



# Practical Malware Analysis & Triage

## Malware Analysis Report

### WannaCry Ransomware

Feb 2023 | Sochurthy | v1.0

## Contents

Executive Summary .....	3
High-Level Technical Summary .....	4
Malware Composition.....	5
Basic Static Analysis .....	6
Basic Dynamic Analysis .....	8
Advanced Static Analysis.....	10
Advanced Dynamic Analysis.....	11
Indicators of Compromise.....	15
Rules & Signatures .....	19

## Executive Summary

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

WannaCry is a ransomware worm that encrypts the files and spreads itself to the network. Microsoft Visual C ++compiled that runs on 32 bits windows operating system. First identified on May of 2017.

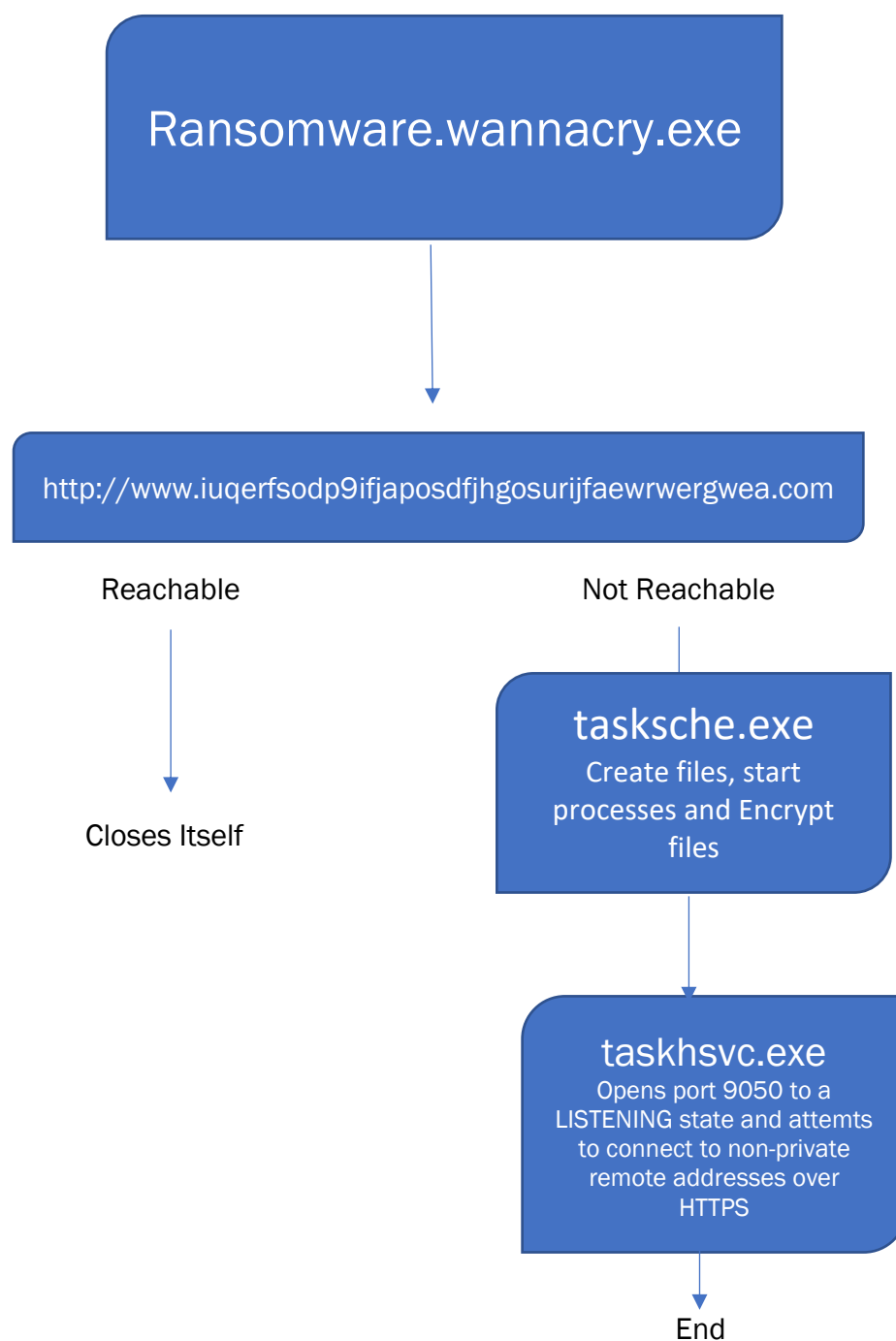
### How it works?

It uses an API "InternetOpenUrlA" to test if the url "<http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com>" is reachable, if so, it spawns the payload "Tasksche.exe" that creates files, encrypt files, "taskhsvc.exe" opens port 9050 to a LISTENING state and attempts to connect to non-private remote addresses over HTTPS. If not, it deletes itself.

### Symptoms of infection?

The wallpaper changes on the infected host plus a program shows up indicating that the host has been infected and the files are encrypted with the appearance of @WanaDecryptor@ "executable file" and @Please\_Read\_Me@ text file on the Desktop

## High-Level Technical Summary



WannaCry consists of the following components:

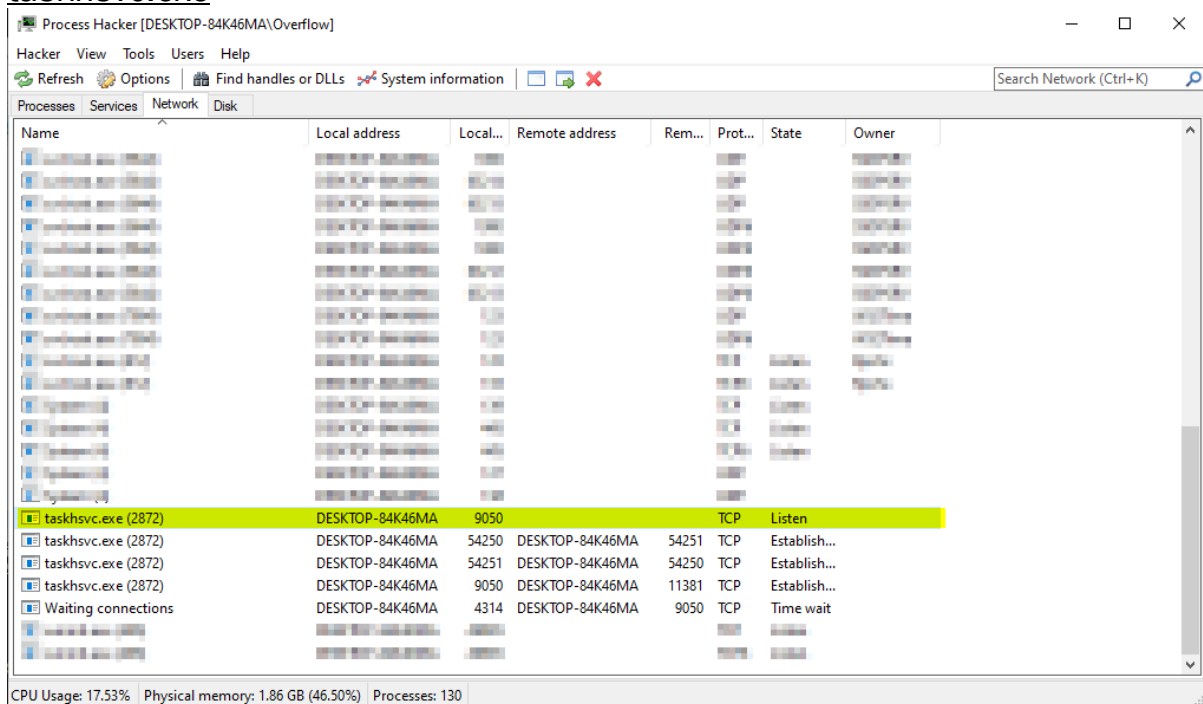
File Name	SHA256 Hash
tasksche.exe	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
taskhsvc.exe	8ac6dc5bb016afc869fcbb713f6a14d3692e866b94f4f1ee83b09a7506a8cb5876
tor.exe	e48673680746fbe027e8982f62a83c298d6fb46ad9243de8e79b7e5a24dcd4eb
taskse.exe	2ca2d550e603d74dedda03156023135b38da3630cb014e3d00b1263358c5f00
taskdl.exe	4a468603fdbc7a2eb5770705898cf9ef37aade532a7964642ecd705a74794b79
@WanaDecryptor@.exe	b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25

