



Practical Malware Analysis & Triage

Malware Analysis Report

WannaCry Malware

Feb 2023 | Gian Paris C. Aksam | v1.0

Table of Contents

Table of Contents	3
Executive Summary	4
High-Level Technical Summary	5
Malware Composition	5
tasksche.exe	6
taskhsvc:	7
Basic Static Analysis	9
Basic Dynamic Analysis	13
Advanced Static Analysis	Error! Bookmark not defined.
Advanced Dynamic Analysis	19
Indicators of Compromise	20
Network Indicators	21
Host-based Indicators	23
Rules & Signatures	26
Appendices	26
A. Yara Rules	26
B. Callback URLs	26
C. Decompiled Code Snippets	27

Executive Summary

SHA256 hash	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
-------------	--

Wannacry is a ransomware malware sample first identified on May 12 2017. It is a Microsoft Visual C++ compiled that runs on the x32 Windows operating system. When the malware is run it encrypts your files and asks for ransom in crypto. When run malware spawns a process called tasksche.exe. However, wannacry malware only runs unless the return status to the url: <http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwengwea.com> is not successful.

High-Level Technical Summary

WannaCry

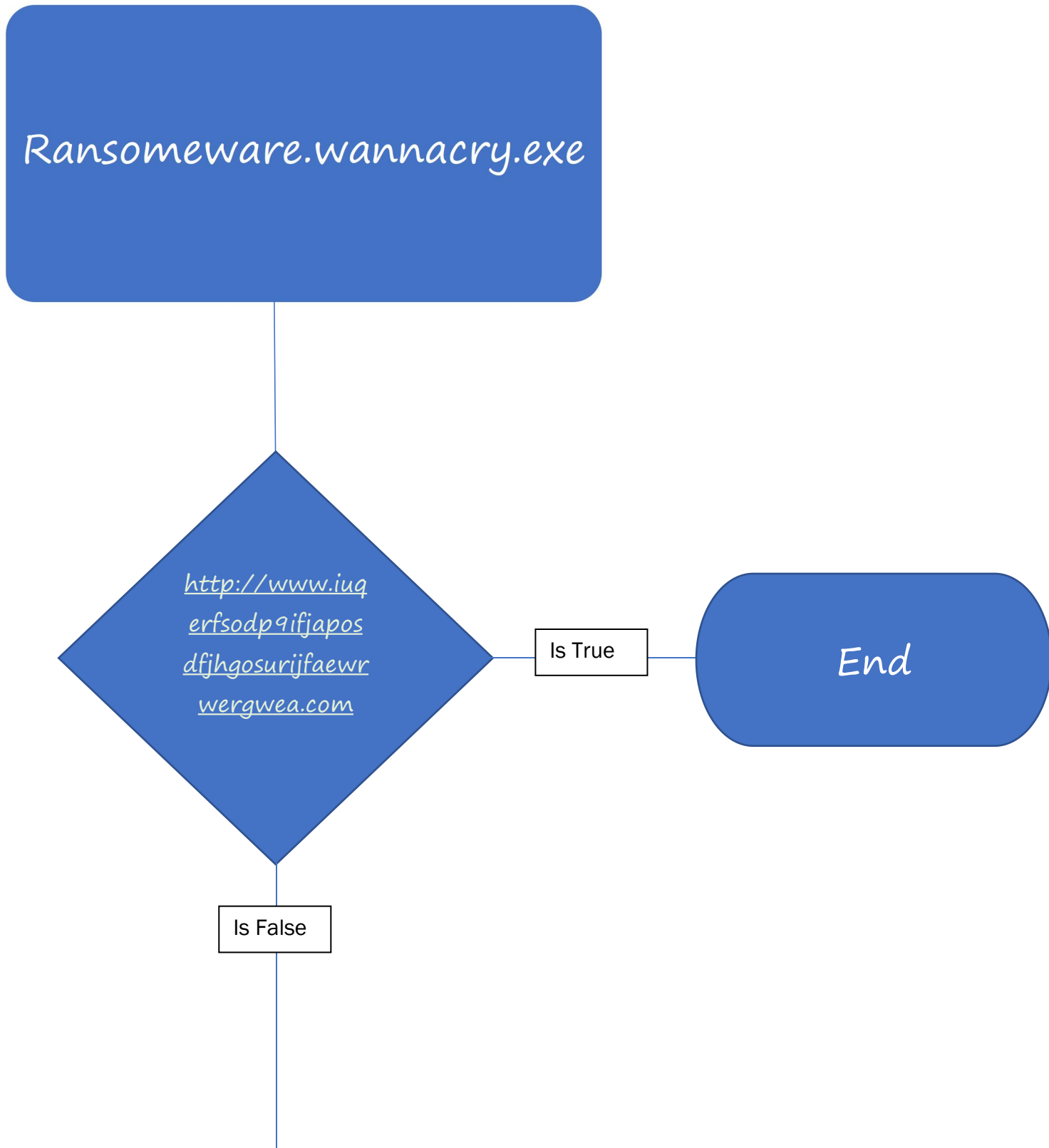
Ransomeware.wannacry.exe

<http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergrwa.com>

Is True

End

Is False



```
graph TD; A[Execute Malware] --> B["tasksche.exe  
(Creates a files, folder to dump it's resources)"]; B --> C["tasksvc.exe  
(Opens port 9050 to a LISTENING state and attempts to connect to non-private remote addresses over HTTPS.)"]; C --> D[End];
```

Execute
Malware

tasksche.exe

(Creates a files, folder to dump it's
resources)

tasksvc.exe

(Opens port 9050 to a LISTENING state
and attempts to connect to non-private
remote addresses over HTTPS.)

End

Malware Composition

DemoWare consists of the following components:

File Name	SHA256 Hash
tasksche.exe	ED01EBFBC9EB5BBEA545AF4D01BF5F1071661840480439C6E5BABE8E080E41AA
taskdl.exe	4A468603FDCB7A2EB5770705898CF9EF37AADE532A7964642ECD705A74794B79
taskse.exe	2CA2D550E603D74DEDDA03156023135B38DA3630CB014E3D00B1263358C5F00DED01EB
taskhsvc.exe	E48673680746FBE027E8982F62A83C298D6FB46AD9243DE8E79B7E5A24DCD4EB

tasksche.exe

Creates directory and dumps it's resources to that directory. The generated directory has a random name.

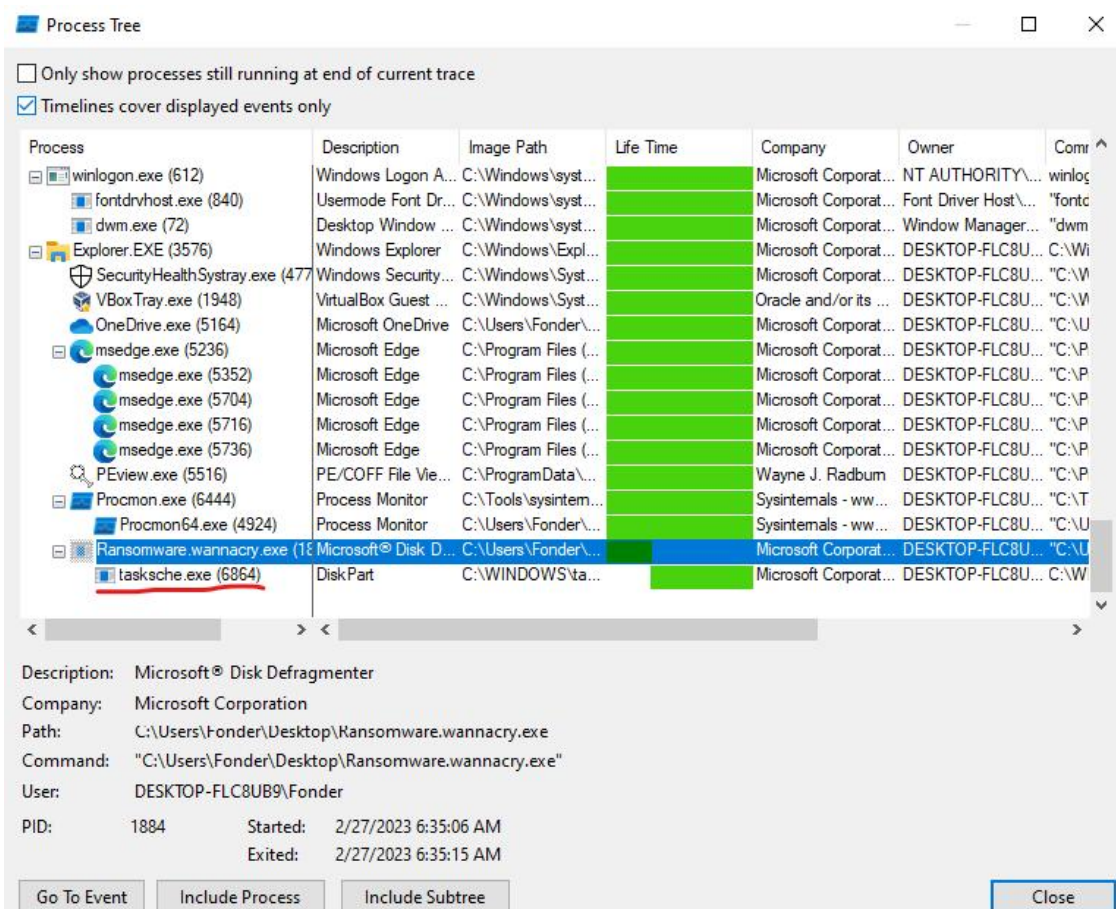



Fig 1:tasksche.exe in processs tree

taskhsvc.exe:



TCPView - Sysinternals: www.sysinternals.com

File Edit View Process Connection Options Help

4 TCP v4 6 TCP v6 4 UDP v4 6 UDP v6 Search

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create
svchost.exe	940	TCP	Listen	0.0.0.0	135	0.0.0.0	0	2/27/2023 5:07:
System	4	TCP	Listen	10.0.0.3	139	0.0.0.0	0	2/27/2023 5:07:
tasksvcs.exe	3680	TCP	Established	127.0.0.1	1637	127.0.0.1	1638	2/27/2023 5:31:
tasksvcs.exe	3680	TCP	Established	127.0.0.1	1638	127.0.0.1	1637	2/27/2023 5:31:
svchost.exe	1196	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	2/27/2023 5:10:
tasksvcs.exe	3680	TCP	Listen	127.0.0.1	9050	0.0.0.0	0	2/27/2023 5:31:
lsass.exe	688	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	2/27/2023 5:07:
wininit.exe	536	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	2/27/2023 5:07:
svchost.exe	1040	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	2/27/2023 5:07:
svchost.exe	752	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	2/27/2023 5:07:
spoolsv.exe	1276	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	2/27/2023 5:07:
svchost.exe	2312	TCP	Listen	0.0.0.0	49669	0.0.0.0	0	2/27/2023 5:07:
services.exe	680	TCP	Listen	0.0.0.0	50185	0.0.0.0	0	2/27/2023 5:08:
System	4	TCP	Listen	0.0.0.0	445	0.0.0.0	0	2/27/2023 5:07:
svchost.exe	1368	TCP	Listen	0.0.0.0	7680	0.0.0.0	0	2/27/2023 5:07:

