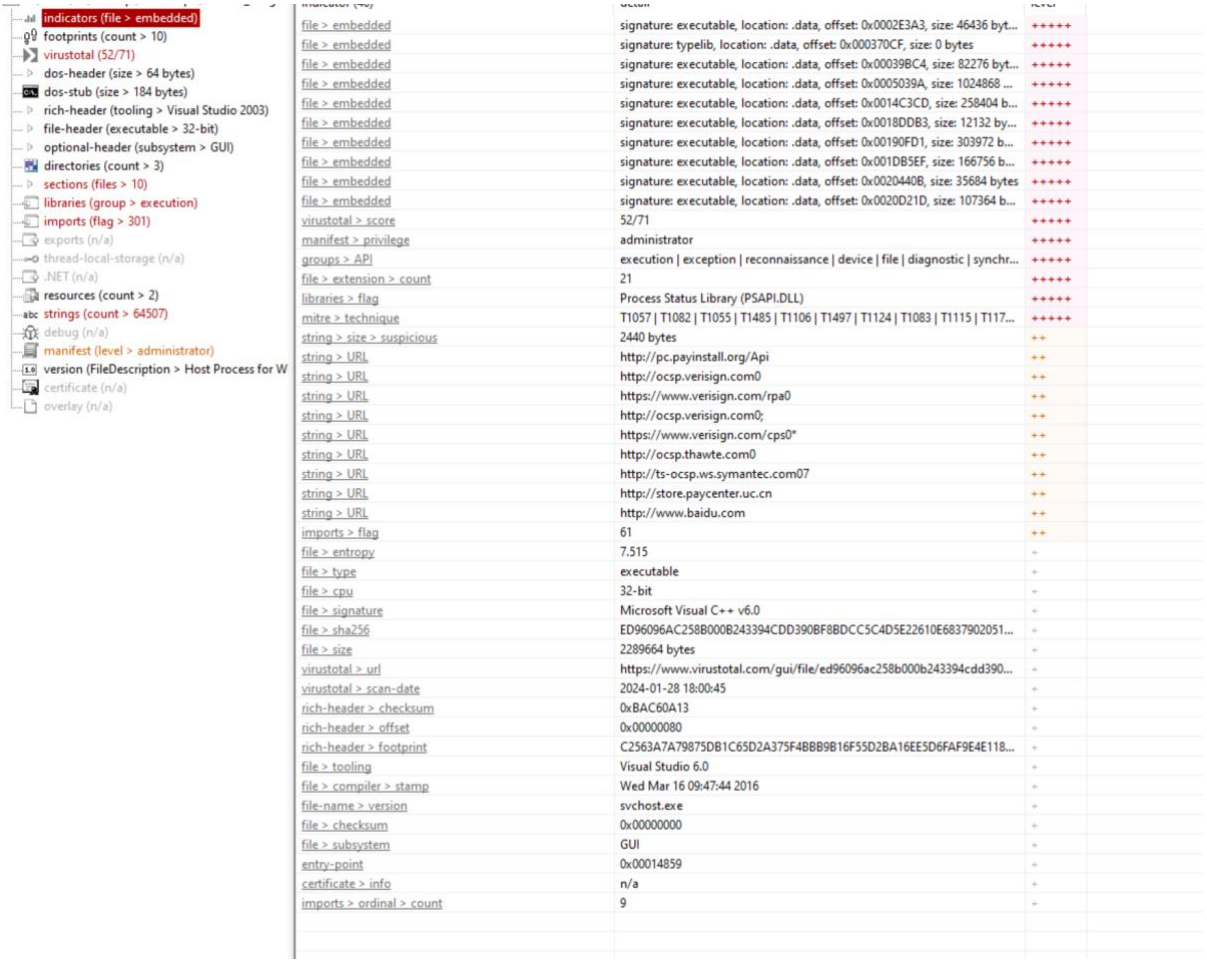
As we know that the program contains embedded packed programs that contains trojan like behaviours we would need to be careful handling the malware.

CFF Explorer Address Converter



Using CFF Explorer to check the address converter again, scrolling down shows us cryptic languages. These cryptic symbols suggest a packer is present.

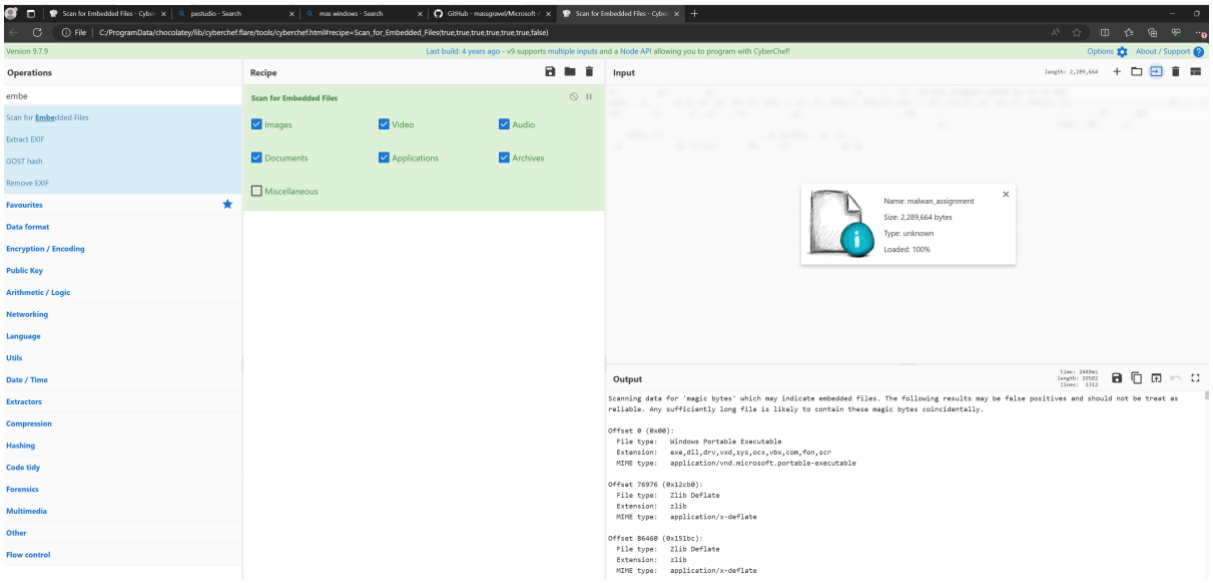
PEStudio Embedded file analysis.



If I were to check the static analysis once more there is indicators of embedded files. This solves the mystery of the packers detected by PEID.

It is believed that this malware appears to be a portable executable that unpacks packages within the malware like a trojan to do its true motives.

Verifying embedded files with cyberchef



To verify that there are embedded files, I used cyberchef to check.

First add the recipe, scan for embedded files. Next add the malware assignment into the cyberchef.

Looks like it has found various embedded files.

This suggest the malware we are dealing with is likely a trojan containing embedded files.

Extract (2 marks)

Identify at least 4 strings that are most relevant to its malicious properties/behaviours and explain why so.

Sample

Address	String	Details
0009AB50	SetWindowsHookExA	Used in keyloggers to hook keyboard input events
0009A24A	GetProcAddress	Retrieves the address of exported function
00170BF0	Filename: pas.txt	File name
00170558	*C:\Program Files\MSN Messenger\msnmsgr.exe	Potential program launched
00095BA0	/pas.txt	File path
00095BB4	www.ourgodfather.com	Website address

Eden analysis

Address	String	Details
0060D425	UPX0	Suggest that the program has a been packed or there is embedded files contained.
0060D44D	UPX1	Suggest that the program has a been packed or there is embedded files contained.
0060D5FD	UPX!	Suggest that the program has a been packed or there is embedded files contained.
0060460B	UPX0	Another file that is being packed Suggest that the program has a been packed or there are embedded files contained.
00604633	UPX1	Another file that is being packed Suggest that the program has a been packed or there are embedded files contained.
006047EB	UPX!	Another file that is being packed Suggest that the program has a been packed or there are embedded files contained.
006043EF	\\download\\zlib1.dll	Importing of a library that was not in the import directory
0057E5CD	GetProcAddress Failed, func_name	Retrieving address of exported function failed
00428950	FileNameW	FileName of a potential file
006292EF	http://www.baidu.com	Website of Baidu.com is present here
0042E2B9	cmd /c netsh firewall set opmode disable	Disables the firewall of the system. Possible to allow for further network attacks.

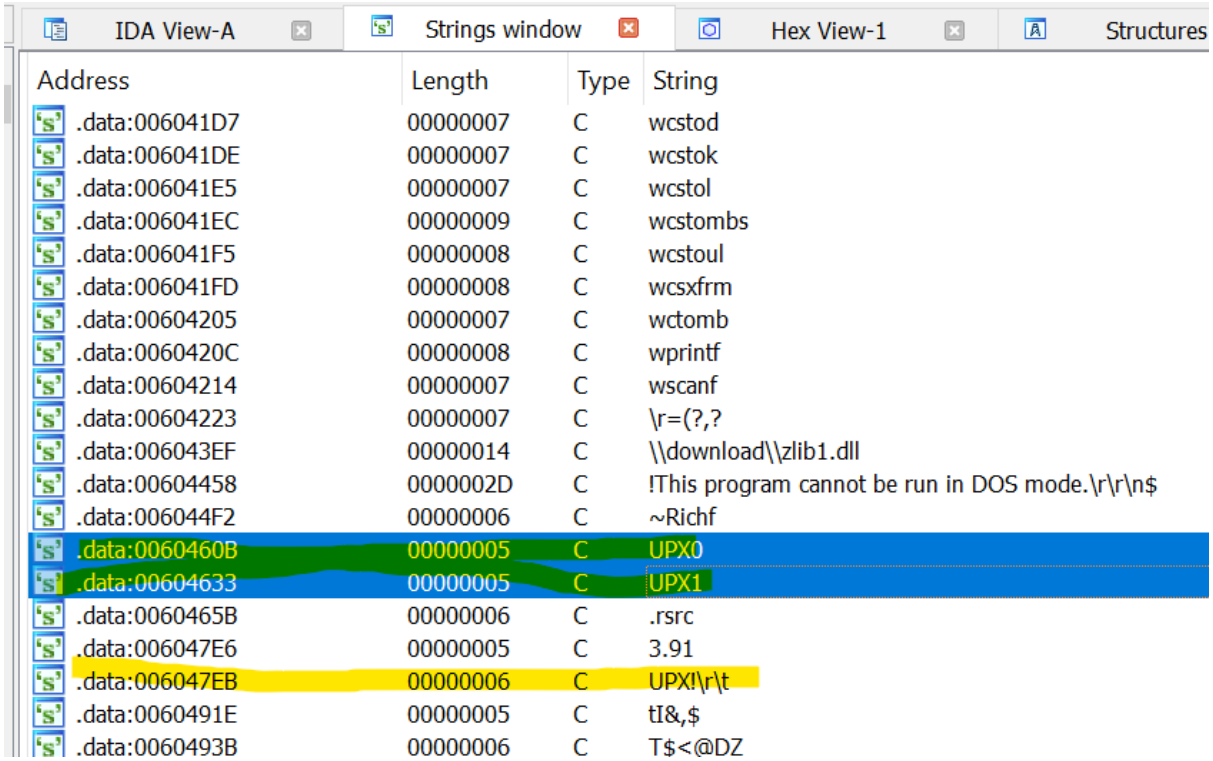
0054C3A3	\\download\\MiniThunderPlatform.exe	Suggest another executable is downloaded when the malicious program is run

Open IDA 70 Pro

UPX manual search Strings

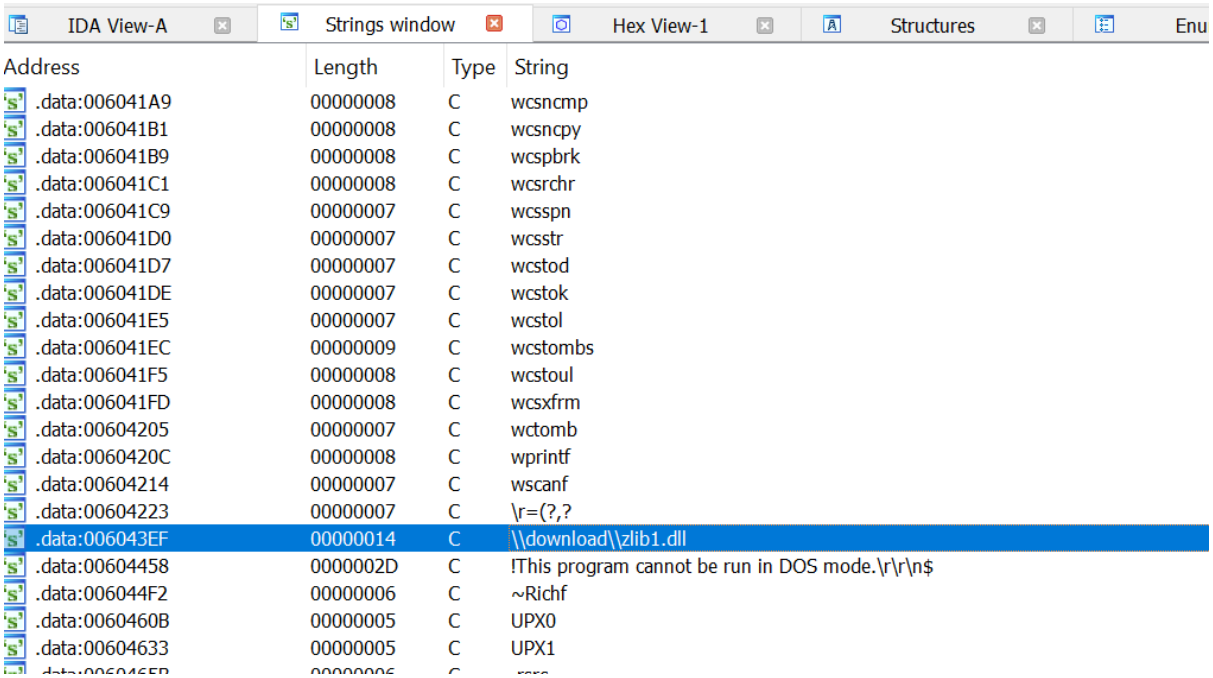
Address	Length	Type	String
.data:0060CFCC	0000000C	C	gzsetparams
.data:0060CFD8	00000007	C	gztell
.data:0060CFDF	00000009	C	gzungetc
.data:0060CFE8	00000008	C	gzwrite
.data:0060CFF0	00000008	C	inflate
.data:0060CFF8	0000000C	C	inflateBack
.data:0060D004	0000000F	C	inflateBackEnd
.data:0060D013	00000011	C	inflateBackInit_
.data:0060D024	0000000C	C	inflateCopy
.data:0060D030	0000000B	C	inflateEnd
.data:0060D03B	0000000E	C	inflateInit2_
.data:0060D049	0000000D	C	inflateInit_
.data:0060D056	0000000D	C	inflateReset
.data:0060D063	00000015	C	inflateSetDictionary
.data:0060D078	0000000C	C	inflateSync
.data:0060D084	00000011	C	inflateSyncPoint
.data:0060D095	0000000B	C	uncompress
.data:0060D0A0	00000007	C	zError
.data:0060D0A7	00000011	C	zlibCompileFlags
.data:0060D0B8	0000000C	C	zlibVersion
.data:0060D20B	0000000A	C	\\xldl.dll
.data:0060D26A	0000002D	C	!This program cannot be run in DOS mode.\r\r\n$
.data:0060D314	00000006	C	[Rich5
.data:0060D425	00000005	C	UPX0
.data:0060D44D	00000005	C	UPX1
.data:0060D475	00000006	C	.rsrc
.data:0060D5F8	00000005	C	3.91
.data:0060D5FD	00000008	C	UPX!\r\t\b\t
.data:0060D6FF	00000005	C	5\bp\nI

During my scrolling of the strings, I have found various strings suggesting UPX0 and UPX1 was used. This suggest that there are embedded files within the trojan that is yet to be unpacked when executed.