[illegible]

## Create files, start processes and Encrypt files

WannaCry Ransomware  
Feb 2023  
v1.0

## taskhsvc.exe



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

## Basic Static Analysis

- Extract strings using Floss



WannaCry Ransomware  
Feb 2023  
v1.0

## Example of suspicious strings

tasksche.exe  
t.wnry  
WNcry@2ol7  
WanaCrypt0r  
[\\192.168.56.20\IPC\\$](http://192.168.56.20\IPC$)  
diskpart.exe  
lhdfrgui.exe  
<http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com>  
SMB2

## - CFF - mz ascii

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 . . . . .
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	F8	00	00	00	. . . . .
00000040	0E	1F	BA	0E	00	B4	09	CD	21	E8	01	4C	CD	21	54	68	. . . . .
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program cannot
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	55	3C	53	90	11	5D	3D	C3	11	5D	3D	C3	11	5D	3D	C3	U<S . . . . .
00000090	6A	41	31	C3	10	5D	3D	C3	92	41	33	C3	15	5D	3D	C3	jA1A . . . . .
000000A0	7E	42	37	C3	1A	5D	3D	C3	7E	42	36	C3	10	5D	3D	C3	~B7A . . . . .
000000B0	7E	42	39	C3	15	5D	3D	C3	D2	52	60	C3	1A	5D	3D	C3	~B9A . . . . .
000000C0	11	5D	3B	C3	4A	5D	3D	C3	27	7B	36	C3	10	5D	3D	C3	0 <A . . . . .
000000D0	D6	5B	3B	C3	10	5D	3D	C3	52	69	63	68	11	5D	3D	C3	O[ .A . . . . .
000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	. . . . .
000000F0	00	00	00	00	00	00	00	50	45	00	00	4C	01	04	00	00	. . . . .
00000100	CC	8E	E7	4C	00	00	00	00	00	00	00	E0	00	0F	01	00	i i c L . . . . .
00000110	0B	01	06	00	00	90	00	00	00	30	38	00	00	00	00	00	. . . . .
00000120	16	9A	00	00	00	10	00	00	00	A0	00	00	00	00	40	00	. . . . .
00000130	00	10	00	00	00	10	00	00	04	00	00	00	00	00	00	00	. . . . .
00000140	04	00	00	00	00	00	00	00	00	B0	66	00	00	10	00	00	. . . . .
00000150	00	00	00	00	02	00	00	00	00	10	00	00	10	00	00	00	. . . . .
00000160	00	00	10	00	00	10	00	00	00	00	00	00	10	00	00	00	. . . . .
00000170	00	00	00	00	00	00	00	E0	A1	00	00	A0	00	00	00	00	. . . . .
00000180	00	00	31	00	54	A4	35	00	00	00	00	00	00	00	00	00	. . . . .
00000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	. . . . .
000001A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	. . . . .

property	value
md5	DB349B97C37D22F5EA1D1841E3C89EB4
sha1	E889544AFF83FFAF8B0DDA705105DEE7C97FE26
sha256	24D004A104D4D54034DBCFC2A4B19A11F39008A575AA614EA04703480B1022C
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF 00 00 B8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
first-bytes-text	MZ . . . . .
file-size	3723264 bytes
entropy	7.964
imphash	n/a
signature	Microsoft Visual C++ v6.0
tooling	wait...
entry-point	55 8B EC 6A FF 68 A0 A1 40 00 68 A2 9B 40 00 64 A1 00 00 00 00 50 64 89 25 00 00 00 00 83 EC 68 53
file-version	6.1.7601.17514 (win7sp1_rtm.101119-1850)
description	Microsoft® Disk Defragmenter
file-type	executable
cpu	32-bit
subsystem	GUI
compiler-stamp	Sat Nov 20 09:03:08 2010 UTC
debugger-stamp	n/a
resources-stamp	0x00000000
import-stamp	0x00000000
exports-stamp	n/a

WannaCry Ransomware  
Feb 2023  
v1.0

## - PESTUDIO:

pestudio 9.46 - Malware Initial Assessment - www.wintor.com - [c:\users\overflow\desktop\ransomware.wannacry.exe.malz]

file settings about

c:\users\overflow\desktop\ransomware.wannacry.exe

imports (91)

imports (91)	flag (28)	first-thunk-original (INT)	first-thunk (IAT)	hint	group (10)	type (1)	ordinal (13)	library
StartServiceCtrlDispatcherA	x	0x0000A6F6	0x0000A6F6	586 (0x024A)	services	implicit	-	ADVAPI32.dll
ChangeServiceConfig2A	x	0x0000A6C0	0x0000A6C0	52 (0x0034)	services	implicit	-	ADVAPI32.dll
CreateServiceA	x	0x0000A688	0x0000A688	100 (0x0064)	services	implicit	-	ADVAPI32.dll
QueryPerformanceFrequency	x	0x0000A43A	0x0000A43A	676 (0x02A4)	reconnaissance	implicit	-	KERNEL32.dll
3 (closesocket)	x	0x80000003	0x80000003	0 (0x0000)	network	implicit	x	WS2_32.dll
16 (recv)	x	0x80000010	0x80000010	0 (0x0000)	network	implicit	x	WS2_32.dll
19 (send)	x	0x80000013	0x80000013	0 (0x0000)	network	implicit	x	WS2_32.dll
8 (htonl)	x	0x80000008	0x80000008	0 (0x0000)	network	implicit	x	WS2_32.dll
14 (ntohl)	x	0x8000000E	0x8000000E	0 (0x0000)	network	implicit	x	WS2_32.dll
115 (WSAStartup)	x	0x80000073	0x80000073	0 (0x0000)	network	implicit	x	WS2_32.dll
12 (inet_ntoa)	x	0x8000000C	0x8000000C	0 (0x0000)	network	implicit	x	WS2_32.dll
10 (ioctlsocket)	x	0x8000000A	0x8000000A	0 (0x0000)	network	implicit	x	WS2_32.dll
18 (select)	x	0x80000012	0x80000012	0 (0x0000)	network	implicit	x	WS2_32.dll
9 (htons)	x	0x80000009	0x80000009	0 (0x0000)	network	implicit	x	WS2_32.dll
23 (socket)	x	0x80000017	0x80000017	0 (0x0000)	network	implicit	x	WS2_32.dll
4 (connect)	x	0x80000004	0x80000004	0 (0x0000)	network	implicit	x	WS2_32.dll
11 (inet_addr)	x	0x8000000B	0x8000000B	0 (0x0000)	network	implicit	x	WS2_32.dll
GetAdaptersInfo	x	0x0000A792	0x0000A792	28 (0x001C)	network	implicit	-	iphlpapi.dll
InternetOpenA	x	0x0000A7DC	0x0000A7DC	146 (0x0092)	network	implicit	-	WININET.dll
InternetOpenUrlA	x	0x0000A7C8	0x0000A7C8	147 (0x0093)	network	implicit	-	WININET.dll
InternetCloseHandle	x	0x0000A7B2	0x0000A7B2	105 (0x0069)	network	implicit	-	WININET.dll
MoveFileExA	x	0x0000A576	0x0000A576	623 (0x026F)	file	implicit	-	KERNEL32.dll
GetCurrentThreadId	x	0x0000A524	0x0000A524	326 (0x0146)	execution	implicit	-	KERNEL32.dll
GetCurrentThread	x	0x0000A53A	0x0000A53A	325 (0x0145)	execution	implicit	-	KERNEL32.dll
CryptGenRandom	x	0x0000A630	0x0000A630	150 (0x0096)	cryptography	implicit	-	ADVAPI32.dll
CryptAcquireContextA	x	0x0000A638	0x0000A638	133 (0x0085)	cryptography	implicit	-	ADVAPI32.dll