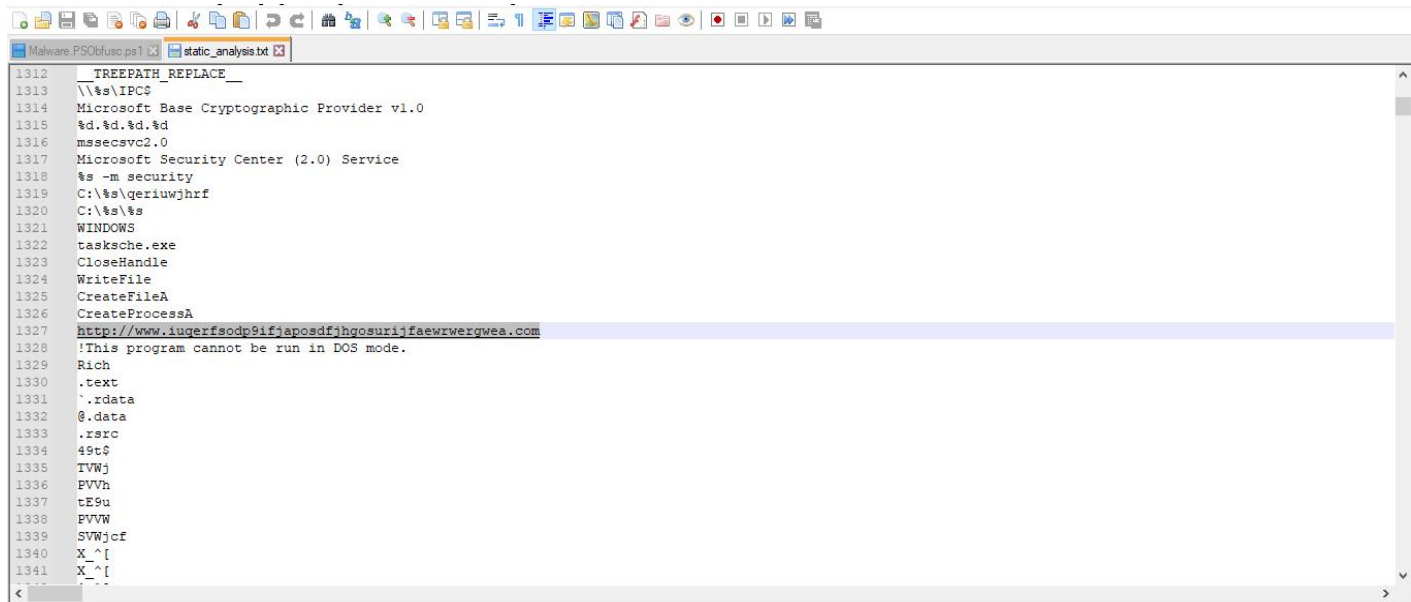
Endpoints: 54 Established: 2 Listening: 23 Time Wait: Close Wait: Update: 2 sec States: (All)

Fig 2:tasksvcs.exe listening on port 9050.

Basic Static Analysis

{Screenshots and description about basic static artifacts and methods}

Floss

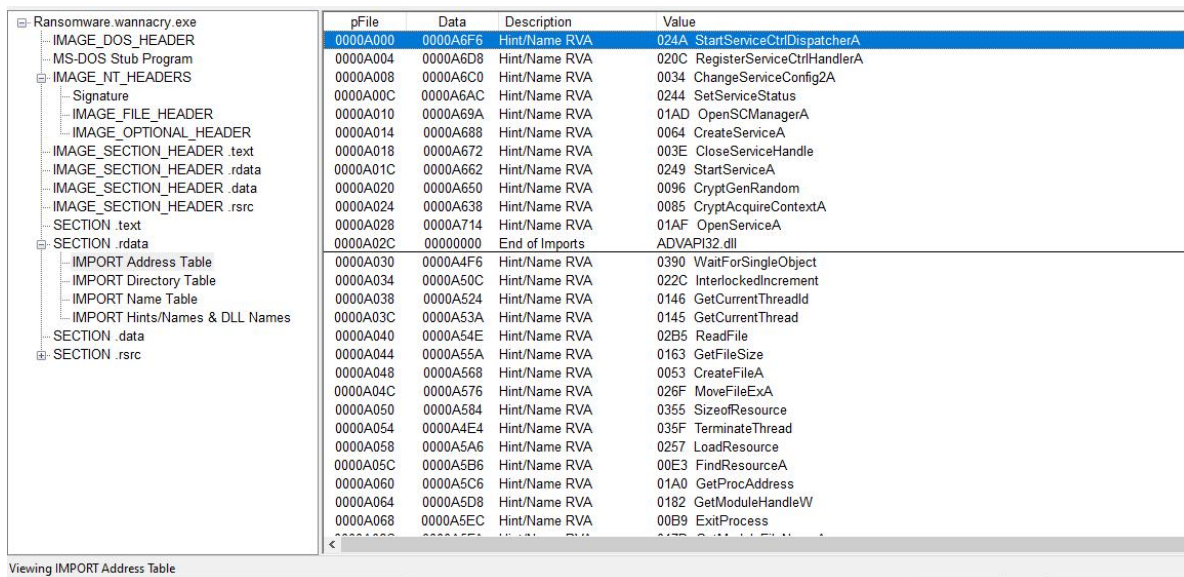


```
1312 TREEPATH_REPLACE_
1313 \\$s\IPC$
1314 Microsoft Base Cryptographic Provider v1.0
1315 %d.%d.%d.%d
1316 mssecsvc2.0
1317 Microsoft Security Center (2.0) Service
1318 %s -m security
1319 C:\$s\qeriuwjhrf
1320 C:\$s\%s
1321 WINDOWS
1322 tasksche.exe
1323 CloseHandle
1324 WriteFile
1325 CreateFileA
1326 CreateProcessA
1327 http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
1328 !This program cannot be run in DOS mode.
1329 Rich
1330 .text
1331 .rdata
1332 @.data
1333 .rsrc
1334 49tc$
1335 TVWj
1336 PVVh
1337 tE9u
1338 PVVW
1339 SVWjcf
1340 X ^[
1341 X ^[
1342 X ^[
```

Analyzed the binary with floss and got interesting strings but most importantly the url:

<http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com>

PEView



pFile	Data	Description	Value
0000A000	0000A6F6	Hint/Name RVA	024A StartServiceCtrlDispatcherA
0000A004	0000A6D8	Hint/Name RVA	020C RegisterServiceCtrlHandlerA
0000A008	0000A6C0	Hint/Name RVA	0034 ChangeServiceConfig2A
0000A00C	0000A6AC	Hint/Name RVA	0244 SetServiceStatus
0000A010	0000A69A	Hint/Name RVA	01AD OpenSCManagerA
0000A014	0000A688	Hint/Name RVA	0064 CreateServiceA
0000A018	0000A672	Hint/Name RVA	003E CloseServiceHandle
0000A01C	0000A662	Hint/Name RVA	0249 StartServiceA
0000A020	0000A650	Hint/Name RVA	0096 CryptGenRandom
0000A024	0000A638	Hint/Name RVA	0085 CryptAcquireContextA
0000A028	0000A714	Hint/Name RVA	01AF OpenServiceA
0000A02C	00000000	End of Imports	ADVAPI32.dll
0000A030	0000A4F6	Hint/Name RVA	0390 WaitForSingleObject
0000A034	0000A50C	Hint/Name RVA	022C InterlockedIncrement
0000A038	0000A524	Hint/Name RVA	0146 GetCurrentThreadId
0000A03C	0000A53A	Hint/Name RVA	0145 GetCurrentThread
0000A040	0000A54E	Hint/Name RVA	02B5 ReadFile
0000A044	0000A55A	Hint/Name RVA	0163 GetFileSize
0000A048	0000A568	Hint/Name RVA	0053 CreateFileA
0000A04C	0000A576	Hint/Name RVA	026F MoveFileExA
0000A050	0000A584	Hint/Name RVA	0355 SizeofResource
0000A054	0000A4E4	Hint/Name RVA	035F TerminateThread
0000A058	0000A5A6	Hint/Name RVA	0257 LoadResource
0000A05C	0000A5B6	Hint/Name RVA	00E3 FindResourceA
0000A060	0000A5C6	Hint/Name RVA	01A0 GetProcAddress
0000A064	0000A5D8	Hint/Name RVA	0182 GetModuleHandleW
0000A068	0000A5EC	Hint/Name RVA	00B9 ExitProcess

Import Address Table(IAT): API functions that the binary used.