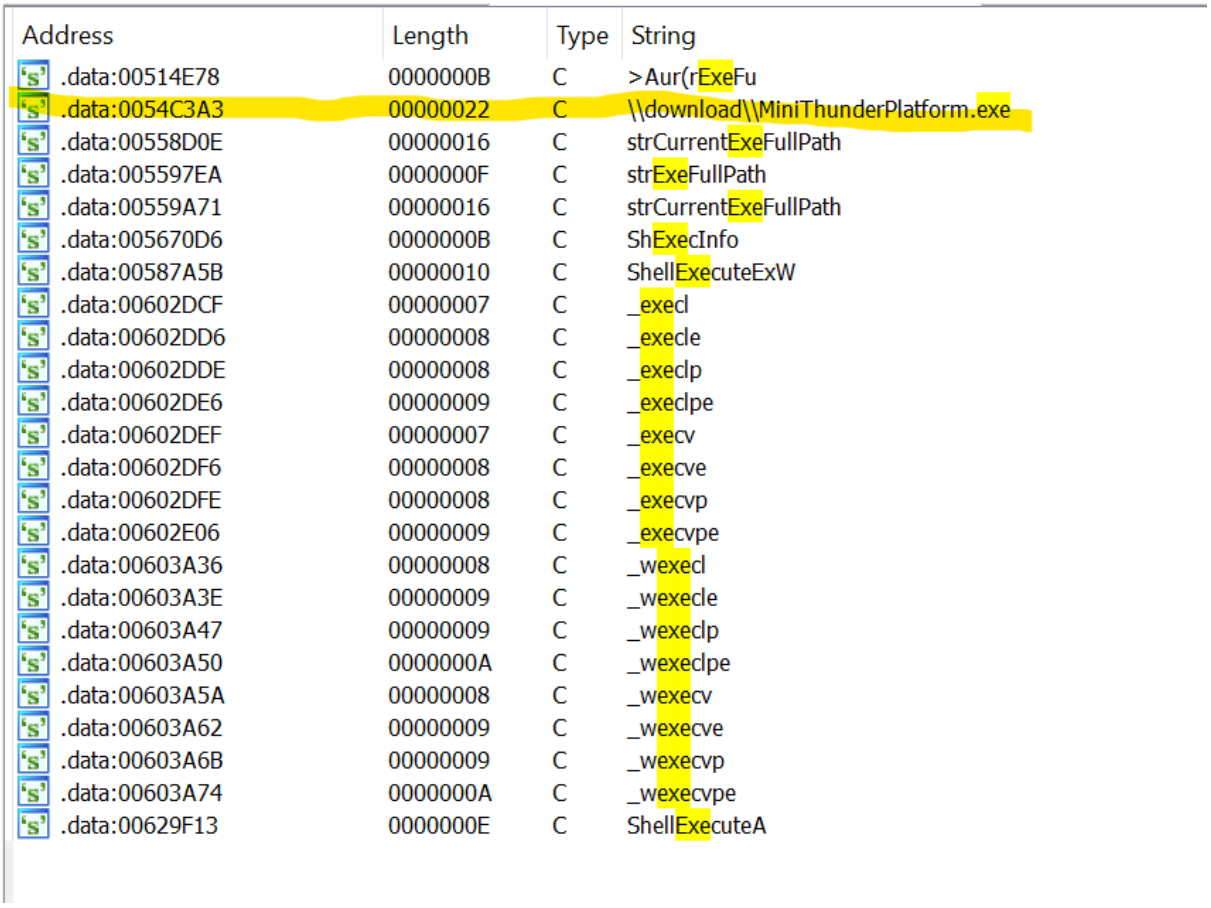
Further manual scrolling let me to see another instance of UPX0 UPX1.

Zlib.dll library being downloaded.



It seems that the malware is downloading external dll to help finish its execution. Perhaps there could be an embedded executable file within this trojan we do not yet discover.

Verifying for presence of EXE file



Address	Length	Type	String
.data:00514E78	0000000B	C	>Aur(rExeFu
.data:0054C3A3	00000022	C	\\download\\MiniThunderPlatform.exe
.data:00558D0E	00000016	C	strCurrentExeFullPath
.data:005597EA	0000000F	C	strExeFullPath
.data:00559A71	00000016	C	strCurrentExeFullPath
.data:005670D6	0000000B	C	ShExecInfo
.data:00587A5B	00000010	C	ShellExecuteExW
.data:00602DCF	00000007	C	_execl
.data:00602DD6	00000008	C	_execle
.data:00602DDE	00000008	C	_execlp
.data:00602DE6	00000009	C	_execlpe
.data:00602DEF	00000007	C	_execv
.data:00602DF6	00000008	C	_execve
.data:00602DFE	00000008	C	_execvp
.data:00602E06	00000009	C	_execvpe
.data:00603A36	00000008	C	_wexecl
.data:00603A3E	00000009	C	_wexecle
.data:00603A47	00000009	C	_wexeclp
.data:00603A50	0000000A	C	_wexeclpe
.data:00603A5A	00000008	C	_wexecv
.data:00603A62	00000009	C	_wexecve
.data:00603A6B	00000009	C	_wexecvp
.data:00603A74	0000000A	C	_wexecvpe
.data:00629F13	0000000E	C	ShellExecuteA

Using idapro, search for exe. Here it seems that it is downloading a program call minithunderplatform.exe.

Perhaps this is the malicious program within the trojan that would be executed.

Importing of functions

Address	Length	Type	String
.data:004392E3	0000000F	C	GetProcAddress
.data:005497C8	0000000F	C	GetProcAddress
.data:0057E5CD	00000023	C	GetProcAddress failed, func_name:
.data:0058768D	0000000F	C	GetProcAddress
.data:00590B3D	0000000F	C	GetProcAddress
.data:005A1A0D	0000000F	C	GetProcAddress
.data:005FFDFF	0000000F	C	GetProcAddress
.data:0060CC23	0000000F	C	GetProcAddress
.data:00627401	0000000F	C	GetProcAddress
.data:0062A002	0000000F	C	GetProcAddress

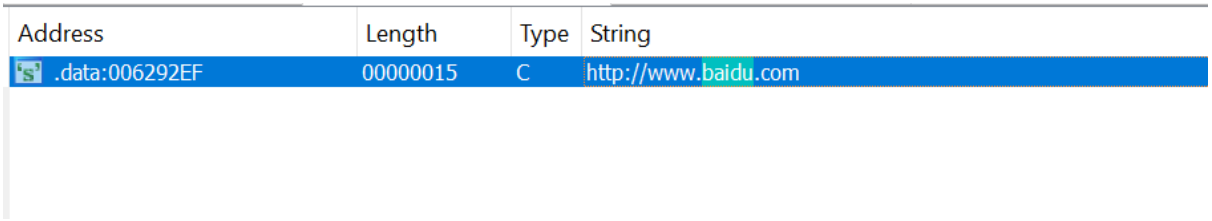
Here I run a string search for GetProcAddress, This is to verify for the importing of functions that the malware might use for malicious intent.

Filenames being imported.

Address	Length	Type	String
.rdata:00428950	0000000A	C	FileNameW
.rdata:0042895C	00000009	C	FileName
.data:00448CB4	0000000B	C	eFileNameA
.data:0054A0A6	00000013	C	get_final_filename
.data:0054A34A	0000000F	C	parse_filename
.data:005877B3	00000013	C	GetModuleFileNameW
.data:0058A7E5	00000013	C	GetModuleFileNameA
.data:00590E62	00000019	C	unzStringFileNameCompare
.data:00629DB8	00000013	C	GetModuleFileNameA
.data:00629DD7	00000012	C	PathFindFileNameA

Here I run idapro string search on filename, this is to check what files are being imported by the malware.

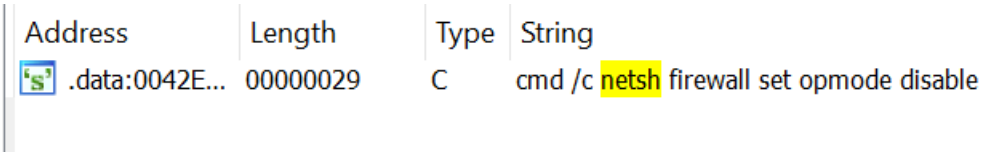
Baidu website being accessed



During my search, I found that the malware is accessing a website call www.baidu.com

It could be used for downloading or calling to a control centre of the malware.

Cmd disabling firewall



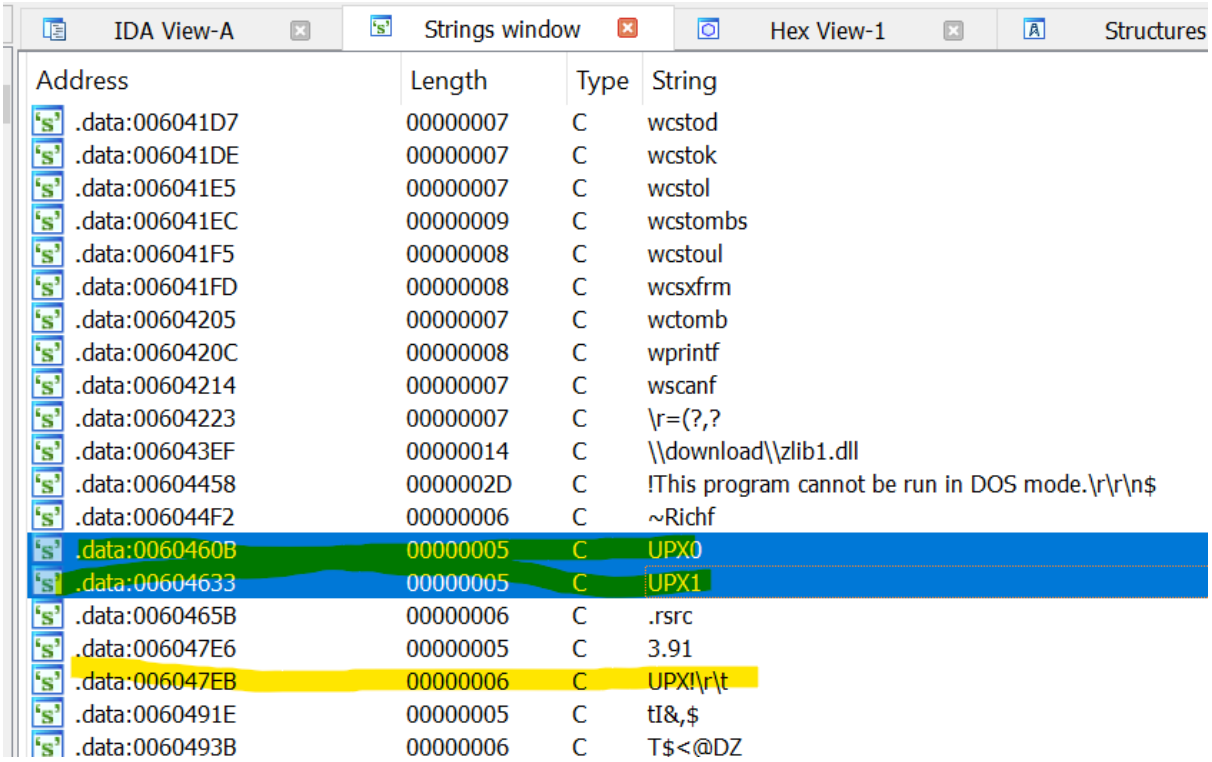
During my manual search I found that the malware uses administrative privileges to disable the firewall of the system. Perhaps it is used to download more malicious payload while evading firewall detection.

Reveal (2 marks)

Does the sample use any packing/obfuscation technique? Support your answer with reasons.

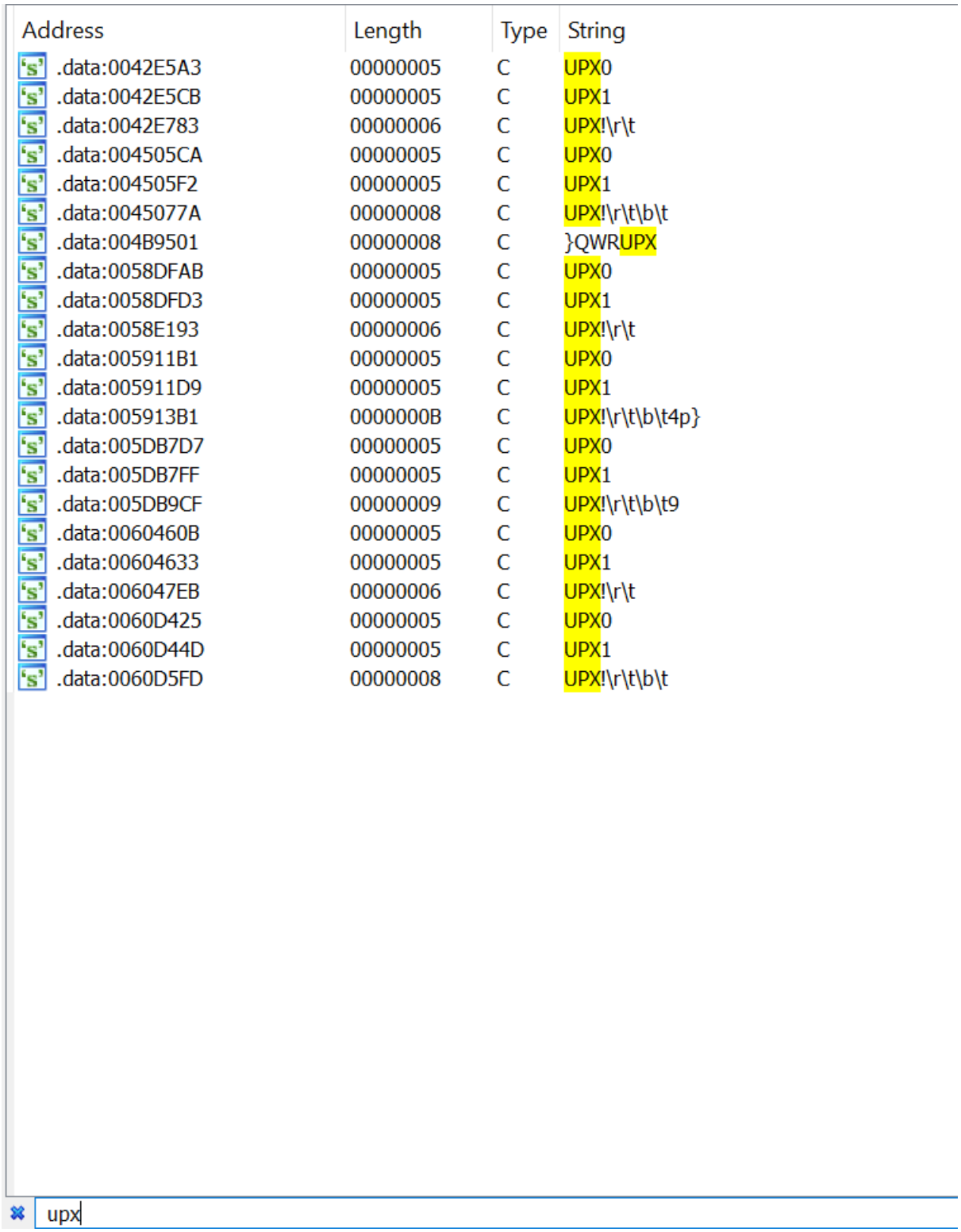
Yes the malware use plenty of packing and obfuscation techniques.

During my string search many instances of UPX0 and UPX1 has appeared.



Another instance of UPX0 UPX1 is seen again., This suggest that packers are used to obfuscate the true nature of the malware.