### Some red flags imports

## Basic Dynamic Analysis

### Running the malware using a fake internet to see the result (inetsim)

Capturing from Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
5	2.688882	10.0.0.5	10.0.0.4	DNS	125	Standard query response 0xe898 A www.iuqerfsodp9ifajposdfjhgousurijfaewwergwea.com A 10.0.0.5
6	2.694094	10.0.0.4	10.0.0.5	TCP	66	49735 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
7	2.694403	10.0.0.5	10.0.0.4	TCP	66	80 → 49735 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
8	2.694458	10.0.0.4	10.0.0.5	TCP	54	49735 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
9	2.694625	10.0.0.4	10.0.0.5	HTTP	154	GET / HTTP/1.1
10	2.694929	10.0.0.5	10.0.0.4	TCP	60	80 → 49735 [ACK] Seq=1 Ack=101 Win=64256 Len=0
11	2.721221	10.0.0.5	10.0.0.4	TCP	204	80 → 49735 [PSH, ACK] Seq=1 Ack=101 Win=64256 Len=150 [TCP segment of a reassembled PDU]
12	2.721258	10.0.0.4	10.0.0.5	TCP	54	49735 → 80 [ACK] Seq=101 Ack=151 Win=261888 Len=0
13	2.722017	10.0.0.5	10.0.0.4	HTTP	312	HTTP/1.1 200 OK (text/html)
14	2.722047	10.0.0.4	10.0.0.5	TCP	54	49735 → 80 [ACK] Seq=101 Ack=409 Win=261632 Len=0
15	2.722646	10.0.0.4	10.0.0.5	TCP	54	49735 → 80 [FIN, ACK] Seq=101 Ack=409 Win=261632 Len=0
16	2.722679	10.0.0.4	10.0.0.5	TCP	54	49735 → 80 [RST, ACK] Seq=102 Ack=409 Win=0 Len=0

Frame 9: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) on interface \Device\NPF... Ethernet II, Src: PcsCompu\_50:d9:98 (08:00:27:50:d9:98), Dst: PcsCompu\_50:7c:a0 (08:00:00:00:00:00)

Internet Protocol Version 4, Src: 10.0.0.4, Dst: 10.0.0.5

Transmission Control Protocol, Src Port: 49735, Dst Port: 80, Seq: 1, Ack: 1, Len: 100

Hypertext Transfer Protocol

GET / HTTP/1.1\r\n

Host: www.iuqerfsodp9ifajposdfjhgousurijfaewwergwea.com\r\n

Cache-Control: no-cache\r\n

\r\n

[Full request URI: http://www.iuqerfsodp9ifajposdfjhgousurijfaewwergwea.com/]

[HTTP request 1/1]

[Response in frame: 13]

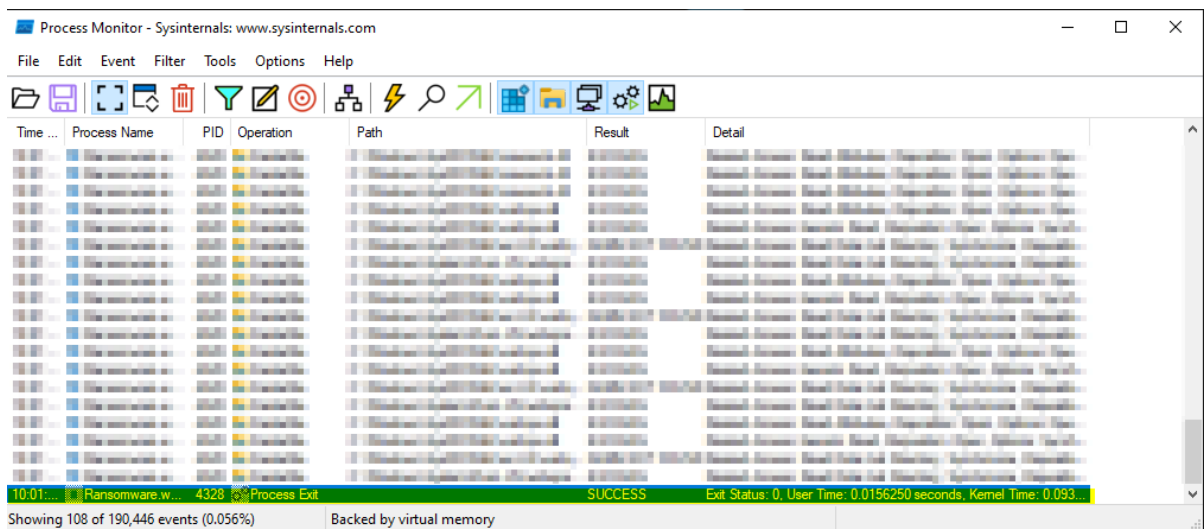
Ethernet: <live capture in progress>

Packets: 111 · Displayed: 111 (100.0%)