PEStudio

indicators (91)	TerminateThread	x	execution	-	kernel32.dll
virustotal (error)	MoveFileExA	x	file	-	kernel32.dll
dos-header (64 bytes)	3 (closesocket)	x	network	x	ws2_32.dll
dos-stub (184 bytes)	16 (recv)	x	network	x	ws2_32.dll
rich-header (9)	19 (send)	x	network	x	ws2_32.dll
file-header (Nov.2010)	8 (htonl)	x	network	x	ws2_32.dll
optional-header (GUI)	14 (ntohl)	x	network	x	ws2_32.dll
directories (3)	115 (WSAStartup)	x	network	x	ws2_32.dll
sections (files)	12 (inet_ntoa)	x	network	x	ws2_32.dll
libraries (blacklist) *	10 (ioctlsocket)	x	network	x	ws2_32.dll
imports (91) *	18 (select)	x	network	x	ws2_32.dll
exports (n/a)	9 (htons)	x	network	x	ws2_32.dll
tls-callbacks (n/a)	23 (socket)	x	network	x	ws2_32.dll
resources (executable) *	4 (connect)	x	network	x	ws2_32.dll
strings (size)	11 (inet_addr)	x	network	x	ws2_32.dll
debug (n/a)	GetAdaptersInfo	x	network	-	iphlpapi.dll
manifest (n/a)	InternetOpenA	x	network	-	wininet.dll
version (lhdfgui.exe)	InternetOpenUrlA	x	network	-	wininet.dll
certificate (n/a)	InternetCloseHandle	x	network	-	wininet.dll
overlay (n/a)	StartServiceCtrlDispatcherA	x	services	-	advapi32.dll
	ChangeServiceConfig2A	x	services	-	advapi32.dll
	CreateServiceA	x	services	-	advapi32.dll
	QueryPerformanceFrequency	x	synchronization	-	kernel32.dll
	CloseHandle	-	-	-	kernel32.dll
	public: thiscall std: Lockit...	-	-	-	msvcp60.dll
	public: thiscall std: Lockit...	-	-	-	msvcp60.dll
	GetPerAdapterInfo	-	-	-	iphlpapi.dll
	_set_app_type	-	-	-	msvcrt.dll
	_stricmp	-	-	-	msvcrt.dll

sha256: 24D004A104D4D54034D8CFFC2A4819A11F39008A575AA614EA04703480B1022C file-type: executable subsystem: GUI

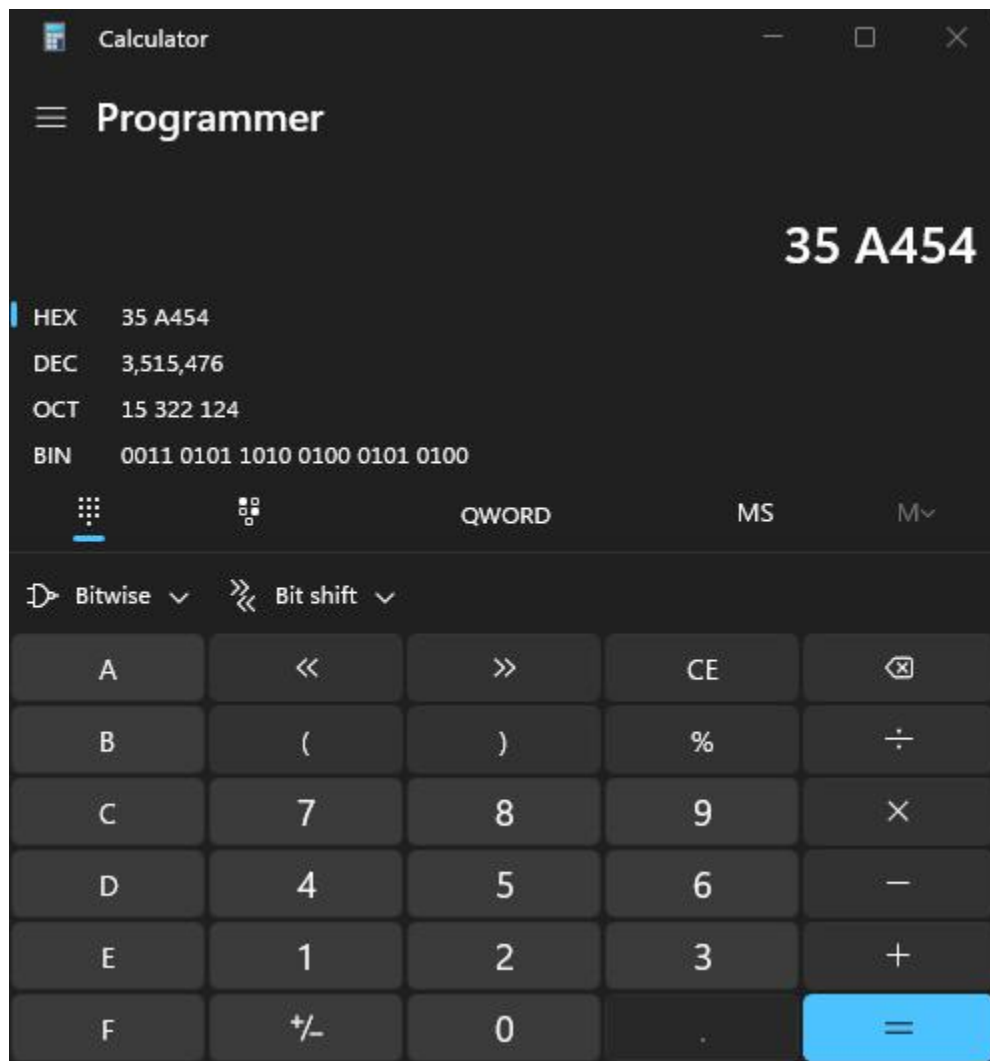
Imported functions flagged as malicious(Most likely).

Binary Packed or Not Packed

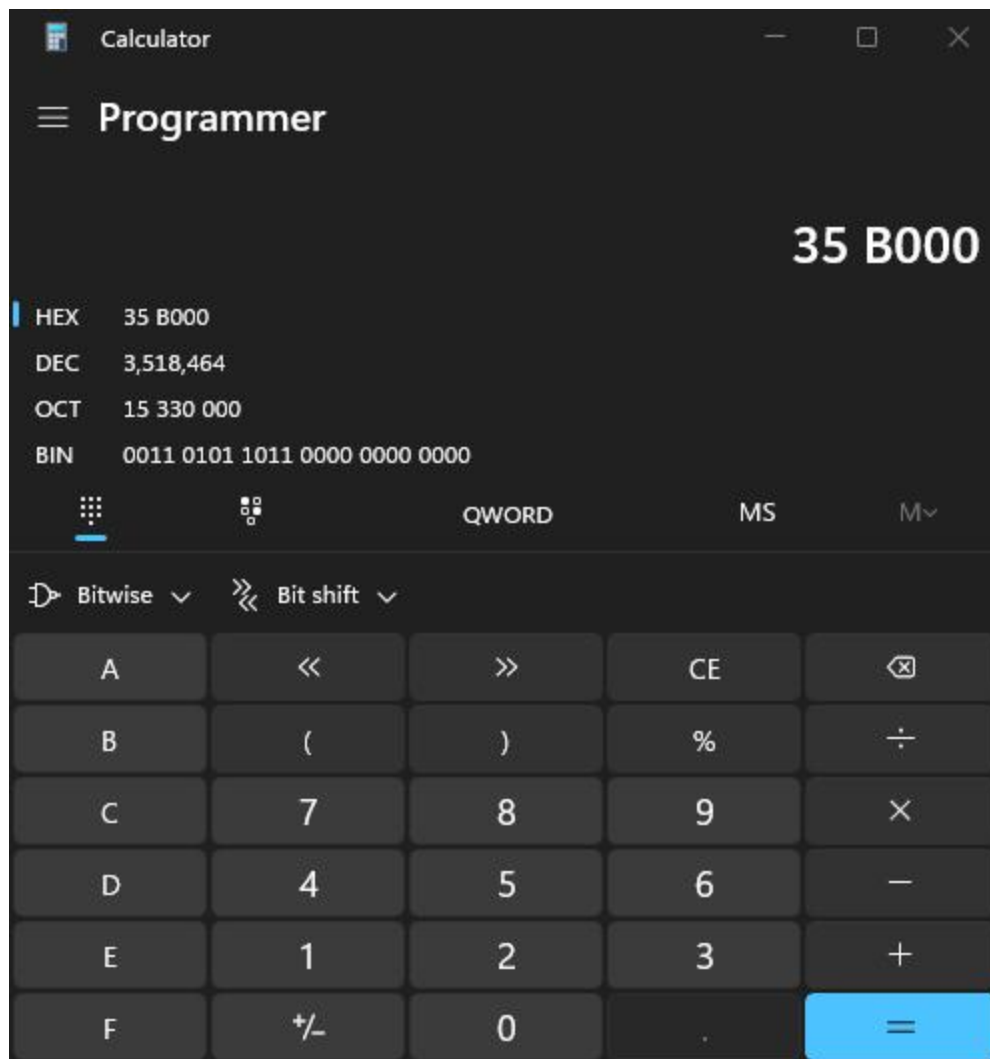
	pFile	Data	Description	Value
Ransomware.wannacry.exe				
IMAGE_DOS_HEADER	00000268	2E 72 73 72	Name	.rsrc
MS-DOS Stub Program	0000026C	63 00 00 00		
+ IMAGE_NT_HEADERS	00000270	0035A454	Virtual Size	
IMAGE_SECTION_HEADER	00000274	00310000	RVA	
IMAGE_SECTION_HEADER	00000278	0035B000	Size of Raw Data	
IMAGE_SECTION_HEADER	0000027C	00032000	Pointer to Raw Data	
IMAGE_SECTION_HEADER	00000280	00000000	Pointer to Relocations	
SECTION .text	00000284	00000000	Pointer to Line Numbers	
SECTION .rdata	00000288	0000	Number of Relocations	
IMPORT Address Table	0000028A	0000	Number of Line Numbers	
IMPORT Directory Table	0000028C	40000040	Characteristics	
IMPORT Name Table		00000040		IMAGE_SCN_CNT_INITIALIZED_DATA
IMPORT Hints/Names & C		40000000		IMAGE_SCN_MEM_READ
SECTION .data				
SECTION .rsrc				
IMAGE_RESOURCE_DIR				
IMAGE_RESOURCE_DIR				
IMAGE_RESOURCE_DIR				
IMAGE_RESOURCE_DAT				
IMAGE_RESOURCE_DIR				
R 0727 0409				
VERSION 0001 0409				

The virtual size and size of raw data are used as reference for the size of the binary.

If the sizes are far apart from each other then the binary is most likely packed.



Here the value of the virtual size is 3,515,476 bytes.



Here the value of the size of raw data is 3,518,464 bytes.

So in comparison the virtual size is 3,515,476 bytes and size of raw data is 3,518,464 bytes which is not too far apart from each other. So most likely this binary is not packed.