In strings of IDA pro-70



Address	Length	Type	String
.data:0042E5A3	00000005	C	UPX0
.data:0042E5CB	00000005	C	UPX1
.data:0042E783	00000006	C	UPX!\r\t
.data:004505CA	00000005	C	UPX0
.data:004505F2	00000005	C	UPX1
.data:0045077A	00000008	C	UPX!\r\t\b\t
.data:004B9501	00000008	C	}QWRUPX
.data:0058DFAB	00000005	C	UPX0
.data:0058DFD3	00000005	C	UPX1
.data:0058E193	00000006	C	UPX!\r\t
.data:005911B1	00000005	C	UPX0
.data:005911D9	00000005	C	UPX1
.data:005913B1	0000000B	C	UPX!\r\t\b\t4p}
.data:005DB7D7	00000005	C	UPX0
.data:005DB7FF	00000005	C	UPX1
.data:005DB9CF	00000009	C	UPX!\r\t\b\t9
.data:0060460B	00000005	C	UPX0
.data:00604633	00000005	C	UPX1
.data:006047EB	00000006	C	UPX!\r\t
.data:0060D425	00000005	C	UPX0
.data:0060D44D	00000005	C	UPX1
.data:0060D5FD	00000008	C	UPX!\r\t\b\t

upx

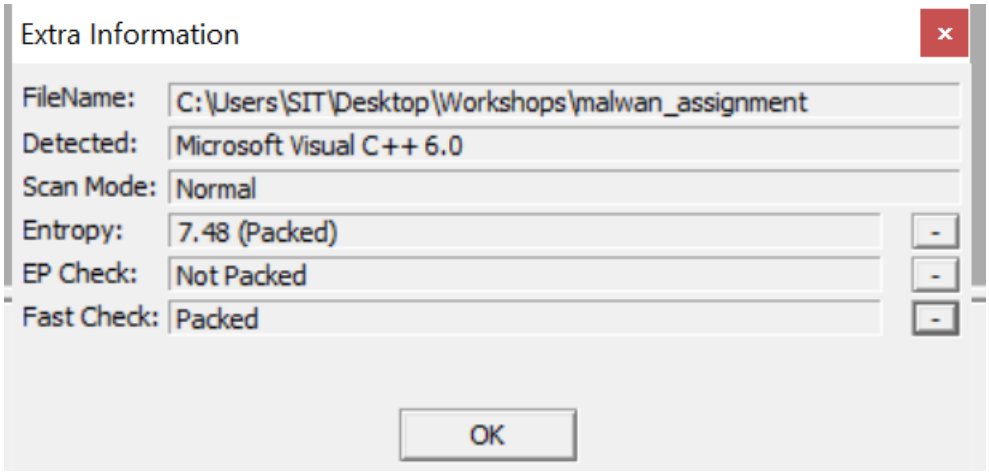
Search UPX

Here we found a lot of UPX files hidden within the executable.

It is likely this malware uses many packers to hide and obfuscate the codes.

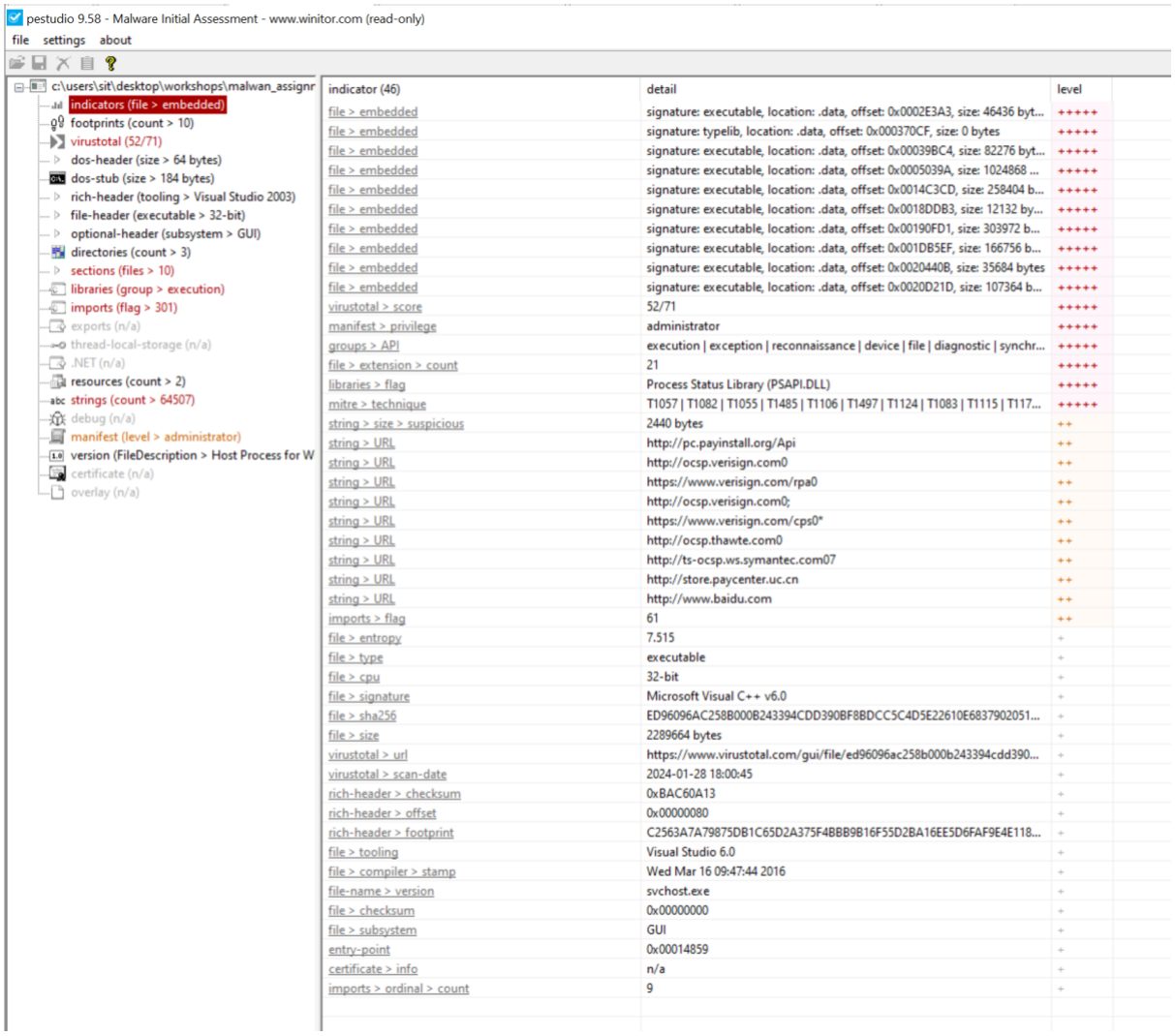
With so many UPX hidden within the file it could be that the malware we are dealing with is a trojan which contains many hidden malicious files within the file. This file will then be unpacked after evading malware detection and to unleash the malicious payloads onto the system.

Using PEiD to check for entropy



It gave a score of 7.48 which suggest that the executable is packed.

And when we referenced PEStudio, It suggest that many embedded files were detected.

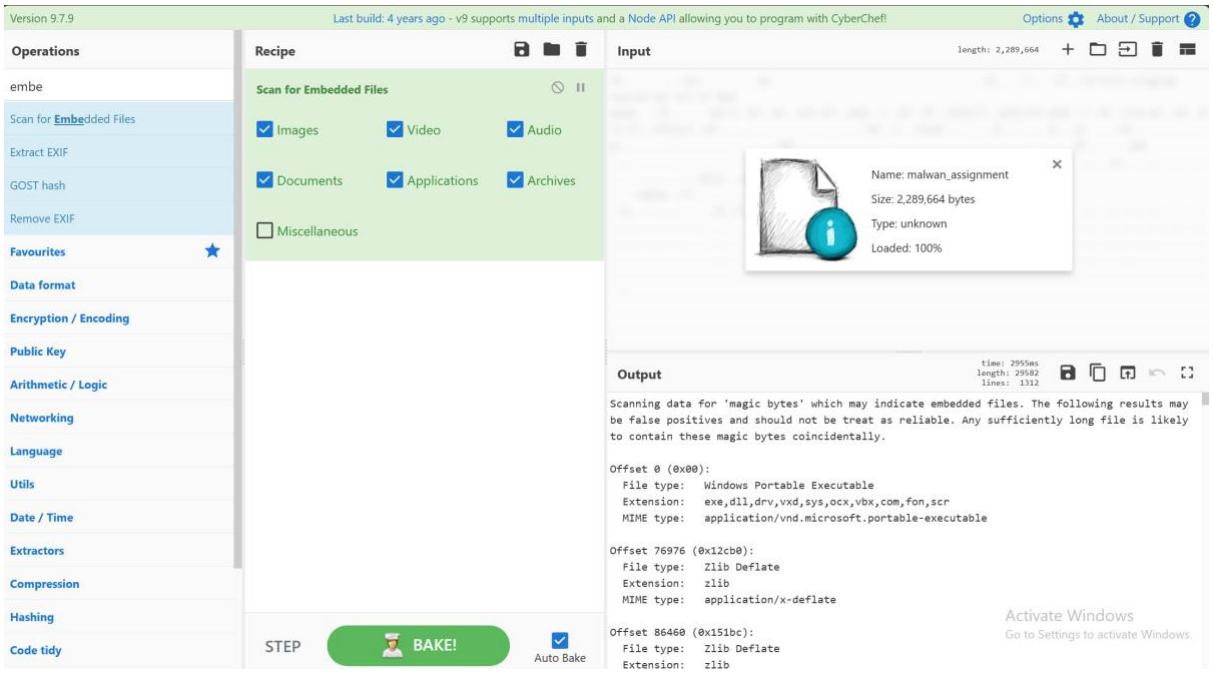


This further proves that the malware is doing obfuscation and packing techniques to evade detection.

Corelate/Research (1 mark)

Plenty of obfuscation techniques as seen earlier

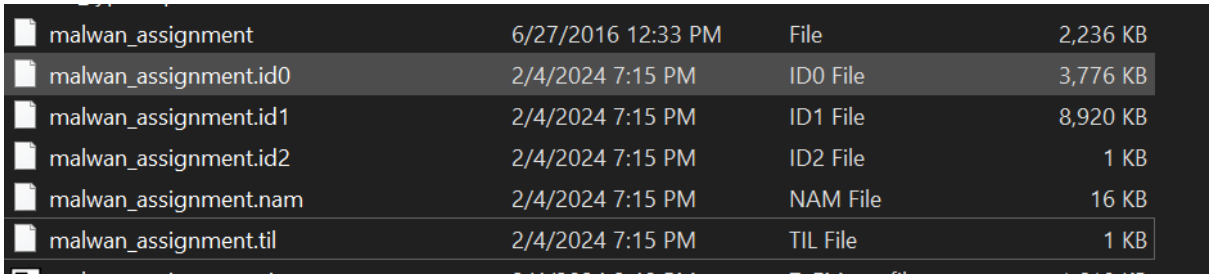
This led me to suspect that there could be embedded files. So, running cyberchef and loading the malware inside. I found plenty of reasons to believe that there are embedded files contained here. As seen by the cyberchef output many embedded files are found.



indicator (46)	detail	level
file > embedded	signature: executable, location: .data, offset: 0x0002E3A3, size: 46436 byt...	+++++
file > embedded	signature: typelib, location: .data, offset: 0x000370CF, size: 0 bytes	+++++
file > embedded	signature: executable, location: .data, offset: 0x00039BC4, size: 82276 byt...	+++++
file > embedded	signature: executable, location: .data, offset: 0x0005039A, size: 1024868 ...	+++++
file > embedded	signature: executable, location: .data, offset: 0x0014C3CD, size: 258404 b...	+++++
file > embedded	signature: executable, location: .data, offset: 0x0018DDB3, size: 12132 by...	+++++
file > embedded	signature: executable, location: .data, offset: 0x00190FD1, size: 303972 b...	+++++
file > embedded	signature: executable, location: .data, offset: 0x001DB5EF, size: 166756 b...	+++++
file > embedded	signature: executable, location: .data, offset: 0x0020440B, size: 35684 bytes	+++++
file > embedded	signature: executable, location: .data, offset: 0x0020D21D, size: 107364 b...	+++++
virustotal > score	52/71	+++++
manifest > privilege	administrator	+++++
groups > API	execution | exception | reconnaissance | device | file | diagnostic | synchr...	+++++
file > extension > count	21	+++++
libraries > flag	Process Status Library (PSAPI.DLL)	+++++
mitre > technique	T1057 | T1082 | T1055 | T1485 | T1106 | T1497 | T1124 | T1083 | T1115 | T117...	+++++
string > size > suspicious	2440 bytes	++
string > URL	http://pc.payinstall.org/Api	++
string > URL	http://ocsp.verisign.com0	++
string > URL	https://www.verisign.com/rpa0	++
string > URL	http://ocsp.verisign.com0;	++
string > URL	https://www.verisign.com/cps0*	++
string > URL	http://ocsp.thawte.com0	++
string > URL	http://ts-ocsp.ws.symantec.com07	++
string > URL	http://store.paycenter.uc.cn	++
string > URL	http://www.baidu.com	++
imports > flag	61	++

Using Pestudio I also found many embedded files contained. This verifies that cyberchef output is credible as well.

Random Files created during static analysis.



Summary

<In Summary, when the program is executed, a program that ..... The program also enumerated through the registry. This could be an attempt to obfuscate the intention of the program. >

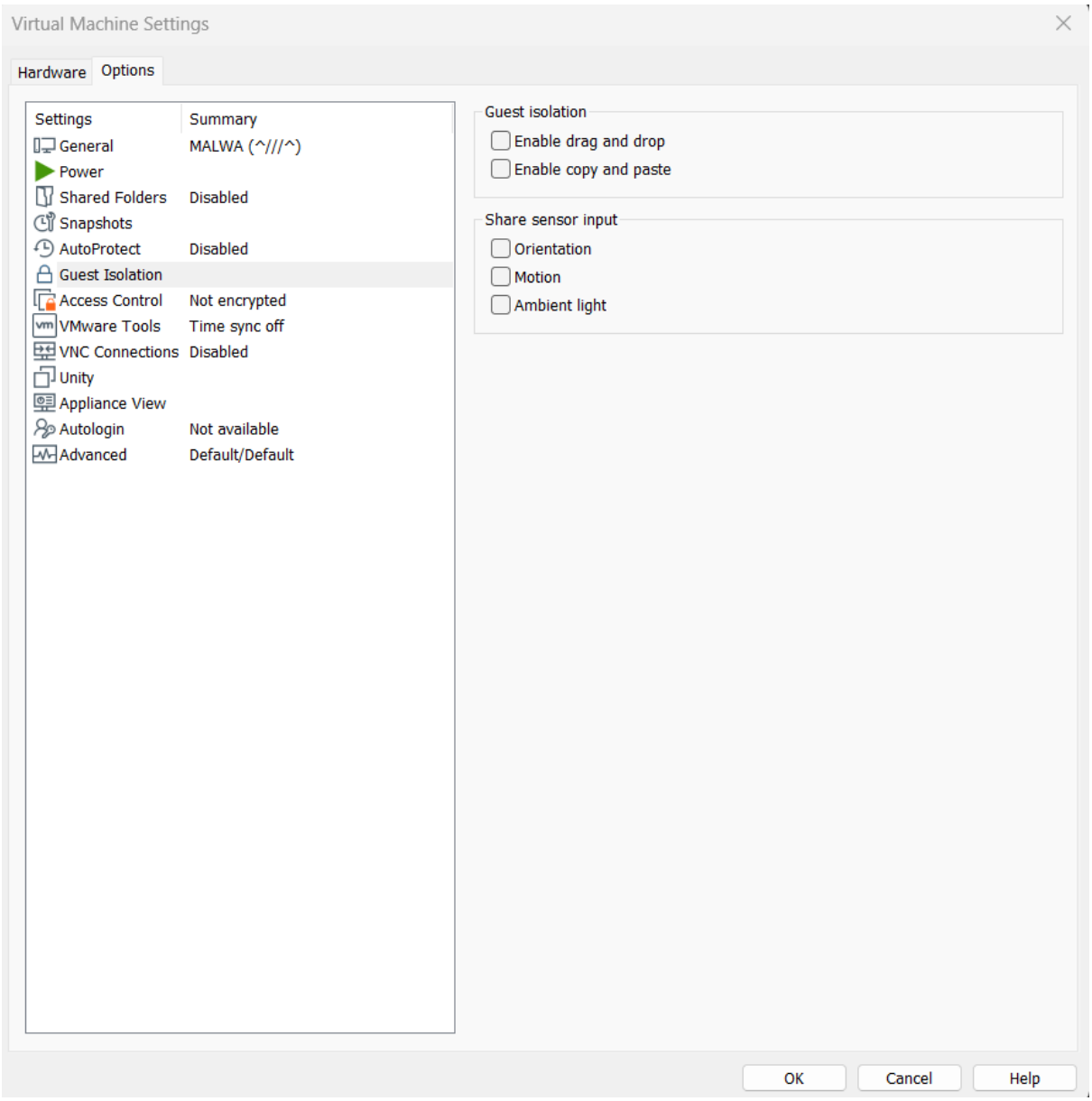
In all during my static analysis I can confirm that this malware is packed and if obfuscating the code of the program. During the disassembling process of strings, I have found that the malware has numerous packers and obfuscated code. It also referenced multiple filenames as well as connect to a few internet sites. It also disables the firewall of the system using administrative privileges.