Profile: Default

The malware end itself after reaching out the server





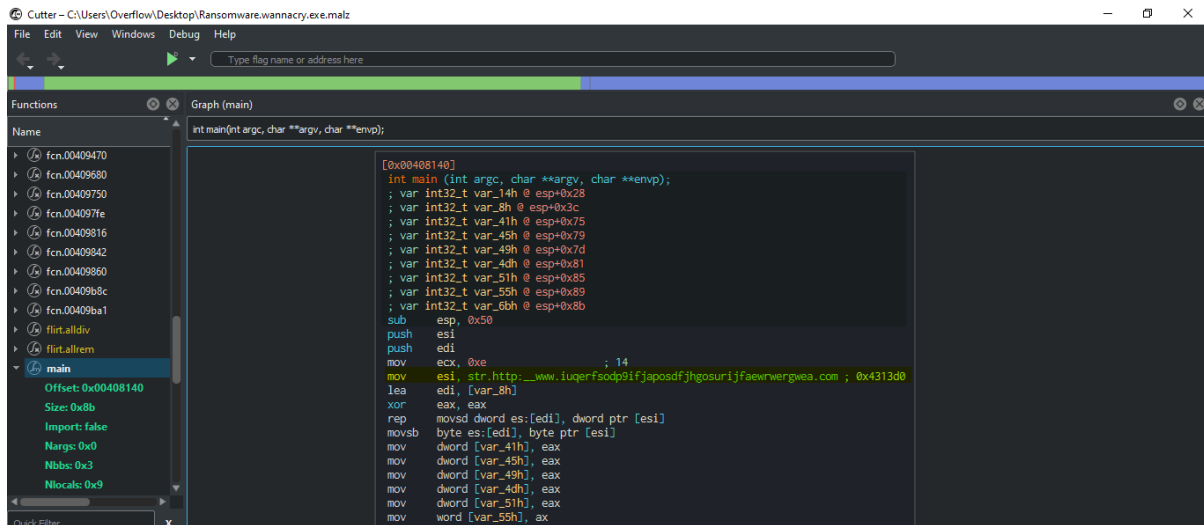
The malware end itself after reaching out the server

For so, let's try to run the ransomware without using inetsim to see how the malware will behave!

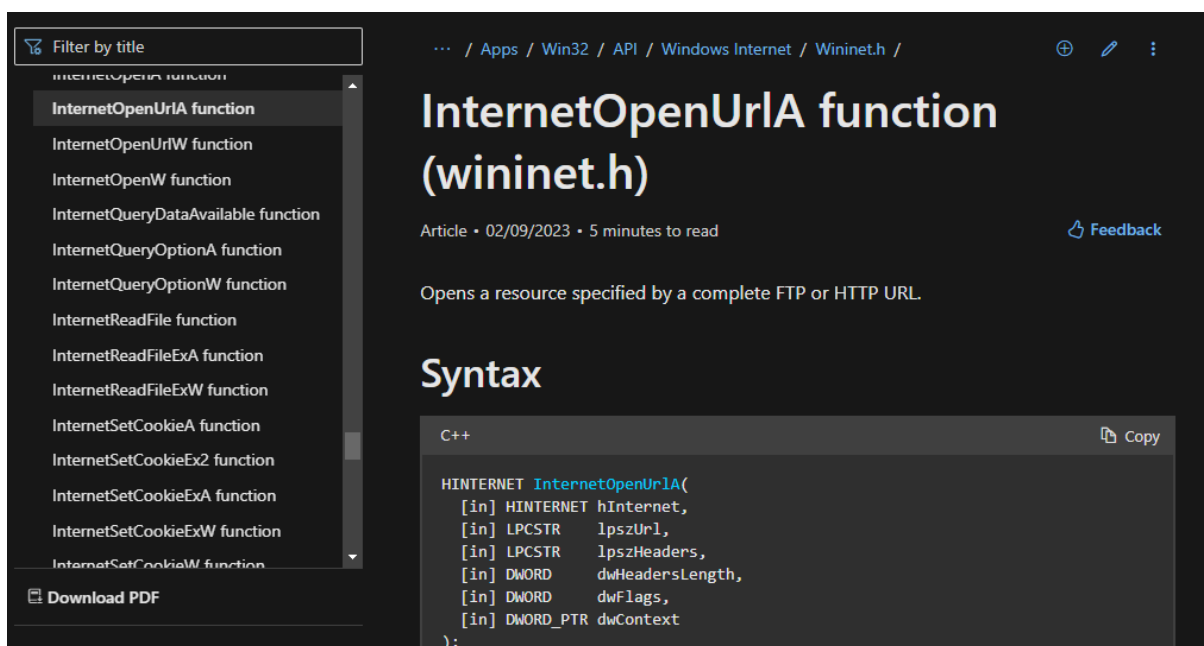
```
Simulation running.
C:\> C:\Program Files\WannaCrypt\WannaCrypt.exe
+ trap 00000000 - stopped (PDB 00000000)
+ sample 00000000 - stopped (PDB 00000000)
+ sample 00000000 - stopped (PDB 00000000)
+ sample 00000000 - stopped (PDB 00000000)
+ sample 00000000 - stopped (PDB 00000000)
+ sample 00000000 - stopped (PDB 00000000)
+ sample 00000000 - stopped (PDB 00000000)
+ sample 00000000 - stopped (PDB 00000000)
+ sample 00000000 - stopped (PDB 00000000)
+ sample 00000000 - stopped (PDB 00000000)
Simulation stopped.
Report written to C:\Program Files\WannaCrypt\WannaCrypt.exe (PDB 00000000)
```

If he can't reach out to the server, the ransomware runs

# Advanced Static Analysis



In the main function, we notice the url that the malware tries to reach out, moving it to the esi, and calling the "InternetOpenUrlA" API