Basic Dynamic Analysis

TCPView

TCPView - Sysinternals: www.sysinternals.com

File Edit View Process Connection Options Help

4 TCP v4 6 TCP v6 4 UDP v4 6 UDP v6

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	Sent Packets
lsass.exe	592	TCPv6	Listen	::	49664	::	0	9/4/2021 3:57:11 PM	lsass.exe	
lsass.exe	592	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	9/4/2021 3:57:11 PM	lsass.exe	
Ransomware.wannacry...	2172	TCP	Syn Sent	169.254.243.48	23820	169.254.40.1	445	10/17/2021 8:54:10 AM	mssecsvcs2.0	
Ransomware.wannacry...	2172	TCP	Syn Sent	169.254.243.48	23799	169.254.24.1	445	10/17/2021 8:54:08 AM	mssecsvcs2.0	
Ransomware.wannacry...	2172	TCP	Syn Sent	169.254.243.48	23798	169.254.23.1	445	10/17/2021 8:54:07 AM	mssecsvcs2.0	
Ransomware.wannacry...	2172	TCP	Syn Sent	169.254.243.48	23823	169.254.43.1	445	10/17/2021 8:54:10 AM	mssecsvcs2.0	
Ransomware.wannacry...	2172	TCP	Syn Sent	169.254.243.48	23824	169.254.44.1	445	10/17/2021 8:54:10 AM	mssecsvcs2.0	
Ransomware.wannacry...	2172	TCP	Syn Sent	169.254.243.48	23825	169.254.45.1	445	10/17/2021 8:54:10 AM	mssecsvcs2.0	
Ransomware.wannacry...	2172	TCP	Syn Sent	169.254.243.48	23826	169.254.46.1	445	10/17/2021 8:54:10 AM	mssecsvcs2.0	
Ransomware.wannacry...	2172	TCP	Syn Sent	169.254.243.48	23827	169.254.47.1	445	10/17/2021 8:54:10 AM	mssecsvcs2.0	
Ransomware.wannacry...	2172	TCP	Syn Sent	169.254.243.48	23806	169.254.30.1	445	10/17/2021 8:54:08 AM	mssecsvcs2.0	
Ransomware.wannacry...	2172	TCP	Syn Sent	169.254.243.48	23829	169.254.49.1	445	10/17/2021 8:54:10 AM	mssecsvcs2.0	
Ransomware.wannacry...	2172	TCP	Syn Sent	169.254.243.48	23831	169.254.50.1	445	10/17/2021 8:54:10 AM	mssecsvcs2.0	
Ransomware.wannacry...	2172	TCP	Syn Sent	169.254.243.48	23832	169.254.51.1	445	10/17/2021 8:54:10 AM	mssecsvcs2.0	
Ransomware.wannacry...	2172	TCP	Syn Sent	169.254.243.48	23834	169.254.52.1	445	10/17/2021 8:54:10 AM	mssecsvcs2.0	
Ransomware.wannacry...	2172	TCP	Syn Sent	169.254.243.48	23797	169.254.22.1	445	10/17/2021 8:54:07 AM	mssecsvcs2.0	
Ransomware.wannacry...	2172	TCP	Syn Sent	169.254.243.48	23804	169.254.29.1	445	10/17/2021 8:54:08 AM	mssecsvcs2.0	
Ransomware.wannacry...	2172	TCP	Syn Sent	169.254.243.48	23807	169.254.31.1	445	10/17/2021 8:54:08 AM	mssecsvcs2.0	
Ransomware.wannacry...	2172	TCP	Syn Sent	169.254.243.48	23796	169.254.21.1	445	10/17/2021 8:54:07 AM	mssecsvcs2.0	
Ransomware.wannacry...	2172	TCP	Syn Sent	169.254.243.48	23803	169.254.28.1	445	10/17/2021 8:54:08 AM	mssecsvcs2.0	
Ransomware.wannacry...	2172	TCP	Syn Sent	169.254.243.48	23802	169.254.27.1	445	10/17/2021 8:54:08 AM	mssecsvcs2.0	
Ransomware.wannacry...	2172	TCP	Syn Sent	169.254.243.48	23801	169.254.26.1	445	10/17/2021 8:54:08 AM	mssecsvcs2.0	
Ransomware.wannacry...	2172	TCP	Syn Sent	169.254.243.48	23800	169.254.25.1	445	10/17/2021 8:54:08 AM	mssecsvcs2.0	
services.exe	584	TCPv6	Listen	::	49669	::	0	9/4/2021 3:57:14 PM	services.exe	
services.exe	584	TCP	Listen	0.0.0.0	49669	0.0.0.0	0	9/4/2021 3:57:14 PM	services.exe	
spoolsv.exe	1756	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	9/4/2021 3:57:13 PM	Spooler	
spoolsv.exe	1756	TCPv6	Listen	::	49668	::	0	9/4/2021 3:57:13 PM	Spooler	

Endpoints: 79 Established: Listening: 23 Time Wait: Close Wait: Update: 2 sec States: (All)

A flood of numerous SMB connection requests to non-private remote addresses.

TCPView - Sysinternals: www.sysinternals.com

File Edit View Process Connection Options Help

4 TCP v4 6 TCP v6 4 UDP v4 6 UDP v6

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create
svchost.exe	948	TCP	Listen	0.0.0.0	135	0.0.0.0	0	2/27/2023 6:58:
System	4	TCP	Listen	10.0.0.3	139	0.0.0.0	0	2/27/2023 6:58:
svchost.exe	1208	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	2/27/2023 6:58:
taskhsvc.exe	1748	TCP	Listen	127.0.0.1	9050	0.0.0.0	0	2/27/2023 8:06:
lsass.exe	688	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	2/27/2023 6:58:
wininit.exe	536	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	2/27/2023 6:58:
svchost.exe	1052	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	2/27/2023 6:58:
svchost.exe	296	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	2/27/2023 6:58:
spoolsv.exe	1512	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	2/27/2023 6:58:
svchost.exe	2256	TCP	Listen	0.0.0.0	49670	0.0.0.0	0	2/27/2023 6:58:
taskhsvc.exe	1748	TCP	Established	127.0.0.1	50029	127.0.0.1	50030	2/27/2023 8:06:
taskhsvc.exe	1748	TCP	Established	127.0.0.1	50030	127.0.0.1	50029	2/27/2023 8:06:
services.exe	680	TCP	Listen	0.0.0.0	50147	0.0.0.0	0	2/27/2023 6:59:
System	4	TCP	Listen	0.0.0.0	445	0.0.0.0	0	2/27/2023 6:58:
svchost.exe	2008	TCP	Listen	0.0.0.0	7680	0.0.0.0	0	2/27/2023 6:58:

Endpoints: 54 Established: 2 Listening: 23 Time Wait: Close Wait: Update: 2 sec States: (All)

taskhsvc.exe listense on port 9050

Wireshark

The image shows a Wireshark network traffic capture window titled "Capturing from enp0s3". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar with various icons. A display filter is set to "<Ctrl-/>".

The packet list pane shows 13 packets. Packet 8 is selected, showing an HTTP GET request. The packet details pane for packet 8 shows the following structure:

- Frame 8: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) on interface enp0s3, id 0
- Ethernet II, Src: PcsCompu 55:06:07 (08:00:27:55:06:07), Dst: PcsCompu 25:8f:13 (08:00:27:25:8f:13)
- Internet Protocol Version 4, Src: 10.0.0.4, Dst: 10.0.0.3
- Transmission Control Protocol, Src Port: 1077, Dst Port: 80, Seq: 1, Ack: 1, Len: 100
- Hypertext Transfer Protocol
 - GET / HTTP/1.1\r\n
 - Host: www.iuqerfsodp9ifjaposdfjhgosurijfaewrrergwea.com\r\n
 - Cache-Control: no-cache\r\n
 - \r\n
 - [Full request URI: http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrrergwea.com/]
 - [HTTP request 1/1]
 - [Response in frame: 12]

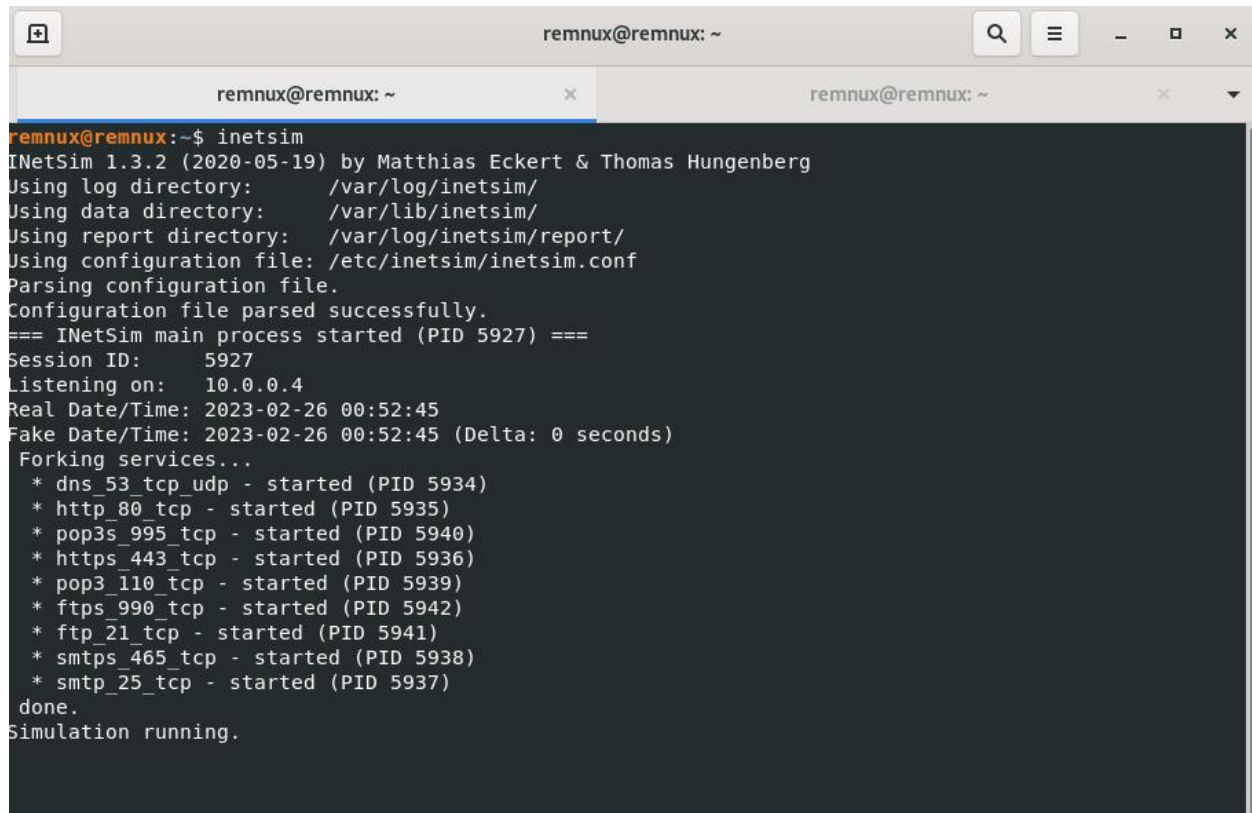
The packet bytes pane shows the raw data of the selected packet, with a hex dump and ASCII representation. The ASCII representation shows the following text:

```
...!%...  
...0...  
...5-P...  
...GET /  
/1.1: Host:  
iuqerfsodp9ifjaposdfjhgosurijfaewrrergwea.com  
Cache-Control:  
no-cache...
```