In all this is likely a trojan.

We will have to dynamically analyse it for further information

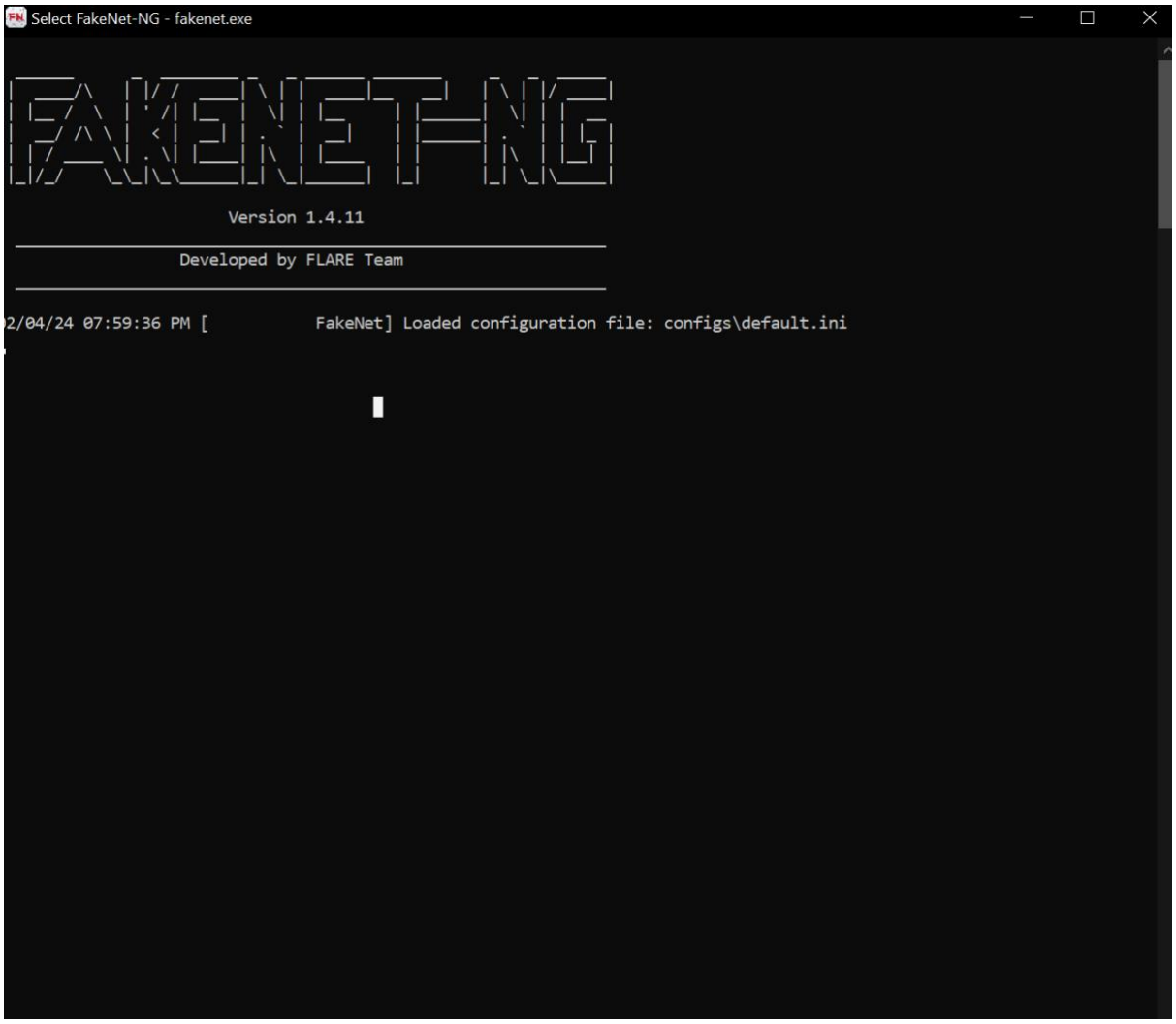
Behavioural Analysis (7 marks)

Before doing behavioural analysis ensure the vm is isolated from the system, off all NAT



This ensure that the malware only interacts in the sandbox environment. It also prevents the Malware from connecting to the actual internet

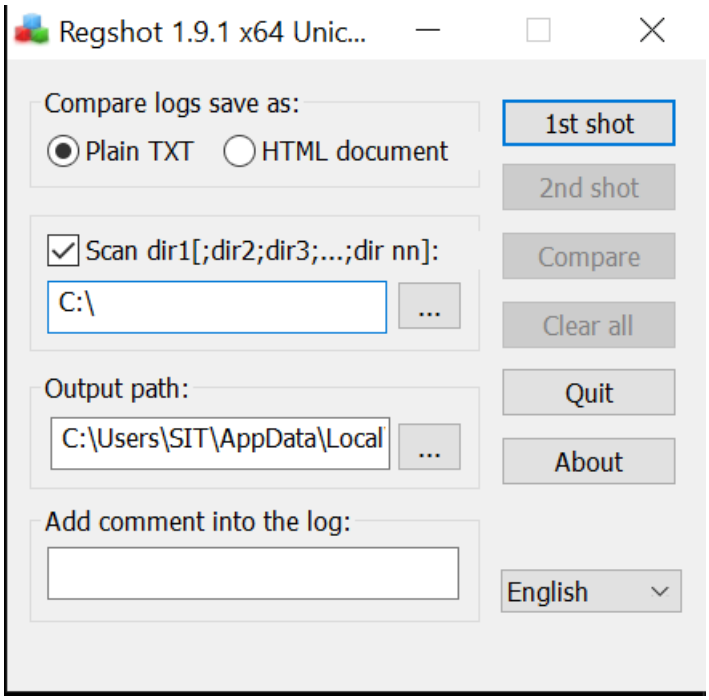
On Fakenet NG too ,



Run Fakenet-Ng to ensure that the malware is tricked that it is connected to the internet.

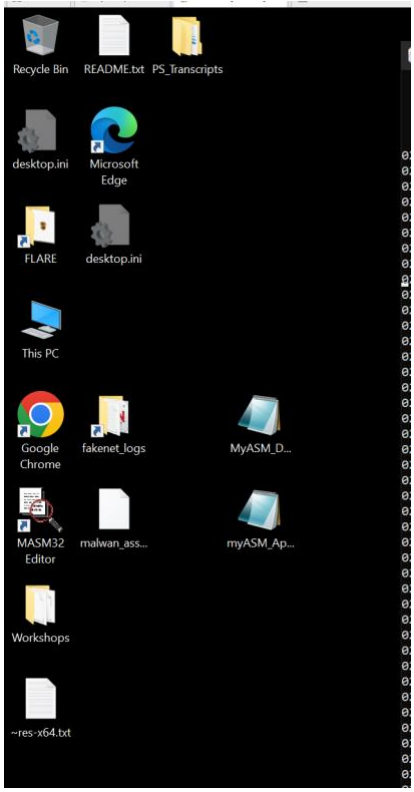
File System/Registry (2 marks)

Document how the sample interacts with the file system and registry

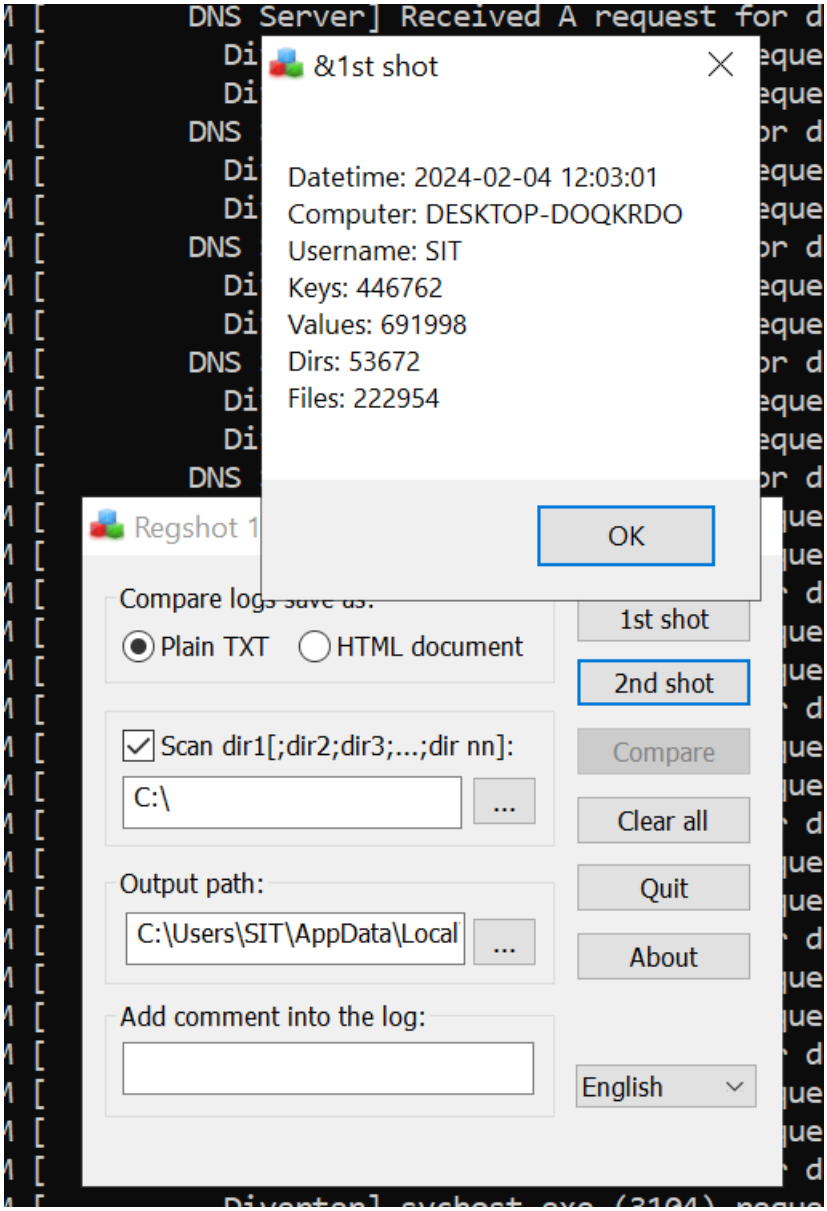


Configure Regshot to be like this, this ensure that regshot will capture the differences before the malware is activated and after the malware is activated.

Now Paste Malware onto desktop

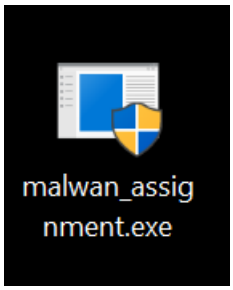


Then Run the first regshot



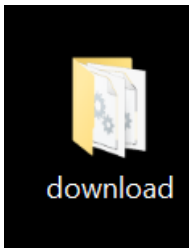
Result of the 1st regsshot. Once this is done proceed to the next step.

Now run the malware, to do so rename the malware to an executable extension. This allows the program to be run.

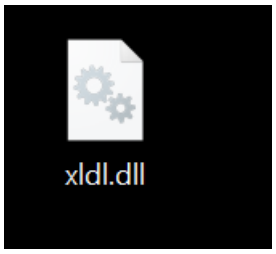


It will look like this. Notice how it requires administrative privileges to be run. This will come handy later on

Now run the malware, It will create some files



It seems to create a download folder



As well as a dll file. We will confirm this from the regshot later on.

Obtain the second regshot.

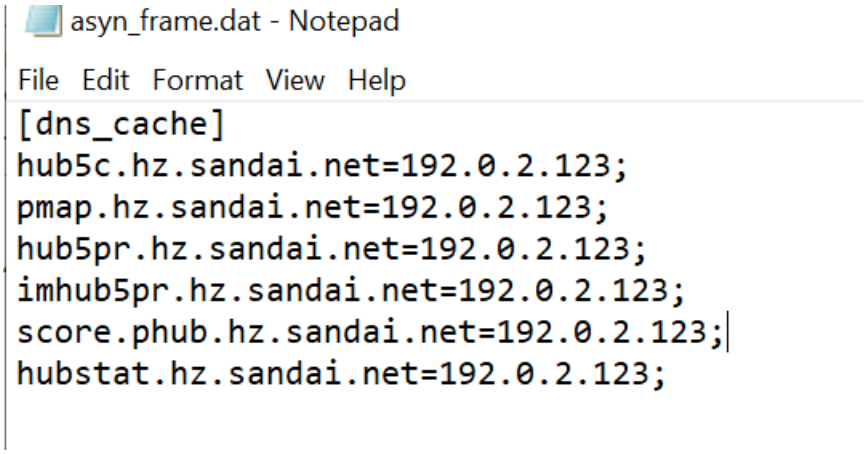
```
----------------------------------
Files added: 27
----------------------------------
C:\ProgramData\Thunder Network\DownloadLib\pub_store.dat
2024-02-04 12:05:13, 0x00002020, 133
C:\Tools\FakeNet-NG\fakenet1.4.11\http_20240204_200513.txt
2024-02-04 12:05:13, 0x00000020, 217
C:\Tools\FakeNet-NG\fakenet1.4.11\http_20240204_200515.txt
2024-02-04 12:05:15, 0x00000020, 217
C:\Users\All Users\Thunder Network\DownloadLib\pub_store.dat
2024-02-04 12:05:13, 0x00002020, 133
C:\Users\Public\Thunder Network\Mini_downloadlib\ODAwMDAzNjA=\Version_3_2_1_42\Profiles\asyn_frame.dat
2024-02-04 12:05:15, 0x00000020, 191
C:\Users\Public\Thunder Network\Mini_downloadlib\ODAwMDAzNjA=\Version_3_2_1_42\Profiles\error.dat
2024-02-04 12:05:13, 0x00000020, 122
C:\Users\Public\Thunder Network\Mini_downloadlib\ODAwMDAzNjA=\Version_3_2_1_42\Profiles\stat.dat
2024-02-04 12:06:11, 0x00000020, 494
C:\Users\SIT\AppData\Local\Microsoft\Windows\Caches\{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0x0000000000000024.db
2024-02-04 12:05:14, 0x00000020, 313568
C:\Users\SIT\AppData\Local\Packages\Microsoft.Windows.Search_cw5n1h2txyewy\LocalState\ConstraintIndex\Apps_{119c5bd3-438c-4d36-a44f-b3cef37852f8}\0.0.filtertrie.intermediate.txt
2024-02-04 12:05:15, 0x00000020, 34979
C:\Users\SIT\AppData\Local\Packages\Microsoft.Windows.Search_cw5n1h2txyewy\LocalState\ConstraintIndex\Apps_{119c5bd3-438c-4d36-a44f-b3cef37852f8}\0.1.filtertrie.intermediate.txt
2024-02-04 12:05:15, 0x00000020, 5
C:\Users\SIT\AppData\Local\Packages\Microsoft.Windows.Search_cw5n1h2txyewy\LocalState\ConstraintIndex\Apps_{119c5bd3-438c-4d36-a44f-b3cef37852f8}\0.2.filtertrie.intermediate.txt
2024-02-04 12:05:15, 0x00000020, 5
C:\Users\SIT\AppData\Local\Packages\Microsoft.Windows.Search_cw5n1h2txyewy\LocalState\ConstraintIndex\Apps_{119c5bd3-438c-4d36-a44f-b3cef37852f8}\Apps.ft
2024-02-04 12:05:15, 0x00000020, 46624
C:\Users\SIT\AppData\Local\Packages\Microsoft.Windows.Search_cw5n1h2txyewy\LocalState\ConstraintIndex\Apps_{119c5bd3-438c-4d36-a44f-b3cef37852f8}\Apps.index
2024-02-04 12:05:15, 0x00000020, 1127220
C:\Users\SIT\AppData\Local\Packages\Microsoft.Windows.Search_cw5n1h2txyewy\LocalState\DeviceSearchCache\AppCache133515219145990165.txt
2024-02-04 12:05:15, 0x00000020, 268220
C:\Users\SIT\Desktop\download\at171.dll
2024-02-04 12:05:11, 0x00000020, 47104
C:\Users\SIT\Desktop\download\dl_peer_id.dll
2024-02-04 12:05:11, 0x00000020, 92080
C:\Users\SIT\Desktop\download\download_engine.dll
2024-02-04 12:05:11, 0x00000020, 1032136
C:\Users\SIT\Desktop\download\id.dat
2024-02-04 12:05:11, 0x00000020, 40
C:\Users\SIT\Desktop\download\MiniThunderPlatform.exe
2024-02-04 12:05:11, 0x00000020, 268744
```