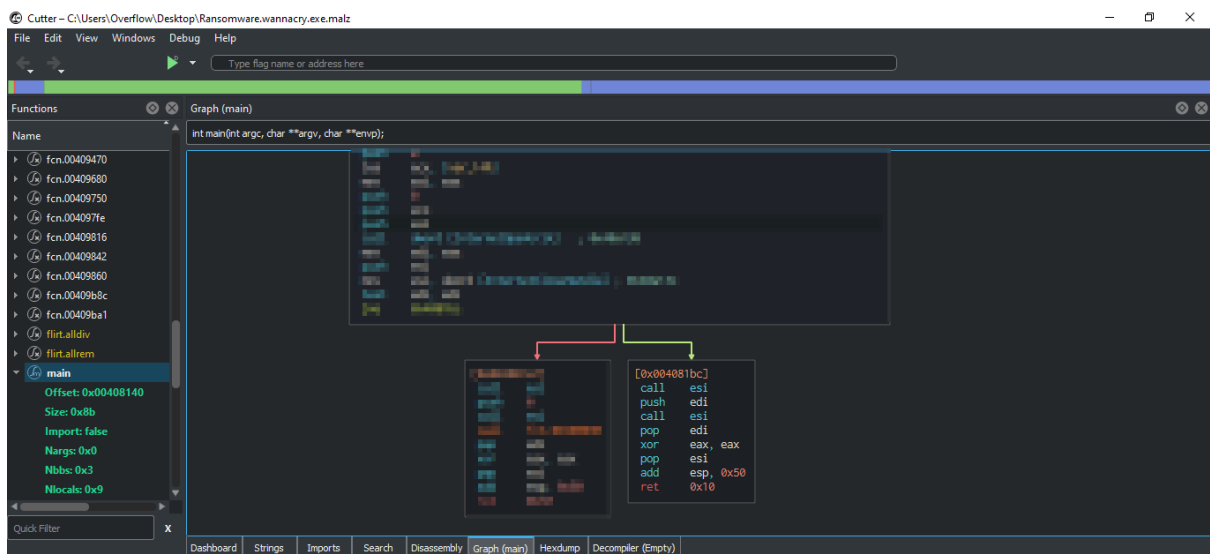


## Return value

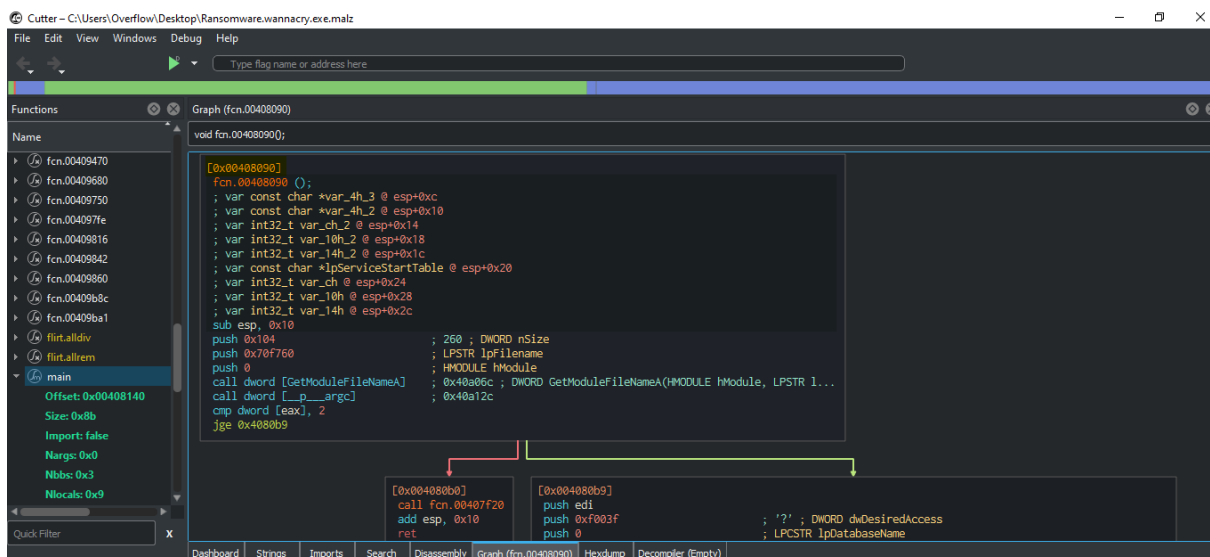
Returns a valid handle to the URL if the connection is successfully established, or **NULL** if the connection fails. To retrieve a specific error message, call **GetLastError**. To determine why access to the service was denied, call **InternetGetLastResponseInfo**.

If it reaches out the url, to malware closes itself => value 1

WannaCry Ransomware  
Feb 2023  
v1.0



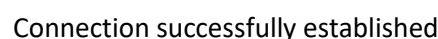
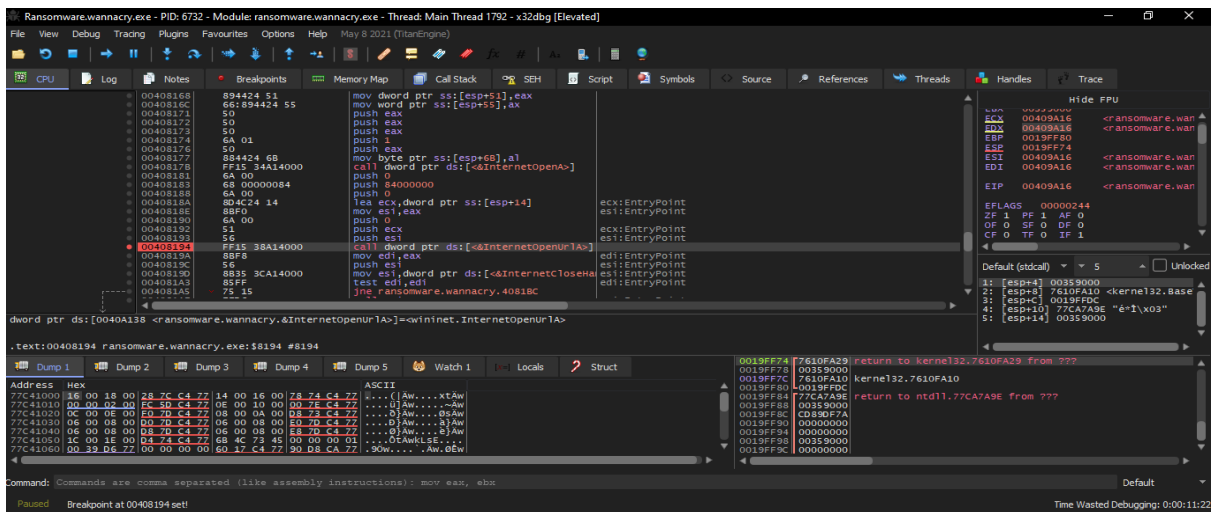
If not, the malware calls fcn.00408090 (payload)



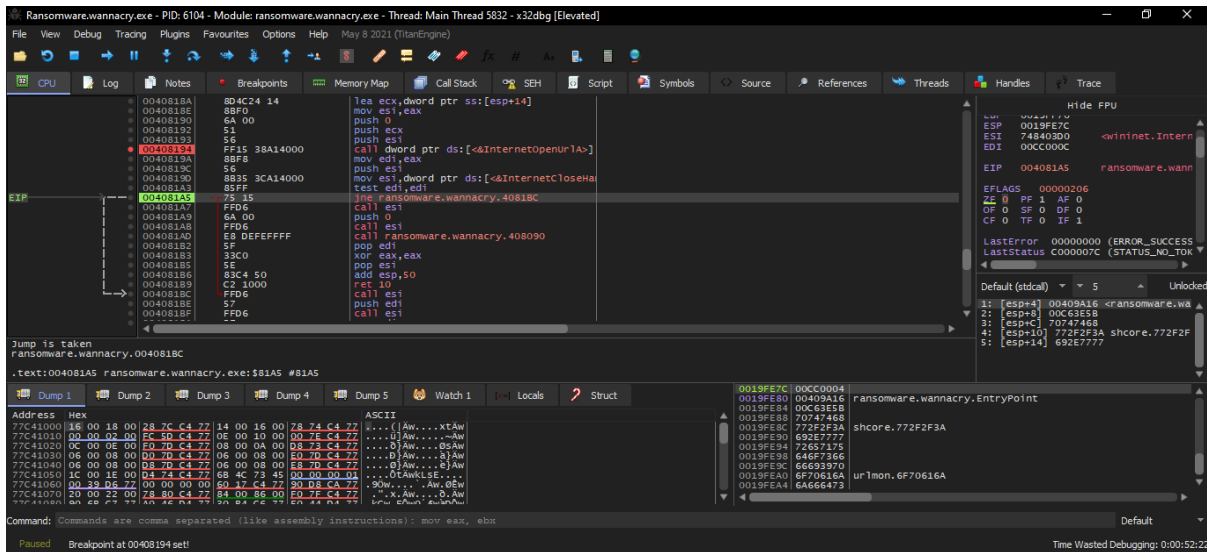
## Advanced Dynamic Analysis

Using x32db, let's search for the API "InternetOpenUrlA" and the Url <http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com> and setting them as breakpoints to see how the malware will behave, also we'll try to change the zero flag value to see if the malware will call fcn.00408090 (payload) even if it reaches out the Url, for so, we'll use the fake internet "inetsim".