The binary attempts to initiate a connection with the weird URL

<http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrrergwea.com>

Inetsim



```
remnux@remnux:~$ inetsim
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory:      /var/log/inetsim/
Using data directory:    /var/lib/inetsim/
Using report directory:   /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
=== INetSim main process started (PID 5927) ===
Session ID:      5927
Listening on:    10.0.0.4
Real Date/Time:  2023-02-26 00:52:45
Fake Date/Time:  2023-02-26 00:52:45 (Delta: 0 seconds)
Forking services...
* dns_53_tcp_udp - started (PID 5934)
* http_80_tcp    - started (PID 5935)
* pop3s_995_tcp  - started (PID 5940)
* https_443_tcp  - started (PID 5936)
* pop3_110_tcp   - started (PID 5939)
* ftps_990_tcp   - started (PID 5942)
* ftp_21_tcp     - started (PID 5941)
* smtps_465_tcp  - started (PID 5938)
* smtp_25_tcp    - started (PID 5937)
done.
Simulation running.
```

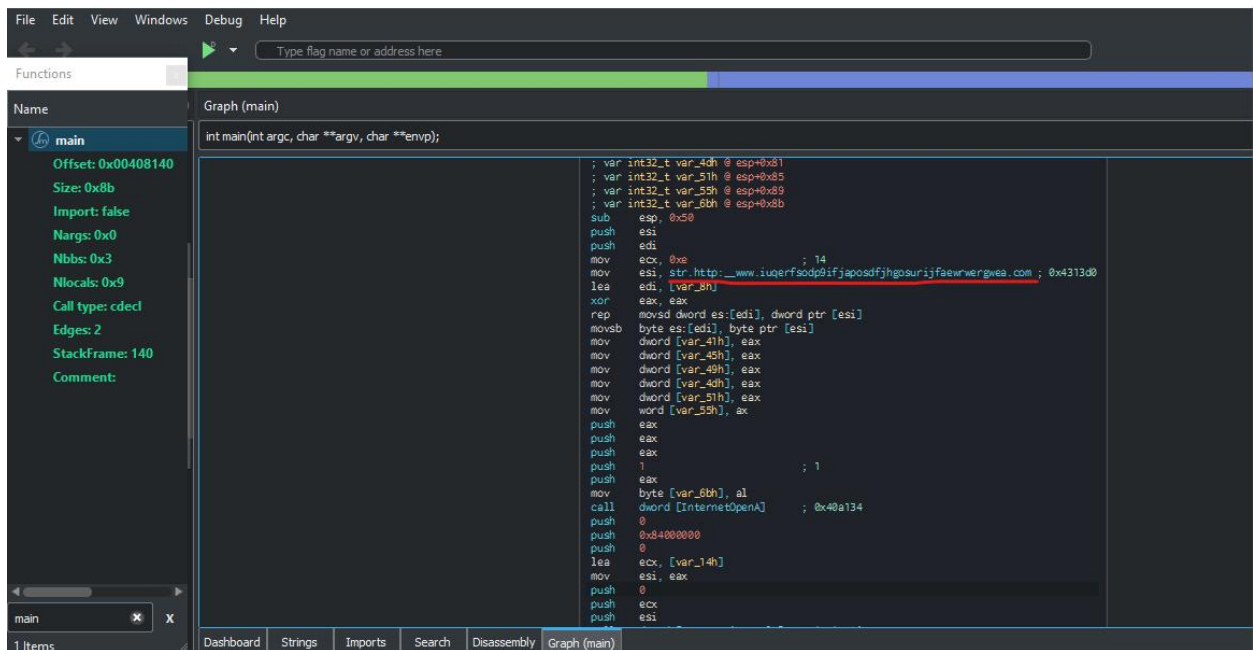
When inetsim is off the malware executes, but when it is on it doesn't. The reason for this is because of how the malware is made, inetsim simulates a fake dns server which when the malware connects to it will think it is connecting to the url:

<http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com>

when in reality it's connected to inetsim's simulated server.

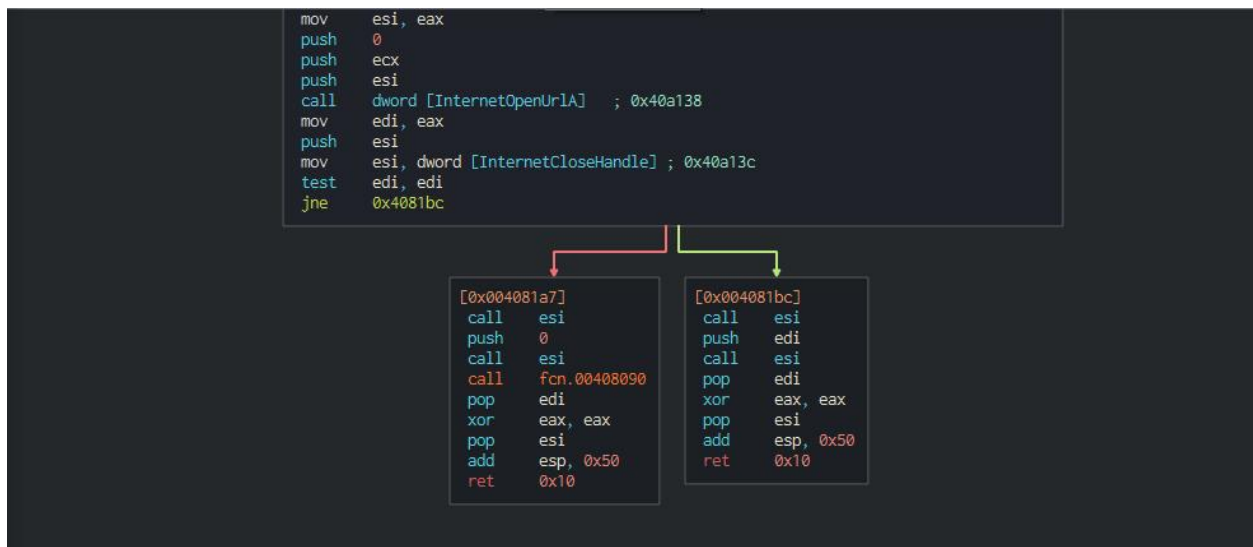
Advanced Static Analysis

Cutter



In the main function we can see the url and if we look below there is a call to InternetOpenA which is an api of windows.

The asm code basically moves the content of the string to esi then a bunch of parameters are filled to do an api call.



There is also a conditional jump of ne(not equal).

Decompiler

```
int32_t var_49h;  
int32_t var_4dh;  
int32_t var_51h;  
int32_t var_55h;  
int32_t var_6bh;  
ecx = 0xe;  
esi = "http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrgwea.com";  
edi = &var_8h;  
eax = 0;
```

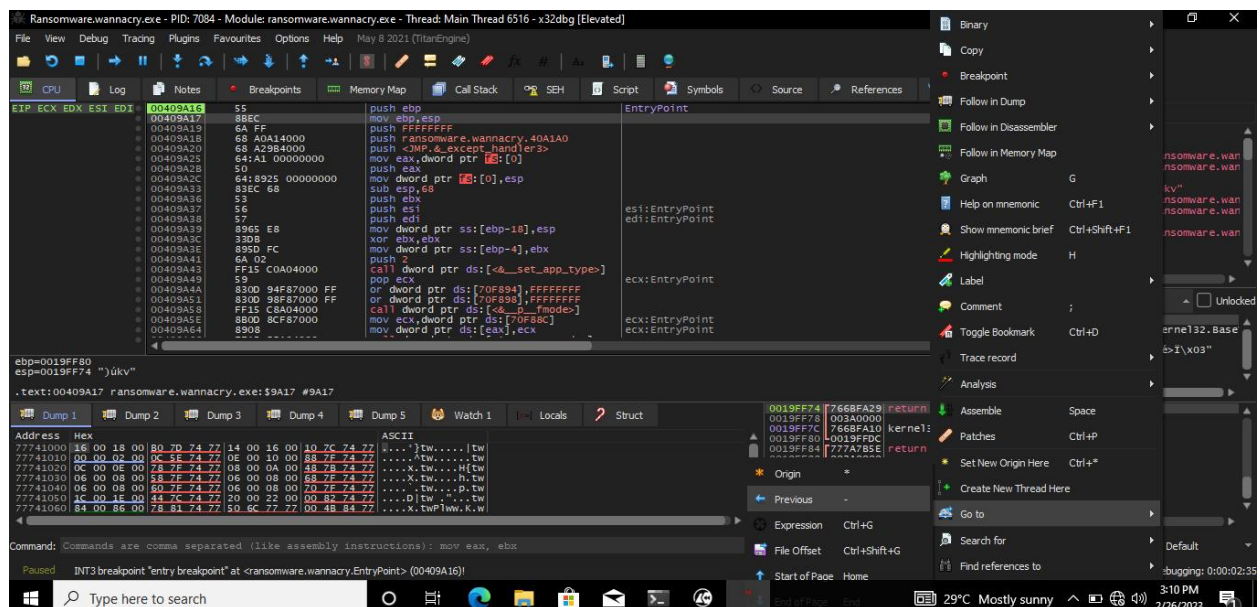
```
do {  
    *(es:edi) = *(esi);  
    ecx--;  
    esi += 4;  
    es:edi += 4;  
} while (ecx != 0);  
*(es:edi) = *(esi);  
esi++;  
es:edi++;  
eax = InternetOpenA (eax, 1, eax, eax, eax, eax, eax, ax, al);  
ecx = &var_14h;  
esi = eax;  
eax = InternetOpenUrlA (esi, ecx, 0, 0, 0x84000000, 0);  
edi = eax;  
esi = imp.InternetCloseHandle;  
if (edi == 0) {  
    void (*esi)() ();  
    void (*esi)(uint32_t) (0);  
    eax = fcn_00408090 ();  
    eax = 0;  
    return eax;  
}  
void (*esi)() ();  
eax = void (*esi)(uint32_t) (edi);  
eax = 0;  
return eax;  
}
```

Here we can better understand how the condition works. API is placed in eax then parameters are filled. A check is performed to see if edi is equal to zero. If it is, then the code declares a function pointer, assigns a function pointer of type void (*)(uint32_t) to it with a parameter value of zero, calls the fcn_00408090 function, sets eax to 0, and returns eax.