Here are the files added. Looks like there is quite a lot files. This matches with the embedded files signature we found from PEStudio.

```
2024-02-04 12:05:11, 0x00000020, 268744
C:\Users\SIT\Desktop\download\minizip.dll
2024-02-04 12:05:11, 0x00000020, 12800
C:\Users\SIT\Desktop\download\msvcp71.dll
2024-02-04 12:05:11, 0x00000020, 304640
C:\Users\SIT\Desktop\download\msvcr71.dll
2024-02-04 12:05:11, 0x00000020, 167424
C:\Users\SIT\Desktop\download\zlib1.dll
2024-02-04 12:05:11, 0x00000020, 36352
C:\Users\SIT\Desktop\malwan_assignment.exe
2016-06-27 04:33:24, 0x00000020, 2289664
C:\Users\SIT\Desktop\xldl.dll
2024-02-04 12:05:11, 0x00000020, 114632
C:\Windows\Prefetch\MALWAN_ASSIGNMENT.EXE-B359F6F2.pf
2024-02-04 12:05:20, 0x00002020, 8607
C:\Windows\Prefetch\MINITHUNDERPLATFORM.EXE-738FA0AA.pf
2024-02-04 12:05:21, 0x00002020, 7113
```

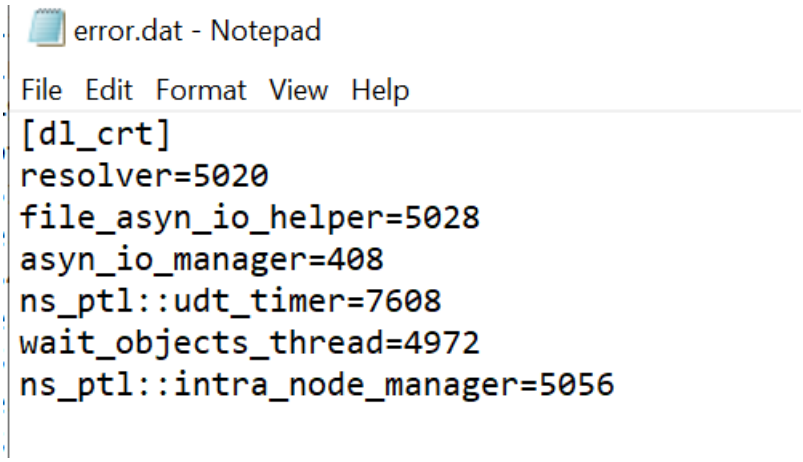
Let's look at what the files the malware has created do.

Asyn_frame.dat

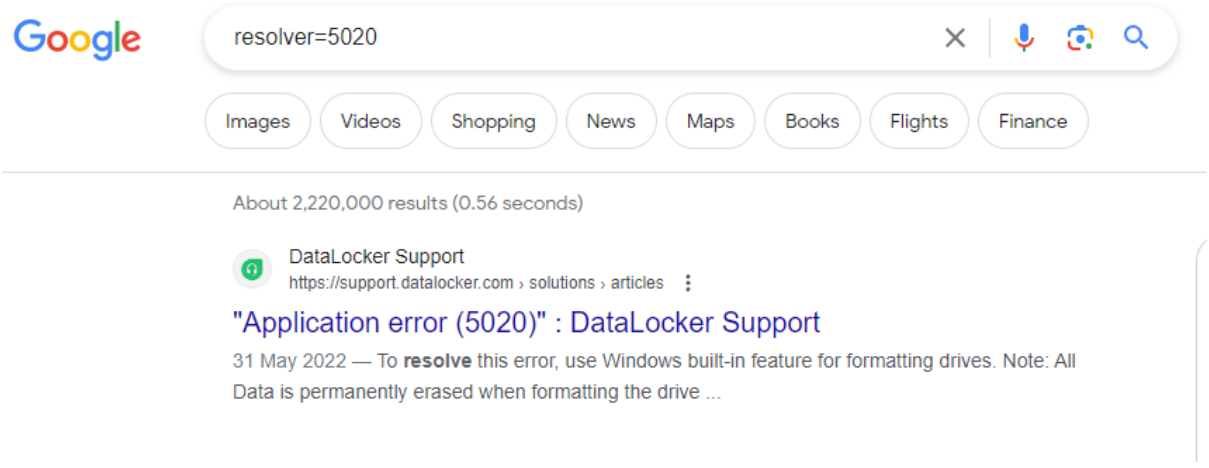


It seems to create the DNS resolution to connect back to. This address could be the command centre for the malware to be created.

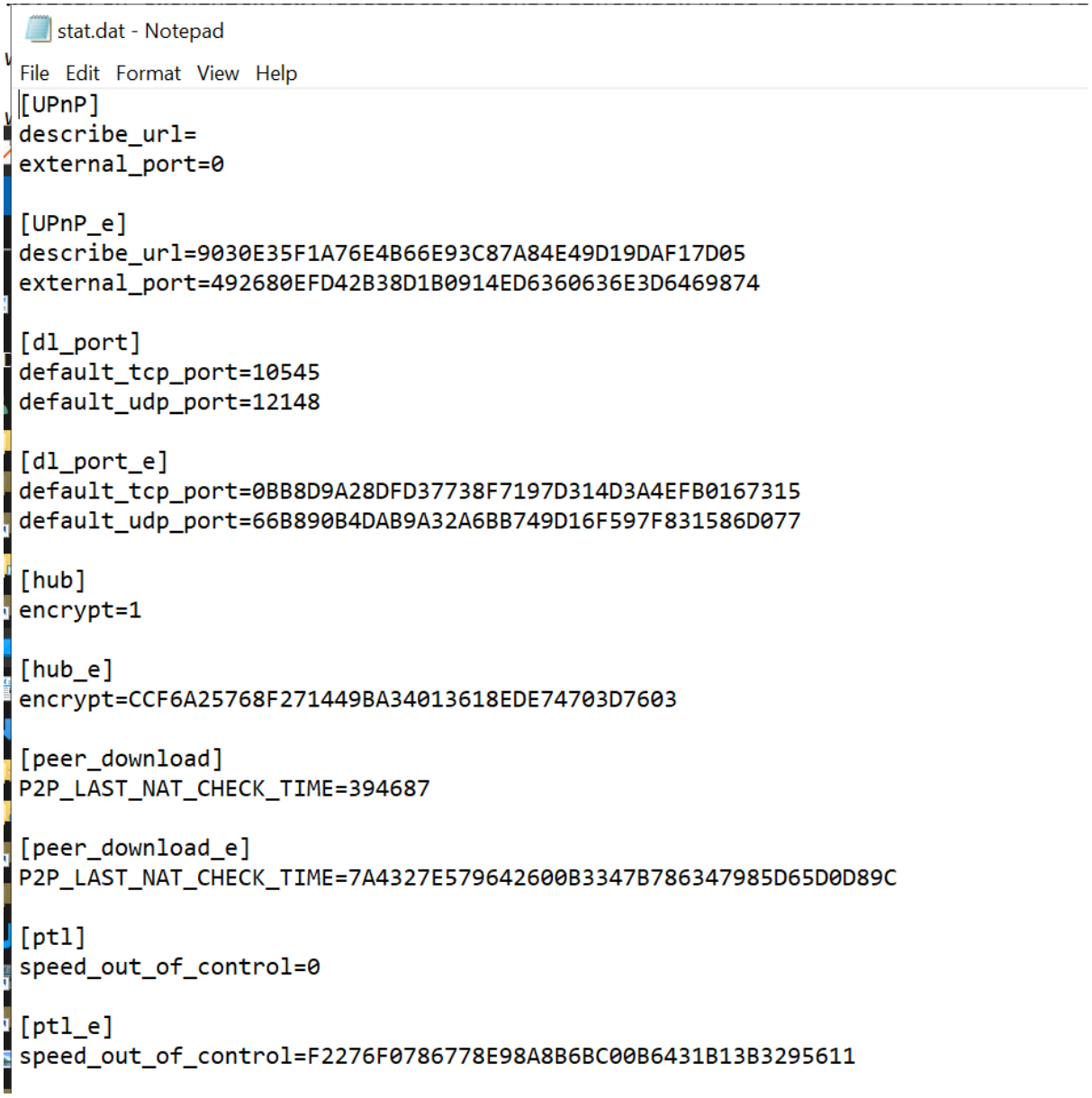
Error.dat



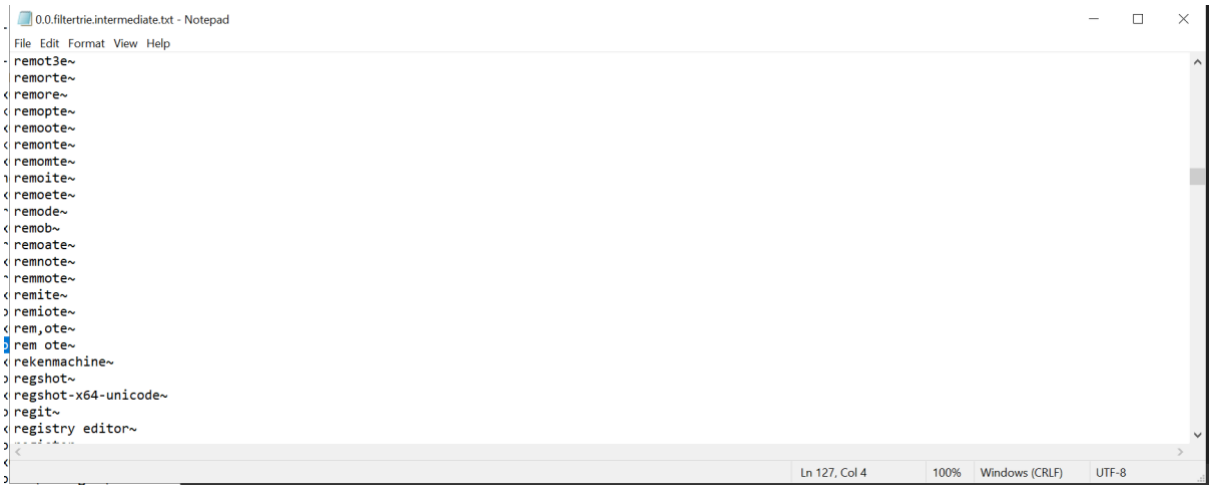
Likely configuration of the malware for any error notifications. Searching the error online reveals that these are error codes.



Stat.dat

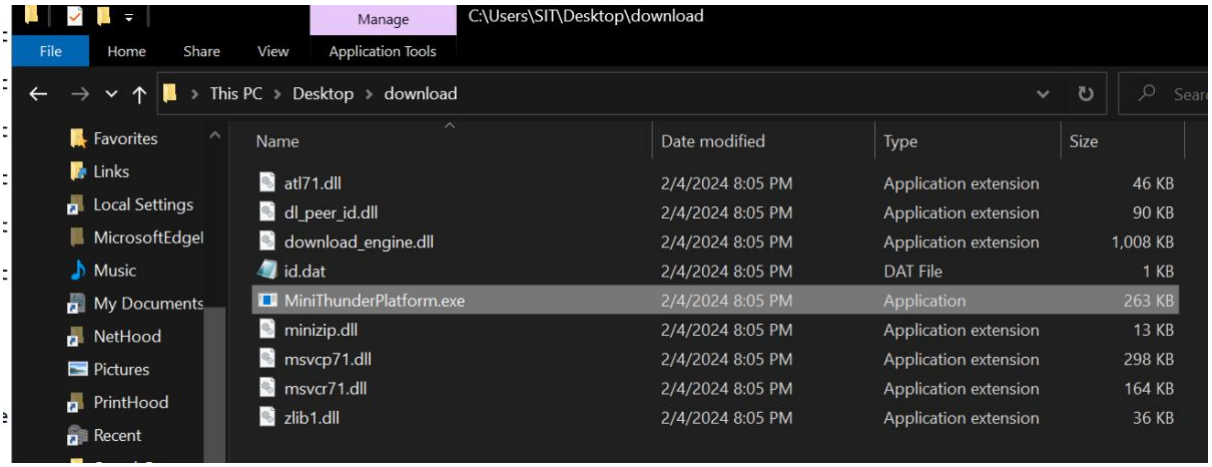


This is the configuration file for the P2P sharing, likely this file belongs to the minithunderplatform executable. I notice that file allows for smooth configuration to the platform sharing it is trying to connect. It appears that this file is creating a P2P client exchange for a malware.



Opening the intermediate file suggest some files being opened. I'm not sure what this file suggest.

Creation of a download folders containing some files



Notice how the minithunderplatform executable is shown here. Likely these are the fiies needed to support this executable to work.

Opening id.dat

Reveals that this is the client id for this infected computer. It even state the version of this minithunderplatform.

Searching google for minithunderplatform, it seems to turn our computer into a P2P sharing client sharing data to other clients trying to download.

file.net

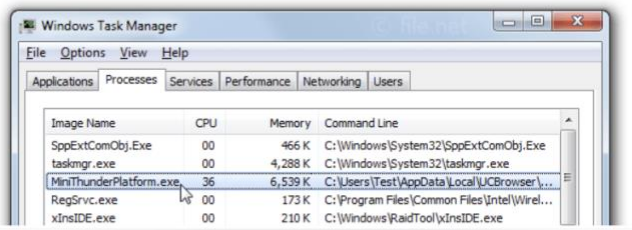
Home Files Software News Contact

What is MiniThunderPlatform.exe?