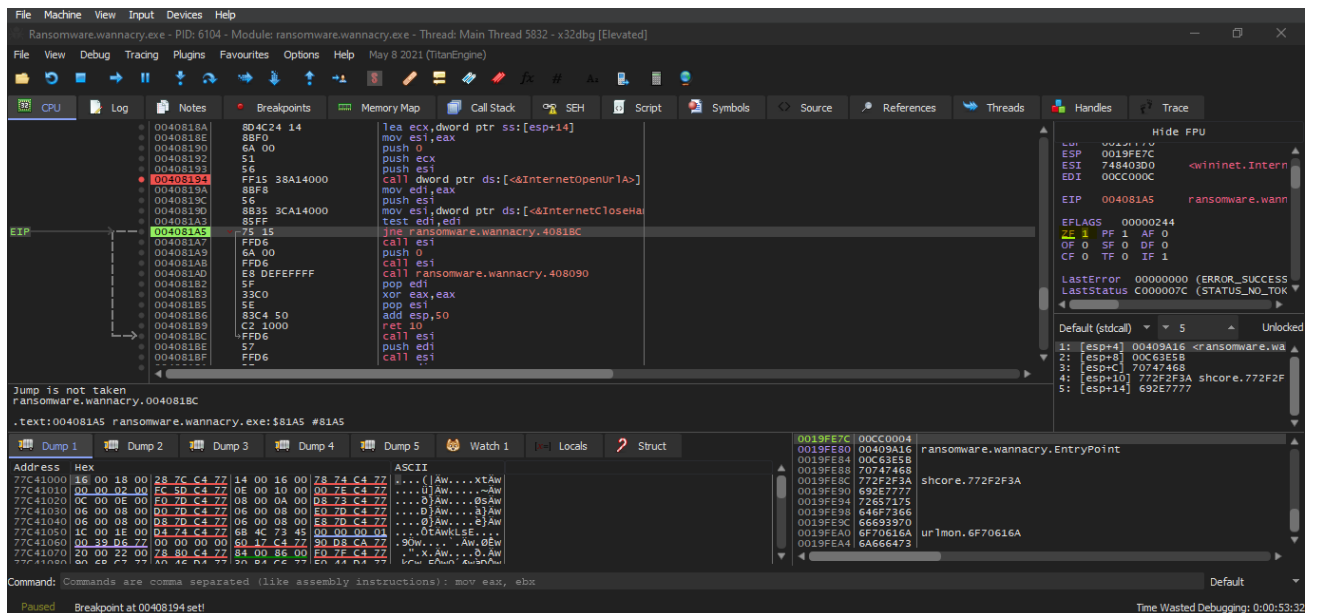




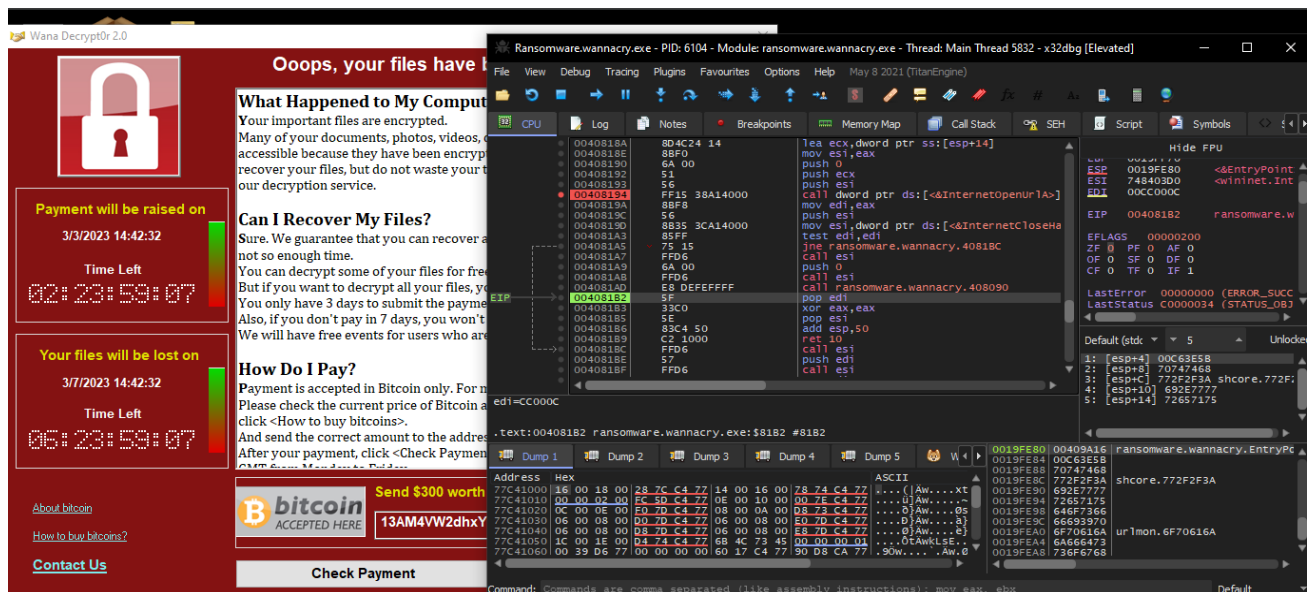
WannaCry Ransomware  
Feb 2023  
v1.0



Let's change the zf value to 1  
 PS => zf => 1 => the value is 0 means we haven't reached out the Url



WannaCry Ransomware  
 Feb 2023  
 v1.0



## Indicators of Compromise

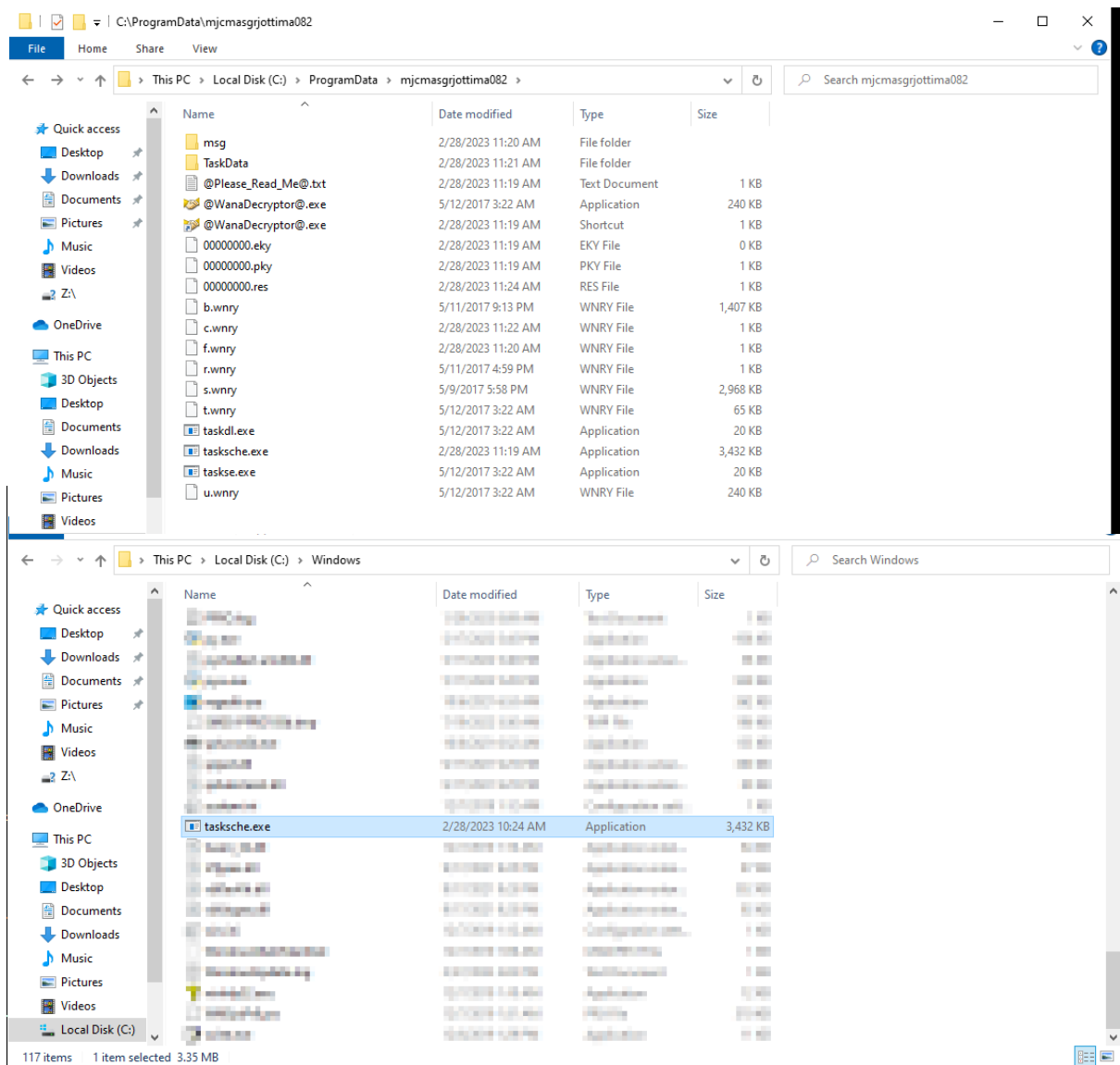
### 1- file creation :