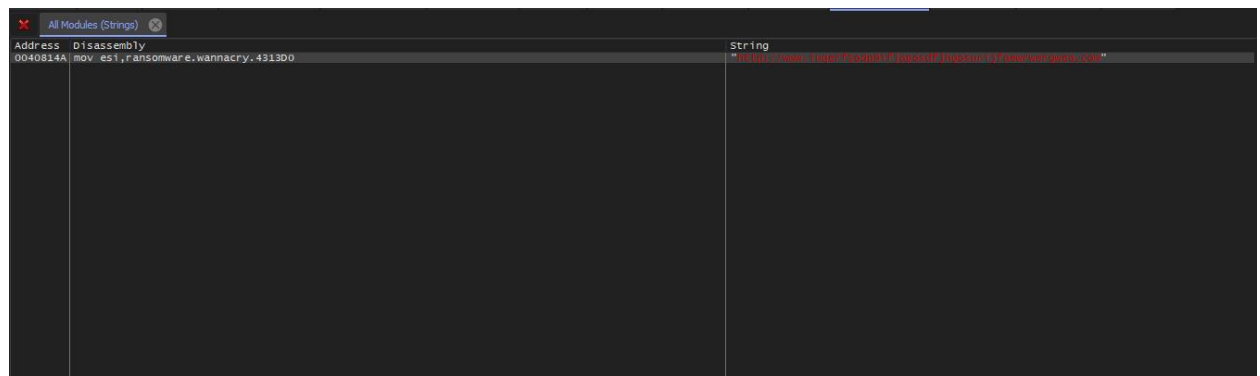
If edi is not equal to zero, the code declares a function pointer, assigns a function pointer of type void (*)(uint32_t) to it with a parameter value of edi, sets eax to 0, and returns eax which calls InternetOpenUrlA.

Advanced Dynamic Analysis

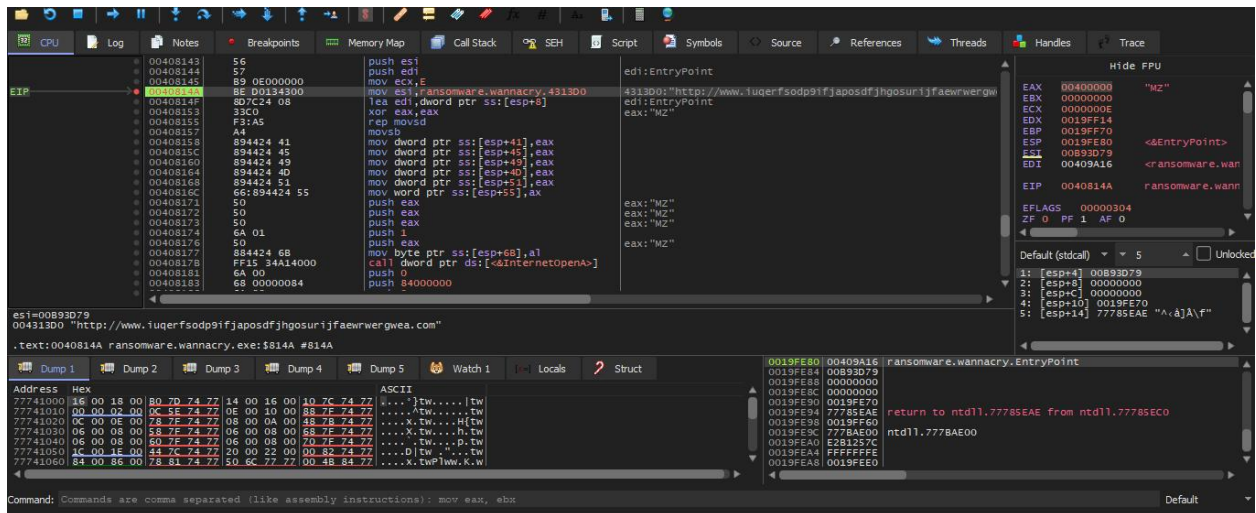
X32 dbg



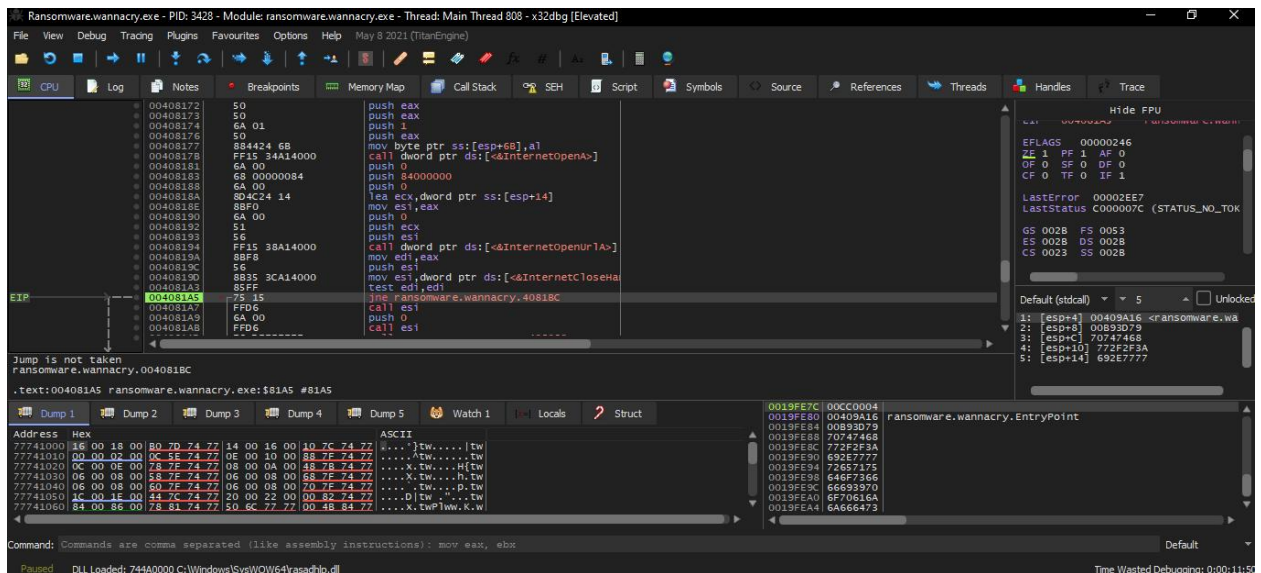
Here we will try to find the string with the url and set our breakpoint there.



We have successfully found our string, now we click the instruction to go there immediately.



Now we are in the instruction, we now set our break point.

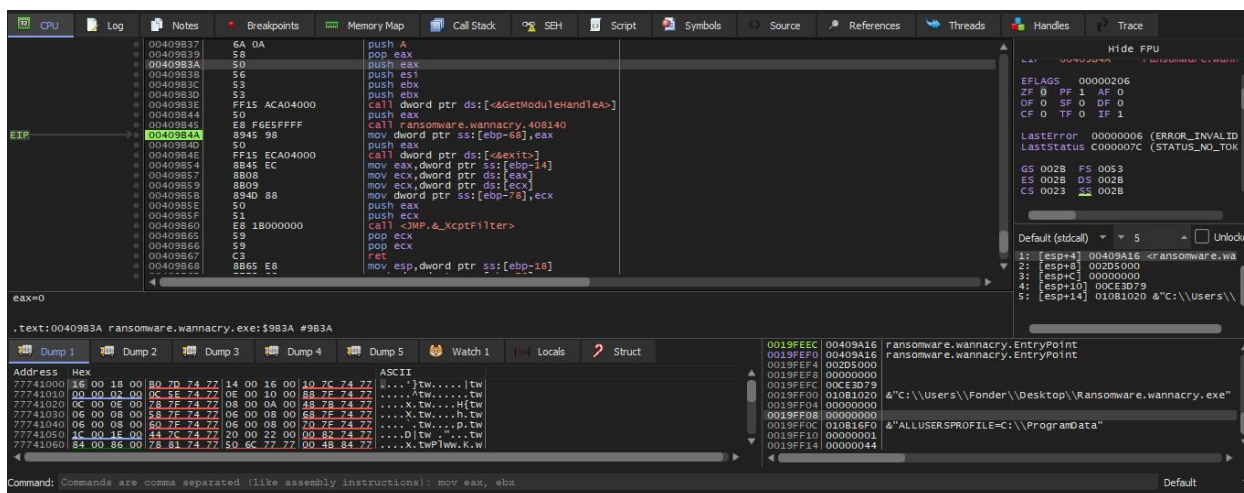


Here we are at the conditional jump.

004081A3	85FF	mov esi,dword ptr ds:[&InternetCtrosen
004081A5	75 15	jne ransomware.wannacry.4081BC
004081A7	FFD6	call esi
004081A9	6A 00	push 0
004081AB	FFD6	call esi
004081AD	E8 DEFEFFFF	call ransomware.wannacry.408090
004081B2	5F	pop edi
004081B3	33C0	xor eax,eax
004081B5	5E	pop esi
004081B6	83C4 50	add esp,50
004081B9	C2 1000	ret 10
004081BC	FFD6	call esi
004081BE	57	push edi
004081BF	FFD6	call esi

Now we have our self a conditional jump of not equal similar to the one we saw in cutter. If ZF(zero flag) is set to 0 it will jump to the end and continue the rest instructions.

Since we did a simple dynamic analysis with inetsim we can conclude that this has to do with the strange url. If the malware connects to it(ZF = 1) it exits otherwise it just runs completely(ZF = 0).



Since we set the ZF value to 0 even if we turn on inetsim it will still run and execute the rest of it's instructions and exit out completely.

Indicators of Compromise

The full list of IOCs can be found in the Appendices.