The .exe extension on a filename indicates an executable file. Executable files may, in some cases, harm your computer. Therefore, please read below to decide for yourself whether the MiniThunderPlatform.exe on your computer is a Trojan that you should remove, or whether it is a file belonging to the Windows operating system or to a trusted application.

Click to Run a Free Scan for MiniThunderPlatform.exe related errors

MiniThunderPlatform.exe file information



MiniThunderPlatform.exe process in Windows Task Manager

The process belongs to software Driver Talent or DriveTheLife by unknown.

Description: MiniThunderPlatform.exe is not essential for Windows and will often cause problems. MiniThunderPlatform.exe is located in a subfolder of the user's profile folder or sometimes in a subfolder of Windows folder for temporary files—e.g.

C:\Users\USERNAME\AppData\Local\UCBrowser\User Data_i18n\Thunder\1.0.0.0\download or *C:\Users\USERNAME\AppData\Roaming\Xiaomi\MiPhoneManager\Plugin\xunlei\download*. Known file sizes on Windows 10/11/7 are 268,744 bytes (88% of all occurrences) or 272,840 bytes.
The MiniThunderPlatform.exe file is a Verisign signed file. The file is not a Windows system file. The program has no visible window. The MiniThunderPlatform.exe file is certified by a trustworthy company. The software uses ports to connect to or from a LAN or the Internet. MiniThunderPlatform.exe is able to monitor applications. Therefore the technical security rating is *67% dangerous*; however you should also read the user reviews.

Recommended: Identify MiniThunderPlatform.exe related errors

- If MiniThunderPlatform.exe is located in a subfolder of "C:\Program Files", the security rating is *43% dangerous*. The file size is 248,264 bytes (75% of all occurrences), 272,840 bytes or 268,744 bytes. The file is not a Windows system file. The software listens for or sends data on open ports to a LAN or the Internet. The program is not visible. The file is a Verisign signed file. It is certified by a trustworthy company. MiniThunderPlatform.exe is able to monitor applications.

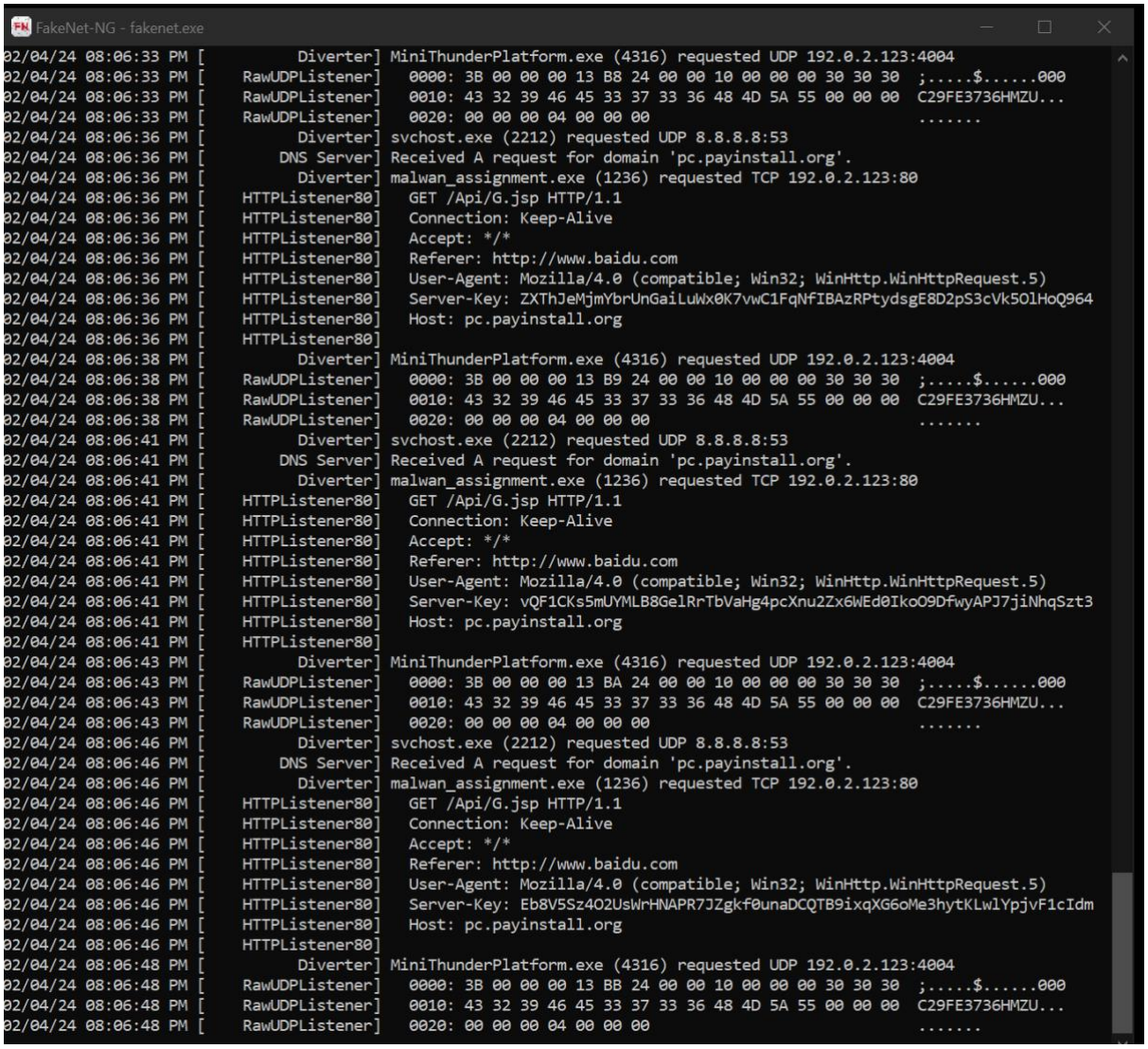
  Uninstalling this variant: In the event of any problems with MiniThunderPlatform.exe, you might want to ask Customer Support to assist you or uninstall *Driver Talent* or *DriveTheLife* from your computer using the Control Panel applet Uninstall a Program.

This suggest the trojan used is meant to be a staging platform for malicious activities later.

Network (2 marks)

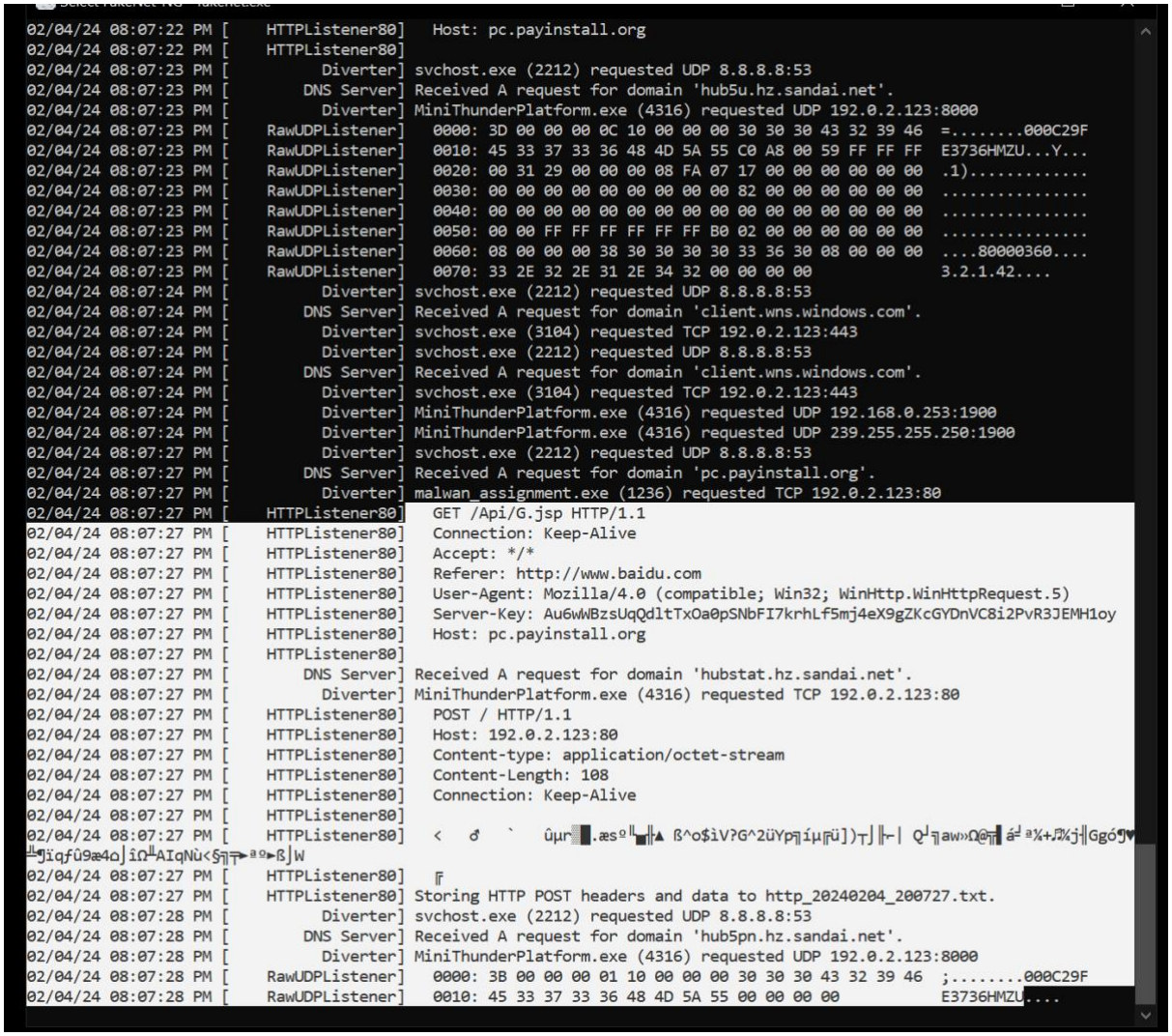
Document the sample's network activities

The malware appears to keep going to the browser Baidu.com and searching pc.pay



I am not sure what it intends to do once it goes pc.payinstall.org.

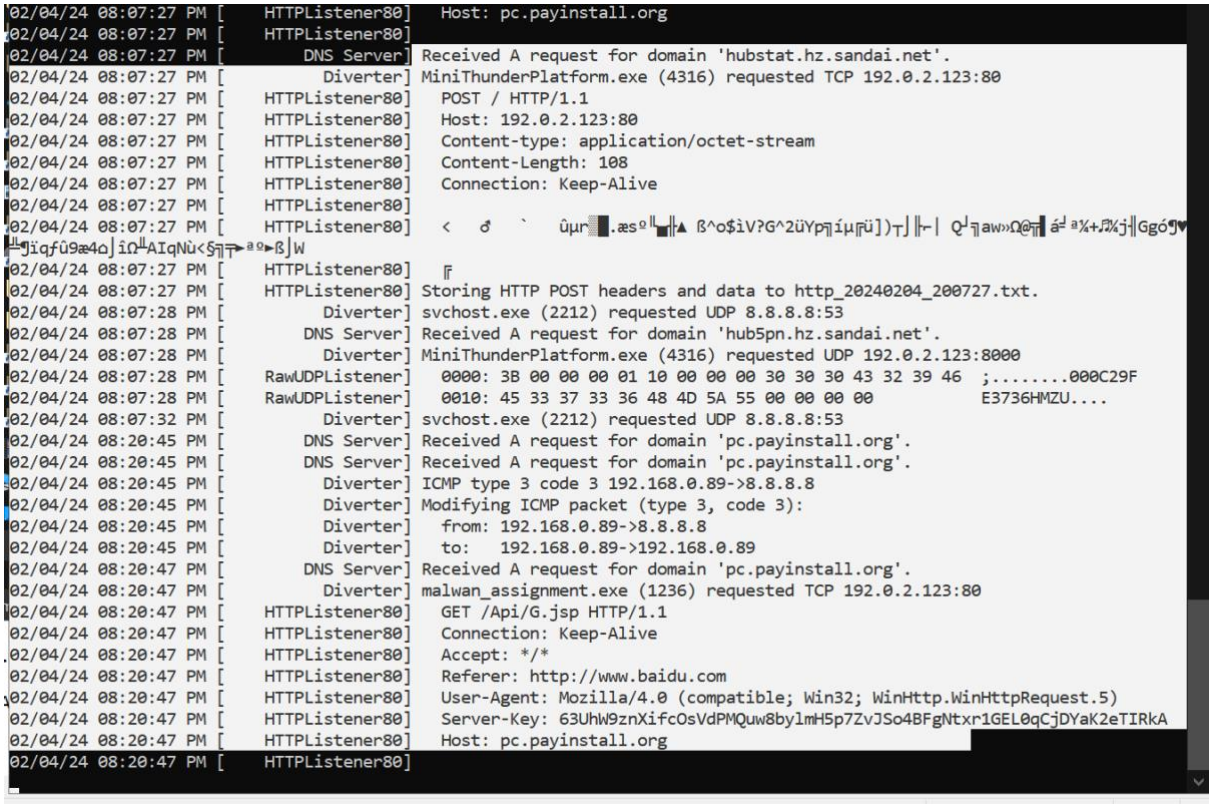
Perhaps its trying to install malicious programs into the computer to do further actions.



Letting the program run, it keeps going to pc.payinstall.org

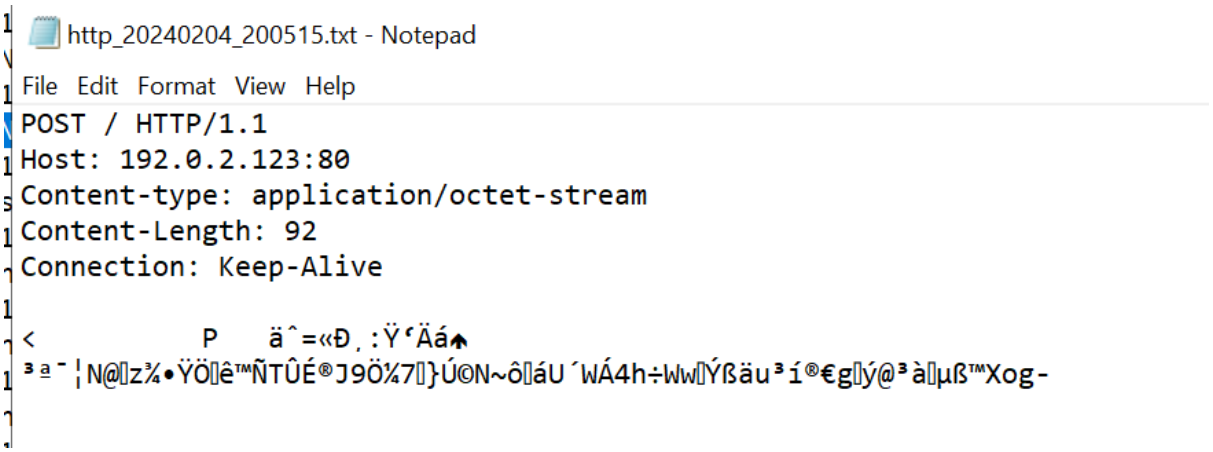
Afterwards it goes to hubstat.hz.sandai.net.

It sends an encrypted message over to the file. This suggest it could be communicating something but I am not sure based on the encrypted string.



Seems like it is doing some activities. That first begin with requesting for hubstat.hz.sanda.net.

Then it sent this data to a txt file

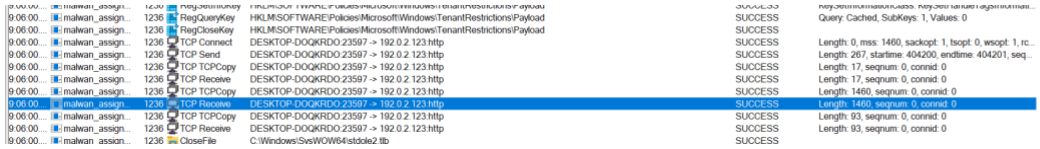


It is an encrypted message.