Process Monitor - Sysinternals: www.sysinternals.com

Time ...	Process Name	PID	Operation	Path	Result	Detail
10:24:...	Ransomware.w...	7340	CreateFile	C:\Windows\SysWOW64\rsadshlp.dll	SUCCESS	Desired Access: R...
10:24:...	Ransomware.w...	7340	CreateFile	C:\Windows\SysWOW64\rsadshlp.dll	SUCCESS	Desired Access: R...
10:24:...	Ransomware.w...	5548	CreateFile	C:\Windows\tasksche.exe	NAME NOT FOUND	Desired Access: R...
10:24:...	Ransomware.w...	7340	CreateFile	C:\Users\Overflow\Desktop\CRYPTSP.dll	NAME NOT FOUND	Desired Access: R...
10:24:...	Ransomware.w...	7340	CreateFile	C:\Windows\SysWOW64\cryptsp.dll	SUCCESS	Desired Access: R...
10:24:...	Ransomware.w...	7340	CreateFile	C:\Windows\SysWOW64\cryptsp.dll	SUCCESS	Desired Access: R...
10:24:...	Ransomware.w...	7340	CreateFile	C:\Windows\SysWOW64\rsasenh.dll	SUCCESS	Desired Access: R...
10:24:...	Ransomware.w...	7340	CreateFile	C:\Windows\SysWOW64\rsasenh.dll	SUCCESS	Desired Access: R...
10:24:...	Ransomware.w...	7340	CreateFile	C:\Users\Overflow\Desktop\CRYPTBASE.dll	NAME NOT FOUND	Desired Access: R...
10:24:...	Ransomware.w...	7340	CreateFile	C:\Windows\SysWOW64\cryptbase.dll	SUCCESS	Desired Access: R...
10:24:...	Ransomware.w...	7340	CreateFile	C:\Windows\SysWOW64\cryptbase.dll	SUCCESS	Desired Access: R...
10:24:...	Ransomware.w...	7340	CreateFile	C:\Users\Overflow\Desktop\Ransomware.wannacry.exe	SUCCESS	Desired Access: G...
10:24:...	Ransomware.w...	5548	CreateFile	C:\Windows\tasksche.exe	SUCCESS	Desired Access: G...
10:24:...	Ransomware.w...	5548	CreateFile	C:\Windows\tasksche.exe	SUCCESS	Desired Access: R...
10:24:...	Ransomware.w...	5548	CreateFile	C:\Windows\tasksche.exe	SUCCESS	Desired Access: R...
10:24:...	Ransomware.w...	5548	CreateFile	C:\Windows\tasksche.exe	SUCCESS	Desired Access: R...
10:24:...	Ransomware.w...	5548	CreateFile	C:\Windows\tasksche.exe	SUCCESS	Desired Access: R...
10:24:...	Ransomware.w...	5548	CreateFile	C:\Windows\apppatch\sysmain.sdb	SUCCESS	Desired Access: G...
10:24:...	Ransomware.w...	5548	CreateFile	C:\Windows\apppatch\sysmain.sdb	SUCCESS	Desired Access: G...
10:24:...	Ransomware.w...	5548	CreateFile	C:\Windows\apppatch\sysmain.sdb	SUCCESS	Desired Access: G...

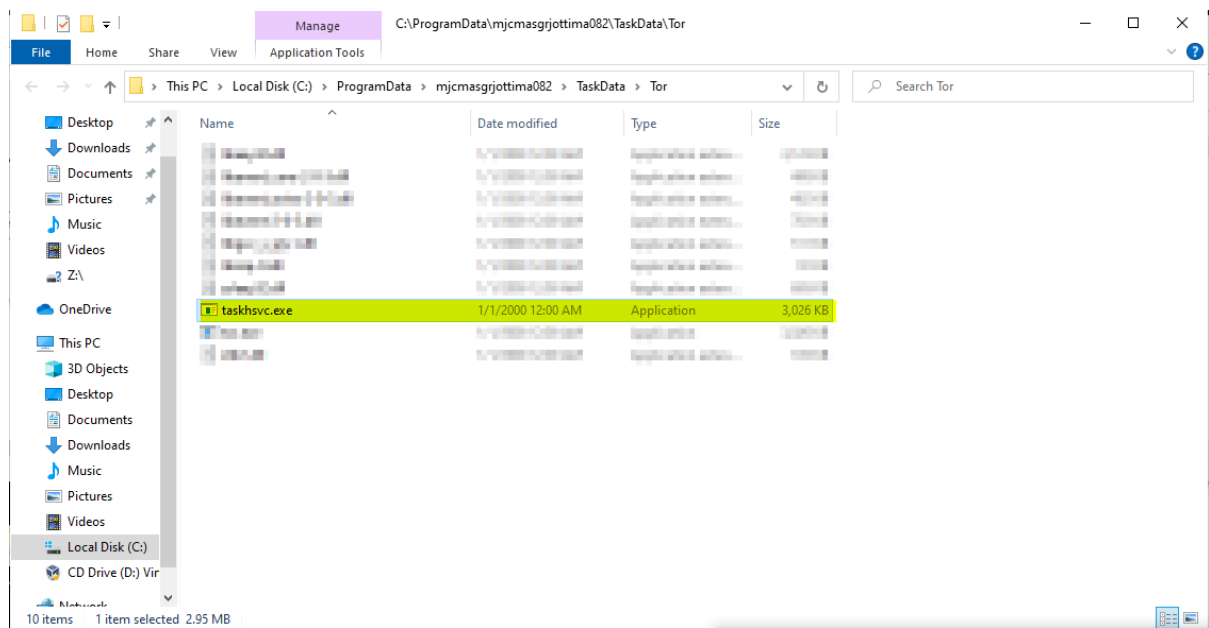
Showing 207 of 1,486,849 events (0.013%) Backed by virtual memory

WannaCry Ransomware  
Feb 2023  
v1.0



WannaCry Ransomware  
Feb 2023  
v1.0





WannaCry Ransomware  
Feb 2023  
v1.0

## 2- Network

Wireshark network traffic capture showing a SYN flood attack. The packet list shows multiple SYN packets from 10.0.0.4 to 10.0.0.6 on port 445. The packet details for packet 204 show a Transmission Control Protocol (TCP) segment with sequence number 1 and destination port 445. The packet bytes show the raw data of the SYN packet.