Network Indicators

Capturing from enp0s3						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
Apply a display filter ... <Ctrl-F>						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.0.3	10.0.0.2	DHCP	332	DHCP Request - Transaction ID 0xd3ef5c16
2	0.002849576	10.0.0.2	10.0.0.3	DHCP	590	DHCP ACK - Transaction ID 0xd3ef5c16
3	4.487491504	10.0.0.4	10.0.0.3	DNS	109	Standard query 0xb162 A www.iuqerfsodp9ifjapoc
4	4.495498320	10.0.0.3	10.0.0.4	DNS	125	Standard query response 0xb162 A www.iuqerfsod
5	4.499516264	10.0.0.4	10.0.0.3	TCP	66	1077 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
6	4.499547384	10.0.0.3	10.0.0.4	TCP	66	80 → 1077 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
7	4.499688101	10.0.0.4	10.0.0.3	TCP	60	1077 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
8	4.500277261	10.0.0.4	10.0.0.3	HTTP	154	GET / HTTP/1.1
9	4.500283671	10.0.0.3	10.0.0.4	TCP	54	80 → 1077 [ACK] Seq=1 Ack=101 Win=64256 Len=0
10	4.507900794	10.0.0.3	10.0.0.4	TCP	204	80 → 1077 [PSH, ACK] Seq=1 Ack=101 Win=64256 Len=0
11	4.508121024	10.0.0.4	10.0.0.3	TCP	60	1077 → 80 [ACK] Seq=101 Ack=151 Win=261888 Len=0
12	4.508132784	10.0.0.3	10.0.0.4	HTTP	312	HTTP/1.1 200 OK (text/html)
13	4.508269114	10.0.0.4	10.0.0.3	TCP	60	1077 → 80 [ACK] Seq=101 Ack=409 Win=261632 Len=0
<ul style="list-style-type: none"> Frame 8: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) on interface enp0s3, id 0 Ethernet II, Src: PcsCompu 55:06:07 (08:00:27:55:06:07), Dst: PcsCompu 25:8f:13 (08:00:27:25:8f:13) Internet Protocol Version 4, Src: 10.0.0.4, Dst: 10.0.0.3 Transmission Control Protocol, Src Port: 1077, Dst Port: 80, Seq: 1, Ack: 1, Len: 100 Hypertext Transfer Protocol <ul style="list-style-type: none"> GET / HTTP/1.1\r\n Host: www.iuqerfsodp9ifjapocdfjhgosurijfaewrergwea.com\r\n Cache-Control: no-cache\r\n \r\n [Full request URI: http://www.iuqerfsodp9ifjapocdfjhgosurijfaewrergwea.com/] [HTTP request 1/1] [Response in frame: 12] 						
0000	08 00 27 25 8f 13 08 00	27 55 06 07 00 00	45 00	
0010	00 8c 1d 14 40 00 00 06	c9 51 0a 00 00 04 0a 00
0020	00 03 04 35 00 50 99 c1	b5 95 5f a1 93 5e 50 18
0030	04 00 03 c8 00 00 47 45	54 20 2f 20 48 54 54 50
0040	2f 31 2e 31 0d 0a 48 6f	73 74 3a 20 77 77 77 2e
0050	69 75 71 65 72 66 73 6f	64 70 39 69 66 6a 61 70
0060	6f 73 64 66 6a 68 67 6f	73 75 72 69 6a 66 61 65
0070	77 72 77 65 72 67 77 65	61 2e 63 6f 6d 0d 0a 43
0080	61 63 68 65 2d 43 6f 6e	74 72 6f 6c 3a 20 6e 6f
0090	2d 63 61 63 68 65 0d 0a	0d 0a

Fig 3: WireShark Packet Capture of HTTP GET Request

The binary tries to access the weird url.

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	Sent Packets
lsass.exe	592	TCPv6	Listen	::	49664	::	0	9/4/2021 3:57:11 PM	lsass.exe	0
lsass.exe	592	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	9/4/2021 3:57:11 PM	lsass.exe	0
Ransomware.wannacr...	2172	TCP	Syn Sent	169.254.243.48	23820	169.254.40.1	445	10/17/2021 8:54:10 AM	mssecsv2.0	
Ransomware.wannacr...	2172	TCP	Syn Sent	169.254.243.48	23799	169.254.24.1	445	10/17/2021 8:54:08 AM	mssecsv2.0	
Ransomware.wannacr...	2172	TCP	Syn Sent	169.254.243.48	23798	169.254.23.1	445	10/17/2021 8:54:07 AM	mssecsv2.0	
Ransomware.wannacr...	2172	TCP	Syn Sent	169.254.243.48	23823	169.254.43.1	445	10/17/2021 8:54:10 AM	mssecsv2.0	
Ransomware.wannacr...	2172	TCP	Syn Sent	169.254.243.48	23824	169.254.44.1	445	10/17/2021 8:54:10 AM	mssecsv2.0	
Ransomware.wannacr...	2172	TCP	Syn Sent	169.254.243.48	23825	169.254.45.1	445	10/17/2021 8:54:10 AM	mssecsv2.0	
Ransomware.wannacr...	2172	TCP	Syn Sent	169.254.243.48	23826	169.254.46.1	445	10/17/2021 8:54:10 AM	mssecsv2.0	
Ransomware.wannacr...	2172	TCP	Syn Sent	169.254.243.48	23827	169.254.47.1	445	10/17/2021 8:54:10 AM	mssecsv2.0	
Ransomware.wannacr...	2172	TCP	Syn Sent	169.254.243.48	23806	169.254.30.1	445	10/17/2021 8:54:08 AM	mssecsv2.0	
Ransomware.wannacr...	2172	TCP	Syn Sent	169.254.243.48	23829	169.254.49.1	445	10/17/2021 8:54:10 AM	mssecsv2.0	
Ransomware.wannacr...	2172	TCP	Syn Sent	169.254.243.48	23831	169.254.50.1	445	10/17/2021 8:54:10 AM	mssecsv2.0	
Ransomware.wannacr...	2172	TCP	Syn Sent	169.254.243.48	23832	169.254.51.1	445	10/17/2021 8:54:10 AM	mssecsv2.0	
Ransomware.wannacr...	2172	TCP	Syn Sent	169.254.243.48	23834	169.254.52.1	445	10/17/2021 8:54:10 AM	mssecsv2.0	
Ransomware.wannacr...	2172	TCP	Syn Sent	169.254.243.48	23797	169.254.22.1	445	10/17/2021 8:54:07 AM	mssecsv2.0	
Ransomware.wannacr...	2172	TCP	Syn Sent	169.254.243.48	23804	169.254.29.1	445	10/17/2021 8:54:08 AM	mssecsv2.0	
Ransomware.wannacr...	2172	TCP	Syn Sent	169.254.243.48	23807	169.254.31.1	445	10/17/2021 8:54:08 AM	mssecsv2.0	
Ransomware.wannacr...	2172	TCP	Syn Sent	169.254.243.48	23796	169.254.21.1	445	10/17/2021 8:54:07 AM	mssecsv2.0	
Ransomware.wannacr...	2172	TCP	Syn Sent	169.254.243.48	23803	169.254.28.1	445	10/17/2021 8:54:08 AM	mssecsv2.0	
Ransomware.wannacr...	2172	TCP	Syn Sent	169.254.243.48	23802	169.254.27.1	445	10/17/2021 8:54:08 AM	mssecsv2.0	
Ransomware.wannacr...	2172	TCP	Syn Sent	169.254.243.48	23801	169.254.26.1	445	10/17/2021 8:54:08 AM	mssecsv2.0	
Ransomware.wannacr...	2172	TCP	Syn Sent	169.254.243.48	23800	169.254.25.1	445	10/17/2021 8:54:08 AM	mssecsv2.0	
services.exe	584	TCPv6	Listen	::	49669	::	0	9/4/2021 3:57:14 PM	services.exe	0
services.exe	584	TCP	Listen	0.0.0.0	49669	0.0.0.0	0	9/4/2021 3:57:14 PM	services.exe	0
spoolsv.exe	1756	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	9/4/2021 3:57:13 PM	Spooler	0
spoolsv.exe	1756	TCPv6	Listen	::	49668	::	0	9/4/2021 3:57:13 PM	Spooler	0

Endpoints: 79 Established: Listening: 23 Time Wait: Close Wait: Update: 2 sec States: (All)

Fig 4: TCPView A flood of numerous SMB connection requests to non-private remote addresses.

Host-based Indicators

Process Tree

☐ Only show processes still running at end of current trace
☒ Timelines cover displayed events only

Process	Description	Image Path	Life Time	Company	Owner	Comr
winlogon.exe (612)	Windows Logon A...	C:\Windows\sys...		Microsoft Corporat...	NT AUTHORITY\...	winlog
fontdrvhost.exe (840)	Font Driver Host...	C:\Windows\sys...		Microsoft Corporat...	Font Driver Host...	"fontc
dwm.exe (72)	Desktop Window ...	C:\Windows\sys...		Microsoft Corporat...	Window Manager...	"dwm
Explorer.EXE (3576)	Windows Explorer	C:\Windows\Expl...		Microsoft Corporat...	DESKTOP-FLC8U...	C:\Wi
SecurityHealthSystray.exe (477)	Windows Security...	C:\Windows\Syst...		Microsoft Corporat...	DESKTOP-FLC8U...	"C:\W
VBxTray.exe (1948)	VirtualBox Guest ...	C:\Windows\Syst...		Oracle and/or its ...	DESKTOP-FLC8U...	"C:\W
OneDrive.exe (5164)	Microsoft OneDrive	C:\Users\Fonder\...		Microsoft Corporat...	DESKTOP-FLC8U...	"C:\U
msedge.exe (5236)	Microsoft Edge	C:\Program Files (...)		Microsoft Corporat...	DESKTOP-FLC8U...	"C:\P
msedge.exe (5352)	Microsoft Edge	C:\Program Files (...)		Microsoft Corporat...	DESKTOP-FLC8U...	"C:\P
msedge.exe (5704)	Microsoft Edge	C:\Program Files (...)		Microsoft Corporat...	DESKTOP-FLC8U...	"C:\P
msedge.exe (5716)	Microsoft Edge	C:\Program Files (...)		Microsoft Corporat...	DESKTOP-FLC8U...	"C:\P
msedge.exe (5736)	Microsoft Edge	C:\Program Files (...)		Microsoft Corporat...	DESKTOP-FLC8U...	"C:\P
PEView.exe (5516)	PE/COFF File Vie...	C:\ProgramData\...		Wayne J. Radburn	DESKTOP-FLC8U...	"C:\P
Procmon.exe (6444)	Process Monitor	C:\Tools\sysintem...		Sysinternals - ww...	DESKTOP-FLC8U...	"C:\T
Procmon64.exe (4924)	Process Monitor	C:\Users\Fonder\...		Sysinternals - ww...	DESKTOP-FLC8U...	"C:\U
Ransomware.wannacr.exe (1884)	Microsoft® Disk D...	C:\Users\Fonder\...		Microsoft Corporat...	DESKTOP-FLC8U...	"C:\U
tasksche.exe (6864)	DiskPart	C:\WINDOWS\ta...		Microsoft Corporat...	DESKTOP-FLC8U...	C:\W

Description: Microsoft® Disk Defragmenter
Company: Microsoft Corporation
Path: C:\Users\Fonder\Desktop\Ransomware.wannacr.exe
Command: "C:\Users\Fonder\Desktop\Ransomware.wannacr.exe"
User: DESKTOP-FLC8UB9\Fonder
PID: 1884 **Started:** 2/27/2023 6:35:06 AM **Exited:** 2/27/2023 6:35:15 AM

Go To Event Include Process Include Subtree Close

Fig 5: Process Tree Ransomware.wannacry.exe is present along with another stage 2 payload.