Process (2 marks)

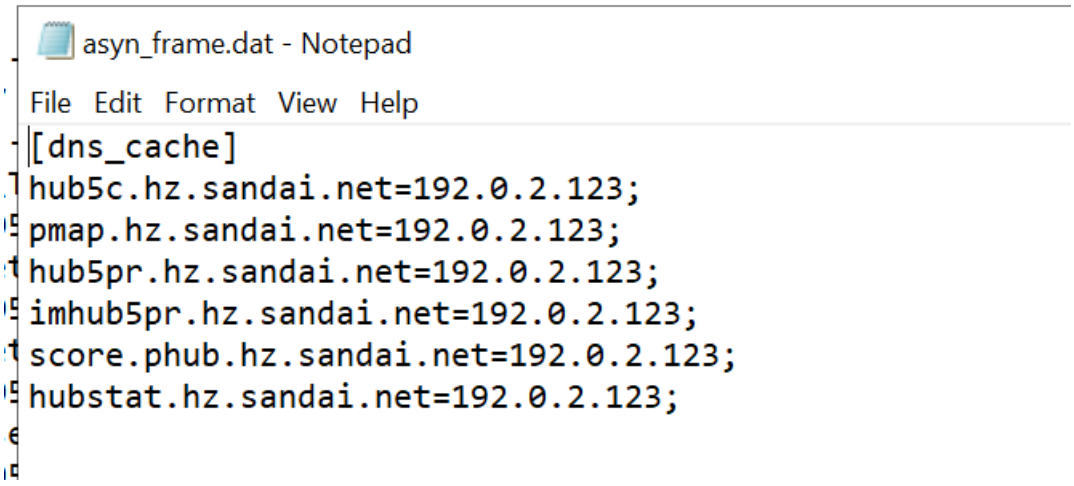
Document the sample's process activities.

Process Monitor



Running Process monitor, it suggest that the program is communicating to this IP address

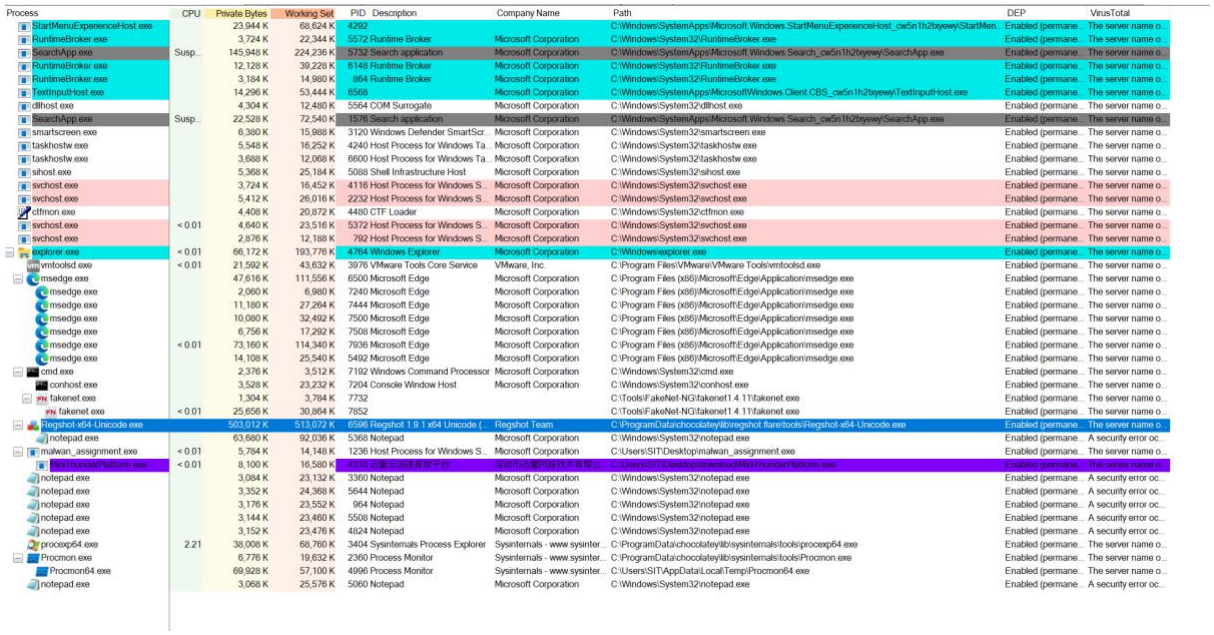
Attempts to communicate to this IP address which is likely to be



As we recall earlier in the DNS files, this ip address belongs to one of these sites.

Other findings include, Connroutehelper might be a dll that helps to navigate the malware to the right connection.

Process explorer



Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Path	DEP	VirusTotal
StartMenuExperienceHost.exe		23,944 K	68,624 K	4292			C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMen...	Enabled (permane...	The server name o...
RuntimeBroker.exe		3,724 K	22,344 K	5572	Runtime Broker	Microsoft Corporation	C:\Windows\System32\RuntimeBroker.exe	Enabled (permane...	The server name o...
SearchApp.exe	Susp...	145,948 K	224,236 K	5732	Search application	Microsoft Corporation	C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe	Enabled (permane...	The server name o...
RuntimeBroker.exe		12,128 K	39,228 K	6148	Runtime Broker	Microsoft Corporation	C:\Windows\System32\RuntimeBroker.exe	Enabled (permane...	The server name o...
RuntimeBroker.exe		3,184 K	14,980 K	864	Runtime Broker	Microsoft Corporation	C:\Windows\System32\RuntimeBroker.exe	Enabled (permane...	The server name o...
TextInputHost.exe		14,296 K	53,444 K	6568		Microsoft Corporation	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\TextInputHost.exe	Enabled (permane...	The server name o...
dllhost.exe		4,304 K	12,480 K	5564	COM Surrogate	Microsoft Corporation	C:\Windows\System32\dllhost.exe	Enabled (permane...	The server name o...
SearchApp.exe	Susp...	22,528 K	72,540 K	1576	Search application	Microsoft Corporation	C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe	Enabled (permane...	The server name o...
smartscreen.exe		6,380 K	15,988 K	3120	Windows Defender SmartScr...	Microsoft Corporation	C:\Windows\System32\smartscreen.exe	Enabled (permane...	The server name o...
taskhostw.exe		5,548 K	16,252 K	4240	Host Process for Windows Ta...	Microsoft Corporation	C:\Windows\System32\taskhostw.exe	Enabled (permane...	The server name o...
taskhostw.exe		3,688 K	12,068 K	6600	Host Process for Windows Ta...	Microsoft Corporation	C:\Windows\System32\taskhostw.exe	Enabled (permane...	The server name o...
sihost.exe		5,368 K	25,184 K	5088	Shell Infrastructure Host	Microsoft Corporation	C:\Windows\System32\sihost.exe	Enabled (permane...	The server name o...
svchost.exe		3,724 K	16,452 K	4116	Host Process for Windows S...	Microsoft Corporation	C:\Windows\System32\svchost.exe	Enabled (permane...	The server name o...
svchost.exe		5,412 K	26,016 K	2232	Host Process for Windows S...	Microsoft Corporation	C:\Windows\System32\svchost.exe	Enabled (permane...	The server name o...
ctfmon.exe		4,408 K	20,872 K	4480	CTF Loader	Microsoft Corporation	C:\Windows\System32\ctfmon.exe	Enabled (permane...	The server name o...
svchost.exe	< 0.01	4,640 K	23,516 K	5372	Host Process for Windows S...	Microsoft Corporation	C:\Windows\System32\svchost.exe	Enabled (permane...	The server name o...
svchost.exe		2,876 K	12,188 K	792	Host Process for Windows S...	Microsoft Corporation	C:\Windows\System32\svchost.exe	Enabled (permane...	The server name o...
explorer.exe	< 0.01	66,172 K	193,776 K	4764	Windows Explorer	Microsoft Corporation	C:\Windows\explorer.exe	Enabled (permane...	The server name o...
vmtoolsd.exe	< 0.01	21,592 K	43,632 K	3976	VMware Tools Core Service	VMware, Inc.	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	Enabled (permane...	The server name o...
msedge.exe		47,616 K	111,556 K	6500	Microsoft Edge	Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	Enabled (permane...	The server name o...
msedge.exe		2,060 K	6,980 K	7240	Microsoft Edge	Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	Enabled (permane...	The server name o...
msedge.exe		11,180 K	27,264 K	7444	Microsoft Edge	Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	Enabled (permane...	The server name o...
msedge.exe		10,080 K	32,492 K	7500	Microsoft Edge	Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	Enabled (permane...	The server name o...
msedge.exe		6,756 K	17,292 K	7508	Microsoft Edge	Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	Enabled (permane...	The server name o...
msedge.exe	< 0.01	73,160 K	114,340 K	7936	Microsoft Edge	Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	Enabled (permane...	The server name o...
msedge.exe		14,108 K	25,540 K	5492	Microsoft Edge	Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	Enabled (permane...	The server name o...
cmd.exe		2,376 K	3,512 K	7192	Windows Command Processor	Microsoft Corporation	C:\Windows\System32\cmd.exe	Enabled (permane...	The server name o...
conhost.exe		3,528 K	23,232 K	7204	Console Window Host	Microsoft Corporation	C:\Windows\System32\conhost.exe	Enabled (permane...	The server name o...
fakenet.exe		1,304 K	3,784 K	7732			C:\Tools\FakeNet-NG\fakenet1.4.11\fakenet.exe	Enabled (permane...	The server name o...
fakenet.exe	< 0.01	25,656 K	30,864 K	7852			C:\Tools\FakeNet-NG\fakenet1.4.11\fakenet.exe	Enabled (permane...	The server name o...
Regshot-x64-Unicode.exe		503,012 K	513,072 K	6596	Regshot 1.9.1 x64 Unicode (	Regshot Team	C:\ProgramData\chocolatey\lib\regshot.flare\tools\Regshot-x64-Unicode.exe	Enabled (permane...	The server name o...
notepad.exe		63,680 K	92,036 K	5368	Notepad	Microsoft Corporation	C:\Windows\System32\notepad.exe	Enabled (permane...	A security error oc...
malwan_assignment.exe	< 0.01	5,784 K	14,148 K	1236	Host Process for Windows S...	Microsoft Corporation	C:\Users\SIT\Desktop\malwan_assignment.exe	Enabled (permane...	The server name o...
MiniThunderPlatform.exe	< 0.01	8,100 K	16,580 K	4316	迅雷云加速开放平台	深圳市迅雷网络技术有限公...	C:\Users\SIT\Desktop\download\MiniThunderPlatform.exe	Enabled (permane...	The server name o...
notepad.exe		3,084 K	23,132 K	3360	Notepad	Microsoft Corporation	C:\Windows\System32\notepad.exe	Enabled (permane...	A security error oc...
notepad.exe		3,352 K	24,368 K	5644	Notepad	Microsoft Corporation	C:\Windows\System32\notepad.exe	Enabled (permane...	A security error oc...
notepad.exe		3,176 K	23,552 K	964	Notepad	Microsoft Corporation	C:\Windows\System32\notepad.exe	Enabled (permane...	A security error oc...
notepad.exe		3,144 K	23,460 K	5508	Notepad	Microsoft Corporation	C:\Windows\System32\notepad.exe	Enabled (permane...	A security error oc...
notepad.exe		3,152 K	23,476 K	4824	Notepad	Microsoft Corporation	C:\Windows\System32\notepad.exe	Enabled (permane...	A security error oc...
procexp64.exe	2.21	38,008 K	68,760 K	3404	Sysinternals Process Explorer	Sysinternals - www.sysinter...	C:\ProgramData\chocolatey\lib\sysinternals\tools\procexp64.exe	Enabled (permane...	The server name o...
Procmon.exe		6,776 K	19,632 K	2360	Process Monitor	Sysinternals - www.sysinter...	C:\ProgramData\chocolatey\lib\sysinternals\tools\Procmon.exe	Enabled (permane...	The server name o...
Procmon64.exe		69,928 K	57,100 K	4996	Process Monitor	Sysinternals - www.sysinter...	C:\Users\SIT\AppData\Local\Temp\Procmon64.exe	Enabled (permane...	The server name o...
notepad.exe		3,068 K	25,576 K	5060	Notepad	Microsoft Corporation	C:\Windows\System32\notepad.exe	Enabled (permane...	A security error oc...

Opening process explorer to check for any programs being run by the malware.

It seems that minithunderplatform is indeed triggered by the malware.

malwan_assignment.exe	< 0.01	5,784 K	14,148 K	1236 Host Process for Windows S...	Microsoft Corporation	C:\Users\SIT\Desktop\malwan_assignment.exe
MiniThunderPlatform.exe	< 0.01	8,100 K	16,580 K	4316 迅雷云加速开放平台	深圳市迅雷网络技术有限公...	C:\Users\SIT\Desktop\download\MiniThunderPlatform.exe

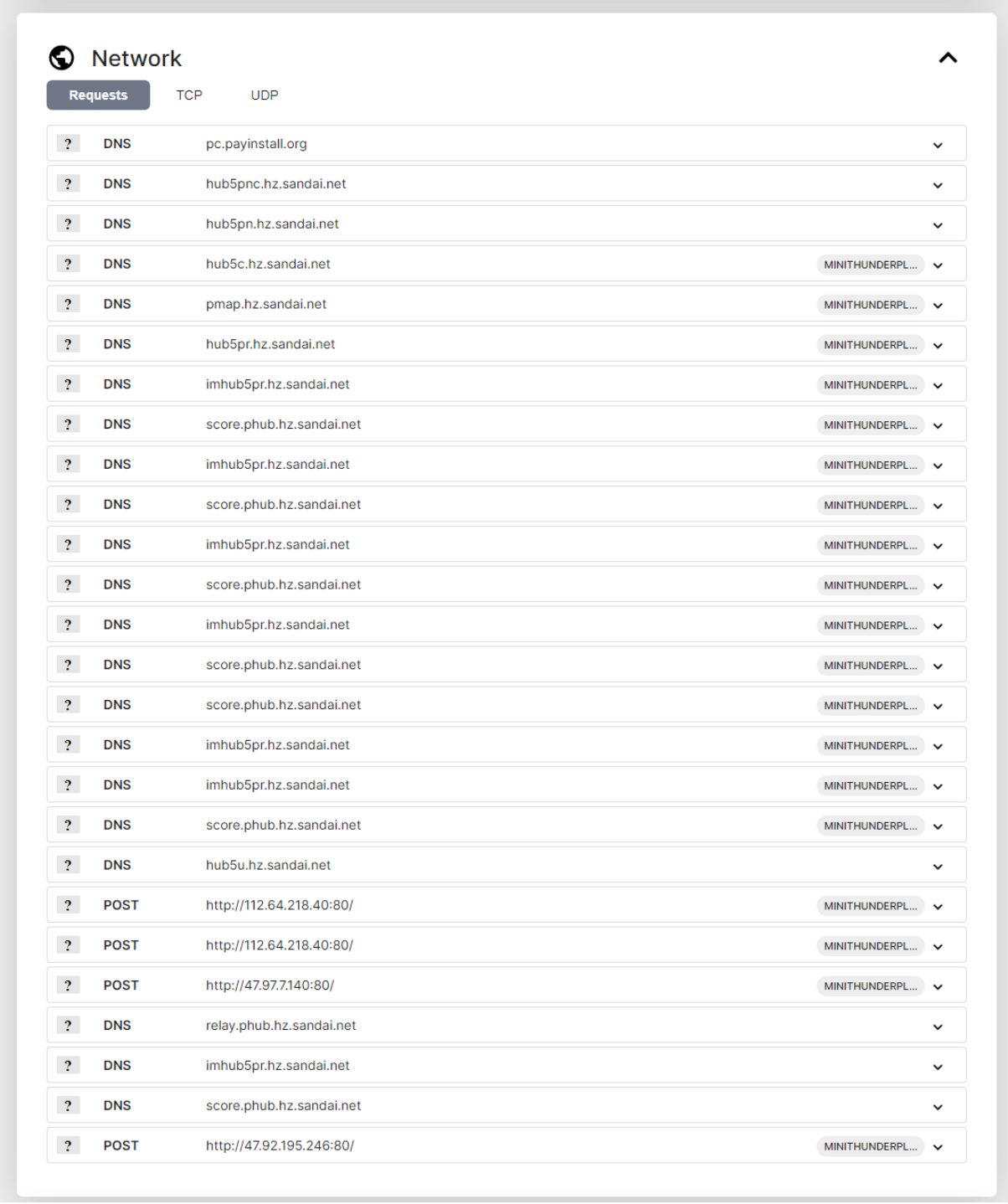
We will have to dig deeper into the program to find out what it does.