No.	Time	Source	Destination	Protocol	Length	Info
194	32.506611	PcsCompu_50:d9:98	Broadcast	ARP	42	Who has 10.0.0.24? Tell 10.0.0.4
195	32.506628	PcsCompu_50:d9:98	Broadcast	ARP	42	Who has 10.0.0.25? Tell 10.0.0.4
196	32.587279	10.0.0.4	10.0.0.5	DNS	81	Standard query 0xad3a PTR 3.0.0.10.in-addr.arpa
197	32.631377	10.0.0.4	10.0.0.5	DNS	81	Standard query 0x47f2 PTR 7.0.0.10.in-addr.arpa
198	32.662460	10.0.0.4	10.0.0.5	DNS	81	Standard query 0xa37e PTR 8.0.0.10.in-addr.arpa
199	32.664681	PcsCompu_50:d9:98	Broadcast	ARP	42	Who has 10.0.0.29? Tell 10.0.0.4
200	32.757824	10.0.0.4	10.0.0.6	TCP	66	49712 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
201	32.758195	10.0.0.6	10.0.0.4	TCP	66	445 → 49712 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
202	32.758275	10.0.0.4	10.0.0.6	TCP	54	49712 → 445 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
203	32.758356	10.0.0.4	10.0.0.6	SMB	191	Negotiate Protocol Request
204	32.758645	10.0.0.6	10.0.0.4	TCP	60	445 → 49712 [RST, ACK] Seq=1 Ack=138 Win=0 Len=0
205	32.831707	PcsCompu_50:d9:98	Broadcast	ARP	42	Who has 10.0.0.30? Tell 10.0.0.4

Frame 204: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0  
 Ethernet II, Src: 0a:00:27:00:00:11 (0a:00:27:00:00:11), Dst: PcsCompu\_50:d9:98  
 Internet Protocol Version 4, Src: 10.0.0.6, Dst: 10.0.0.4  
 Transmission Control Protocol, Src Port: 445, Dst Port: 49712, Seq: 1, Ack: 138, Win: 0, Len: 0  
 Source Port: 445  
 Destination Port: 49712  
 [Stream index: 4]  
 [Conversation completeness: Complete, WITH\_DATA (47)]  
 [TCP Segment Len: 0]  
 Sequence Number: 1 (relative sequence number)  
 Sequence Number (raw): 4051638428  
 [Next Sequence Number: 1 (relative sequence number)]

The malware tries to spread itself over the network, the attack uses SMB and TCP port 445 to propagate

Ransomware.wannacr...	1772	TCP	Syn Sent	10.0.0.4	49789	10.0.0.87	445	2/28/2023 10:38:03
Ransomware.wannacr...	1772	TCP	Syn Sent	10.0.0.4	49790	10.0.0.88	445	2/28/2023 10:38:03
Ransomware.wannacr...	1772	TCP	Syn Sent	10.0.0.4	49791	10.0.0.89	445	2/28/2023 10:38:03
Ransomware.wannacr...	1772	TCP	Syn Sent	10.0.0.4	49793	10.0.0.90	445	2/28/2023 10:38:03
Ransomware.wannacr...	1772	TCP	Syn Sent	10.0.0.4	49794	10.0.0.91	445	2/28/2023 10:38:03
Ransomware.wannacr...	1772	TCP	Syn Sent	10.0.0.4	49796	10.0.0.92	445	2/28/2023 10:38:03
Ransomware.wannacr...	1772	TCP	Syn Sent	10.0.0.4	49797	10.0.0.93	445	2/28/2023 10:38:03
Ransomware.wannacr...	1772	TCP	Syn Sent	10.0.0.4	49799	10.0.0.94	445	2/28/2023 10:38:03
Ransomware.wannacr...	1772	TCP	Syn Sent	10.0.0.4	49800	10.0.0.95	445	2/28/2023 10:38:03
Ransomware.wannacr...	1772	TCP	Syn Sent	10.0.0.4	49801	10.0.0.96	445	2/28/2023 10:38:03
Ransomware.wannacr...	1772	TCP	Syn Sent	10.0.0.4	49760	10.0.0.67	445	2/28/2023 10:38:03
Ransomware.wannacr...	1772	TCP	Syn Sent	10.0.0.4	49768	10.0.0.73	445	2/28/2023 10:38:03
Ransomware.wannacr...	1772	TCP	Syn Sent	10.0.0.4	49761	10.0.0.68	445	2/28/2023 10:38:03
Ransomware.wannacr...	1772	TCP	Syn Sent	10.0.0.4	49762	10.0.0.69	445	2/28/2023 10:38:03
Ransomware.wannacr...	1772	TCP	Syn Sent	10.0.0.4	49770	10.0.0.74	445	2/28/2023 10:38:03

WannaCry Ransomware  
 Feb 2023  
 v1.0

## Tasksvcs opens port 9050 to a listen state

Process Hacker [DESKTOP-84K46MA\Overflow]

Hacker View Tools Users Help

Refresh Options Find handles or DLLs System information Search Network (Ctrl+K)

Processes Services Network Disk

Name	Local address	Local...	Remote address	Rem...	Prot...	State	Owner
tasksvcs.exe (2872)	DESKTOP-84K46MA	9050			TCP	Listen	tasksvcs.exe
tasksvcs.exe (2872)	DESKTOP-84K46MA	54250	DESKTOP-84K46MA	54251	TCP	Establish...	tasksvcs.exe
tasksvcs.exe (2872)	DESKTOP-84K46MA	54251	DESKTOP-84K46MA	54250	TCP	Establish...	tasksvcs.exe
tasksvcs.exe (2872)	DESKTOP-84K46MA	9050	DESKTOP-84K46MA	11381	TCP	Establish...	tasksvcs.exe
Waiting connections	DESKTOP-84K46MA	4314	DESKTOP-84K46MA	9050	TCP	Time wait	tasksvcs.exe

CPU Usage: 17.53% Physical memory: 1.86 GB (46.50%) Processes: 130

## Rules & Signatures

```
rule Detect
{
    meta:
        description = "Detect wannacry"
    strings:
        $s1 =
            "http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com"
        $s2 = "InternetOpenUrlA"
        $s3 = "tasksche"
        $s4 = "smb"
    condition:
        (all of them)
}
```

Cmder

```
C:\Users\Overflow\Desktop
λ yara64.exe -s -r wannacry.yara Ransomware.wannacry.exe
Detect Ransomware.wannacry.exe
0x313d0:$s1: http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
0xa7ca:$s2: InternetOpenUrlA
0x3136c:$s3: tasksche
0x4157c:$s3: tasksche
0x35f1eb:$s4: smb

C:\Users\Overflow\Desktop
λ
```

WannaCry Ransomware  
Feb 2023  
v1.0