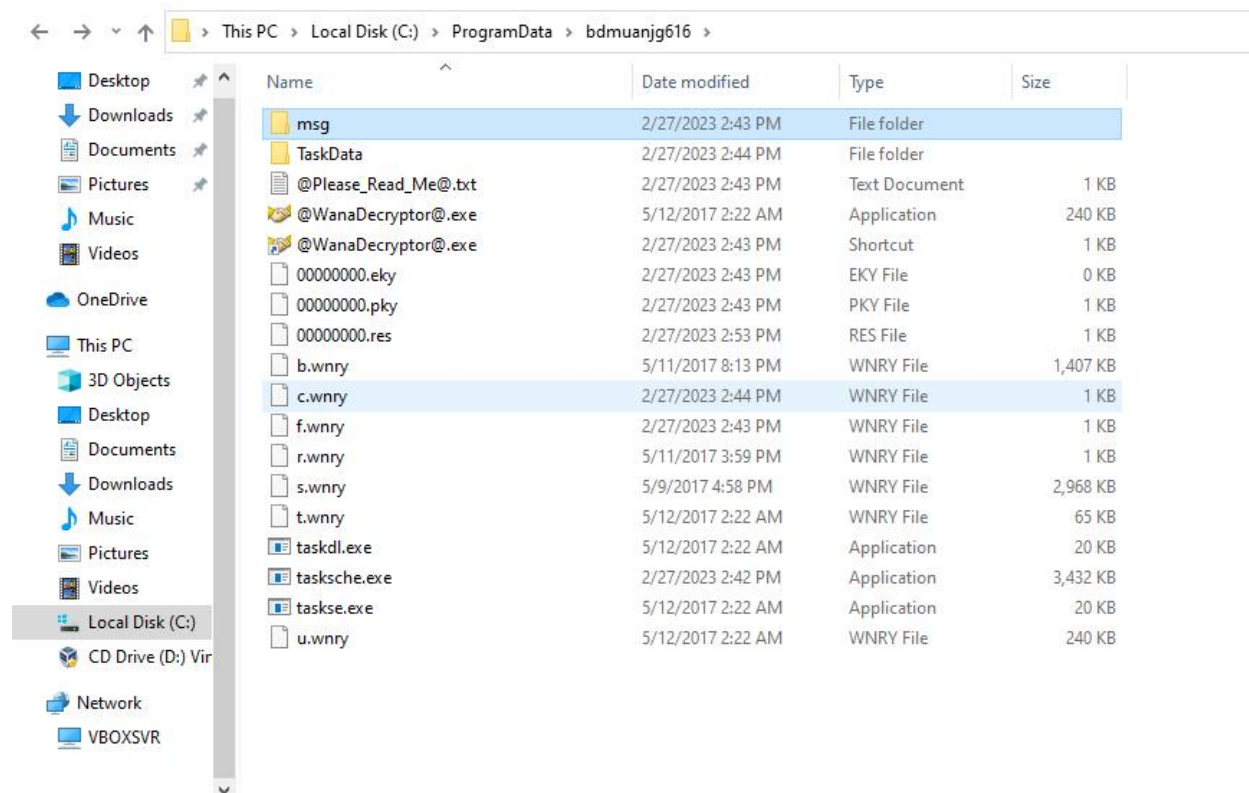


Fig 6: New folder created, seen in Procmon with a random generated chars.

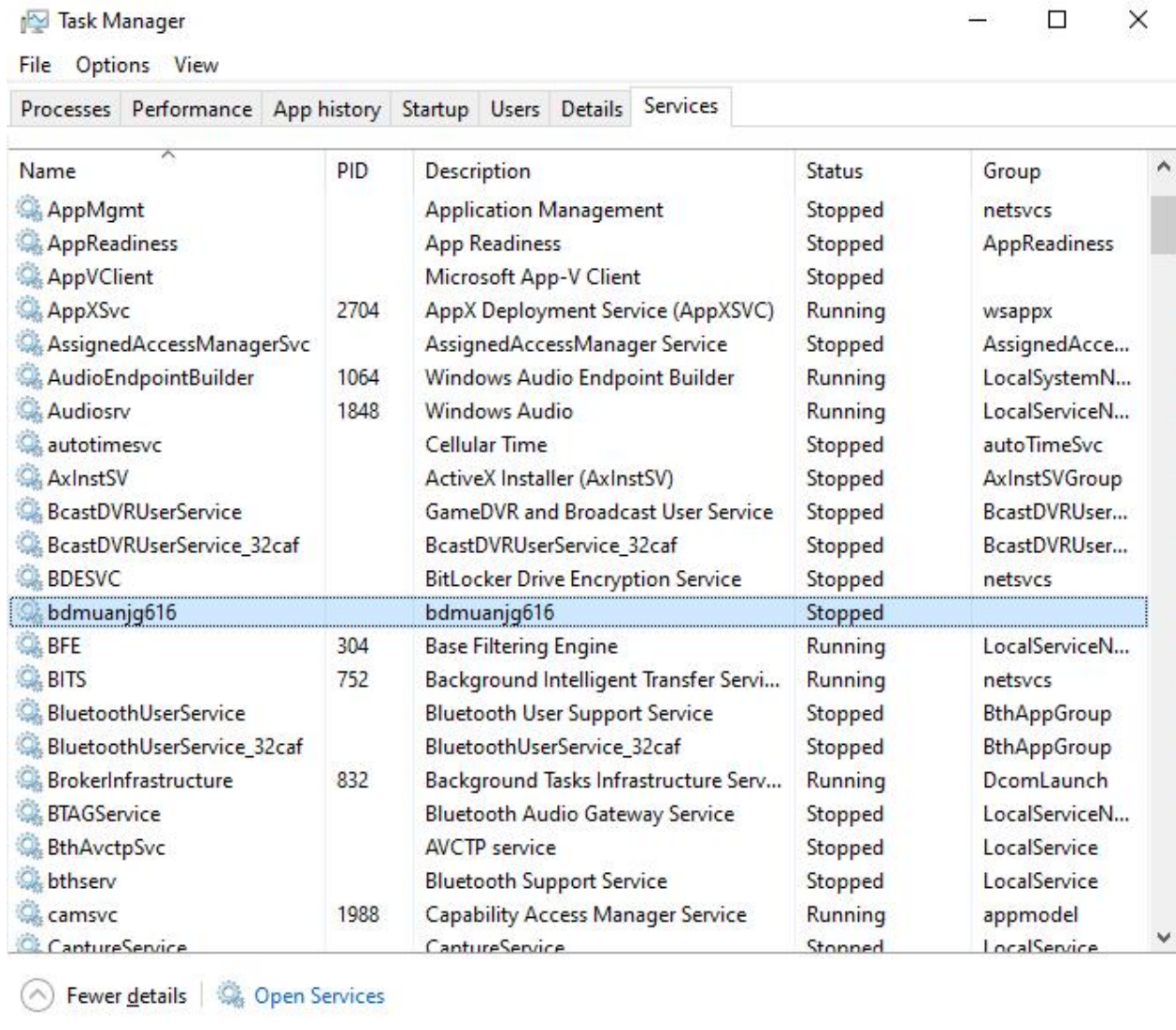


Fig 7: Persistent service, has the same name with the folder created.

Rules & Signatures

Appendices

A. Yara Rules

Full Yara repository located at:

```
rule WannaCry_Detection {
  meta:
    description = "Matches a collection of strings from Wannacry"
    author = "FonderElite"
    date = "2023-02-28"
    reference = "Ransomware.wannacry.exe"
    category = "security"
  strings:
    $str1 = "%s -m security"
    $str2 = "C:\\%s\\qeriuwjhrf"
    $str3 = "tasksche.exe"
    $str4 = "icaccls . /grant Everyone:F /T /C /Q"
    $str5 = "WNCry@2017"
    $str6 = "http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com"
  condition:
    any of ($str*) or all of them
}
```

```
C:\Users\Fonder\Desktop
λ yara64 yaratest.yara -w -p 32 Ransomware.wannacry.exe
string_rule Ransomware.wannacry.exe
```

B. Callback URLs

Domain	Port
http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com	80

C. Decompiled Code Snippets

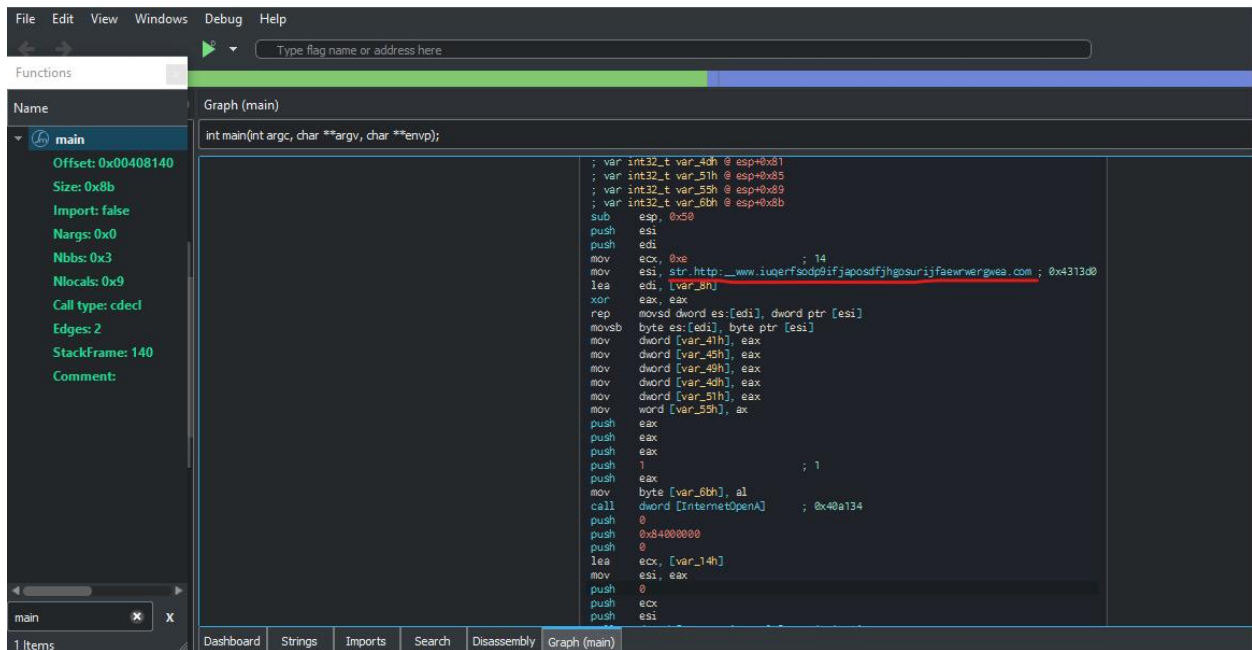


Fig 6: Opens a URL and closes itself upon a condition.