In all we have concluded that this malware is contacting several websites. It is confirmed that minithunderplatform.exe belongs to the malware being triggered.

Others (1 mark)

Research with relevant sources.

Searching the websites pc.payinstall and hubstat.hz.sandai.net online suggest the website is malicious in nature:

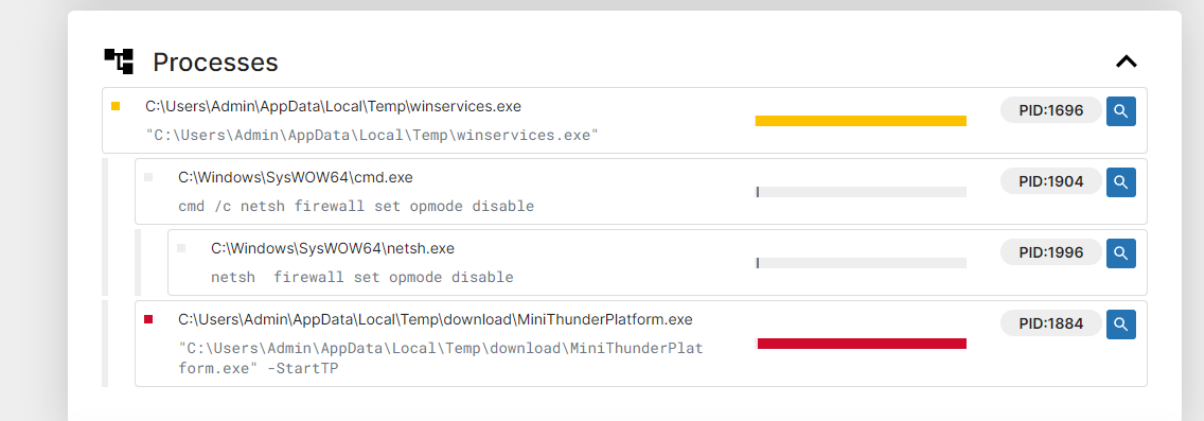


Sources used: https://tria.ge/201219-xsh8fk1tke/behavioral1

Other analysis used

Malware analysis http://hubstat.hz.sandai.net/ Malicious activity | ANY.RUN - Malware Sandbox Online

Like many of the analysis online



It triggers for the disabling of the firewall and triggering of the minithunder platform.

Summary

In Summary, when the program is executed, a program that …... The program also enumerated through the registry. This could be an attempt to obfuscate the intention of the program.

In summary when the program is launched

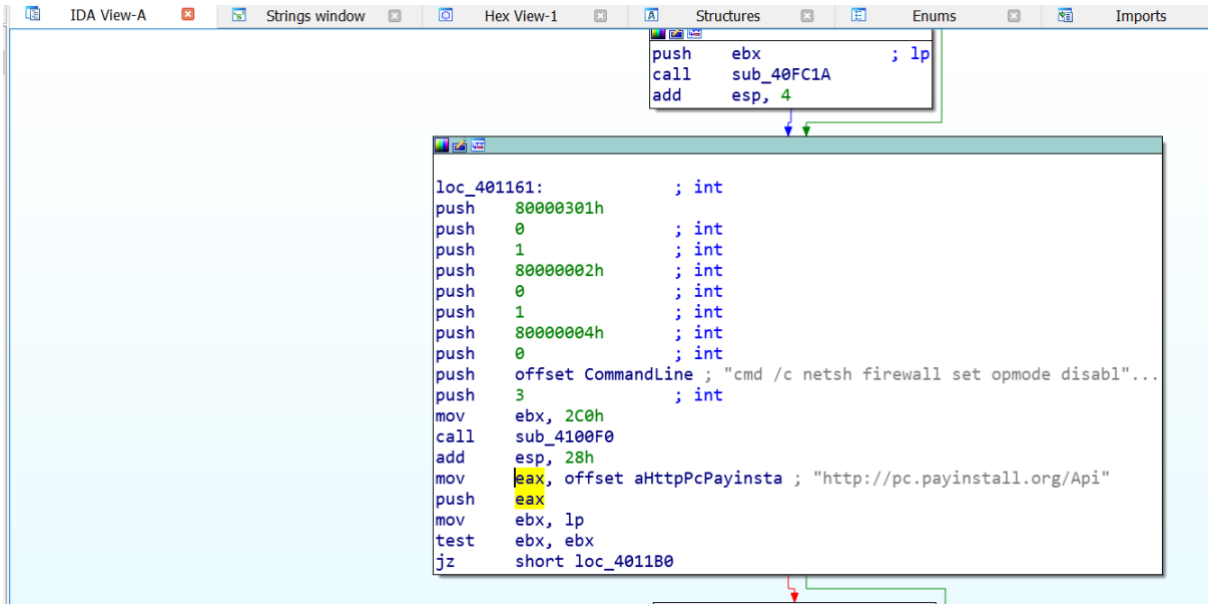
The program begins the unpacking of various programs, these various programs contain dll, executables and more which is launched upon the execution of the program. Once the programs are unpacked it does a call to the software hubstat.hz.sandai.net and sent some information via http

Afterwards it begins to attempt to look for the hostname pc.payinstall.org, it also contacts other websites such as score.phub.hz.sandai.net. I do not know what the intend of going to these websites are due to the encrypted messages. However, one thing is certain the malware turns this computer into a P2P client that is sharing downloads. P2P clients to a unknown website is dangerous and it could be used as a staging platform for further malicious activities.

Manual Code Reversing (4 marks)

Identify at least 1 code segment that is related to the malicious properties/behaviours you've observed in the previous two sections. Explain how the codes work to deliver the malicious property/behaviour.

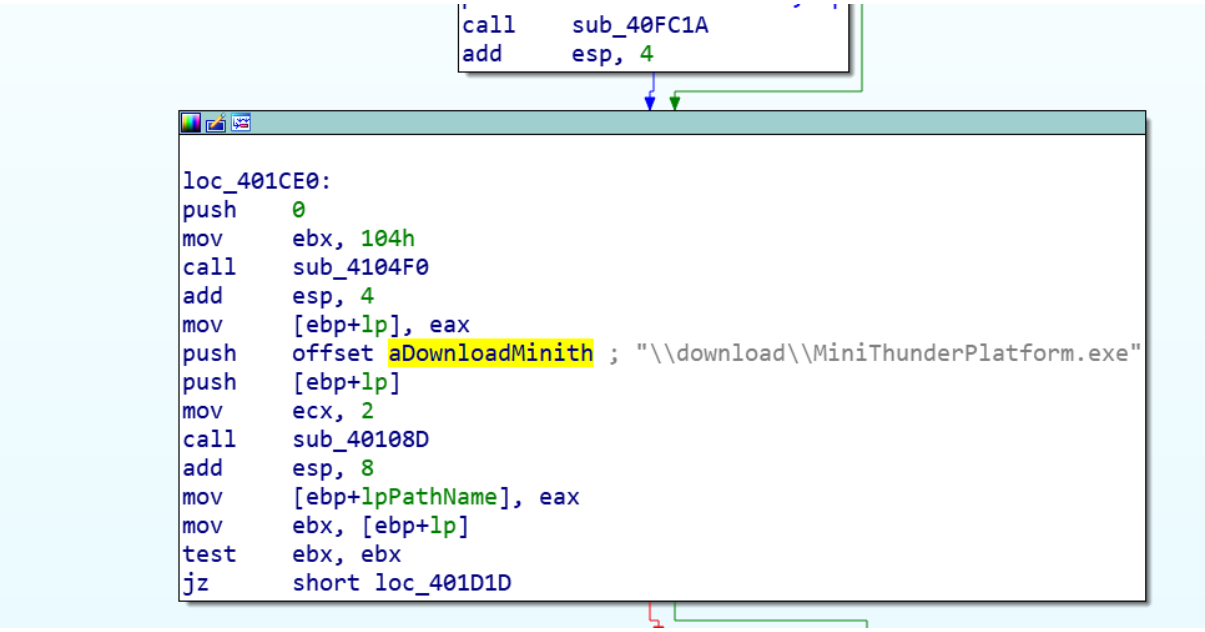
```
.data:0042E2AF                  db    0
.data:0042E2B0 a20151012        db '20151012',0         ; DATA XREF: sub_401122+1E↑o
.data:0042E2B9 ; CHAR CommandLine[]
.data:0042E2B9 CommandLine      db 'cmd /c netsh firewall set opmode disable',0
.data:0042E2B9                                          ; DATA XREF: sub_401122+5E↑o
.data:0042E2E2 aHttpPcPayinsta db 'http://pc.payinstall.org/Api',0
.data:0042E2E2                                          ; DATA XREF: sub_401122+75↑o
.data:0042E2FF aStart           db 'start',0            ; DATA XREF: sub_401122+123↑o
.data:0042E305 ; const CHAR WindowName
.data:0042E305 WindowName       db 0                    ; DATA XREF: sub_401122+138↑o
.data:0042E305                                          ; sub_401122+823↑o ...
.data:0042E306 aStart_0         db ' -start',0          ; DATA XREF: sub_401122+165↑o
.data:0042E30E aAppdataMicroso db '%APPDATA%\Microsoft\Internet Explorer\Quick Launch\User Pinned\Ta'
.data:0042E30E                                          ; DATA XREF: sub_401122+43E↑o
.data:0042E30E                  db 'skBar',0
.data:0042E355 off_42E355       dd offset sub_40C0F6    ; DATA XREF: sub_401122+63E↑o
.data:0042E359                  dd offset sub_40C11F
.data:0042E35D                  dd offset sub_40B618
.data:0042E361                  dd offset sub_40B695
.data:0042E365                  dd offset sub_40BC54
.data:0042E369                  dd offset sub_40BCDE
.data:0042E36D                  dd offset sub_40BD12
.data:0042E371                  dd offset sub_40BD25
.data:0042E375                  dd offset sub_40BF45
.data:0042E379                  dd offset sub_40C022
.data:0042E37D aDownload        db '\download',0        ; DATA XREF: sub_401A68+1E↑o
.data:0042E387 aDownloadAtl71D db '\download\atl71.dll',0
```



The codes here disable the firewall of the host machine.

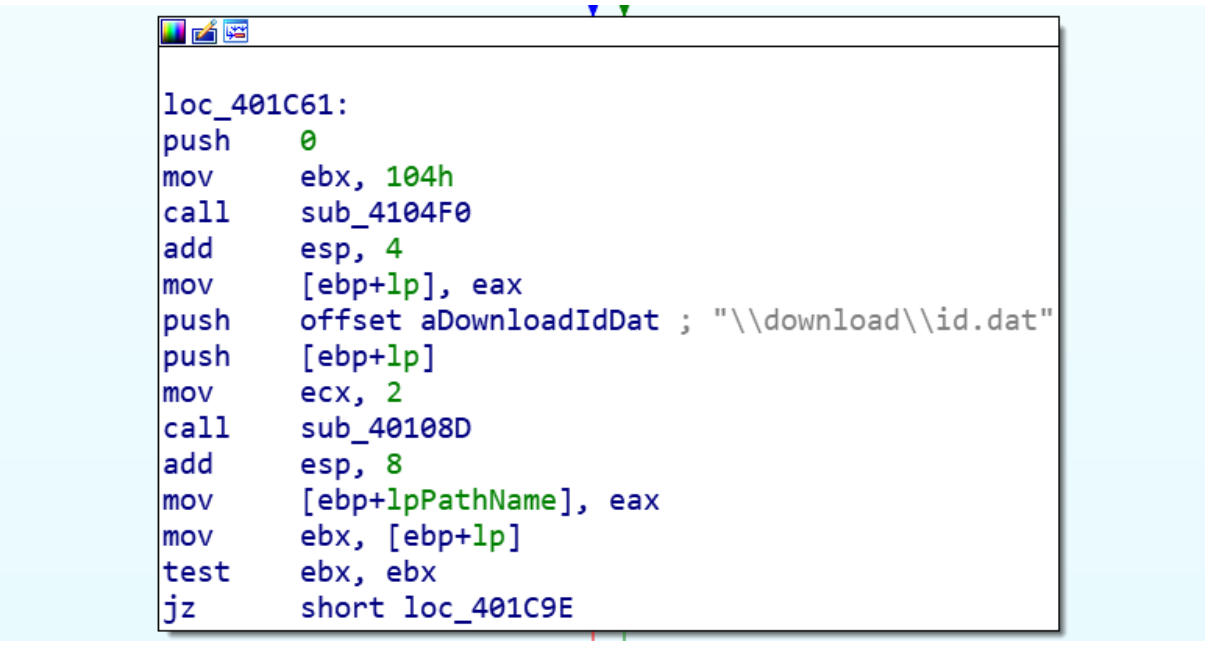
Doing so would allow for the calling of the API from the website pc.payinstall.org.

Once it calls the API it will jump to another function if the execution is smooth.



Here is another executable assembly code snippet.

What it basically does is to create a download folder with a file called MiniThunderPlatform.exe inside the folder. This will be executed later



Similarly, this code snippet suggest the creation of the id.dat file

This file would be the id file for minithunderplatform.exe.

Summary

In summary this malware is dangerous, it creates this machine to be a P2P sharing client using minithunderplatform to allow the downloading of packages and dll from a Chinese server.

This Chinese server can allow for any download of suspicious payload. Basically, this machine then becomes a staging platform for malicious payloads to be loaded here.

The program is persistent. Despite removal it can restart itself. Referring to many online sources, has affirm that this malware is persistent.

As it creates the infected host to be a P2P client for an unknown platform.

This is highly dangerous and should be dealt with.

Conclusion

The program imitates the file svchost. It is also obfuscated with various UPX files to evade detection from AV malware. It also disables the firewall of the system.

There are various ways to mitigate these issues.

First and foremost, as there are plenty of malware analysis, updating the anti-malware software would allow for easy detection of this malware.

Next, since it just creates a P2P Client, delete all existence of this program first. Run scans to detect if the persistency of this program still exists. Ensure that the program generated is quarantined.

If the program persists, perhaps booting windows in safe mode and attempt the deletion of the malware.

References

1. **Triage.(n.d.) malwan_assignment. Retrieved Feb 01 from the triage website: https://tria.ge/230219-kmxw8aef5s**
2. **JaffaCakes118(n.d.). Malwan_assignment. Retrieved 2024, Feb 01 from the virus total website: https://www.virustotal.com/gui/file/ed96096ac258b000b243394cdd390bf8bdcc5c4d5e22610e6837902051bdc3a1/community**
3. **Any run (2021, April 18) hubstat.hz.sandai.net analysis. Retrieved 2024, Feb 01 from the any run website: https://any.run/report/5f71b4085f9f4e10c887e5ed4008aa8303b709403b9e03f888d54b58450d44af/85c1eec2-05ad-4ea2-a633-a6a23b6b8c0a**
4. **Joe Sandbox Cloud (May 8th 2021) svchost.exe. Retrieved 2024 Feb 01 from the joe sandbox cloud website: https://www.joesandbox.com/analysis/408466/0/pdf**