Malware Analysis Report

Ransomware.wannacry.exe

March 2023

Ido Abramov

Table of contents

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.

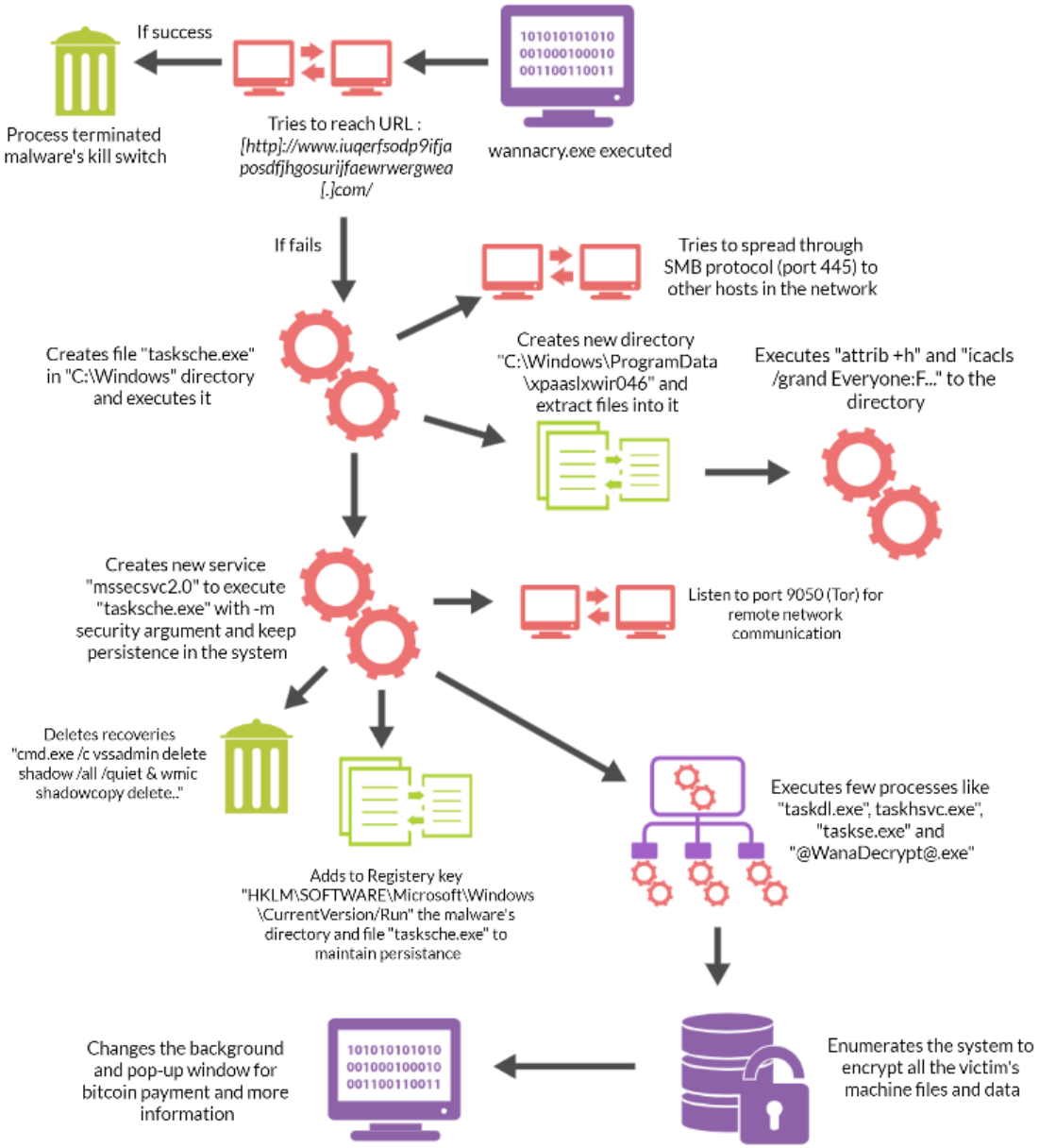
The authors demanded bitcoin payment to perform decryption of the encrypted files.

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

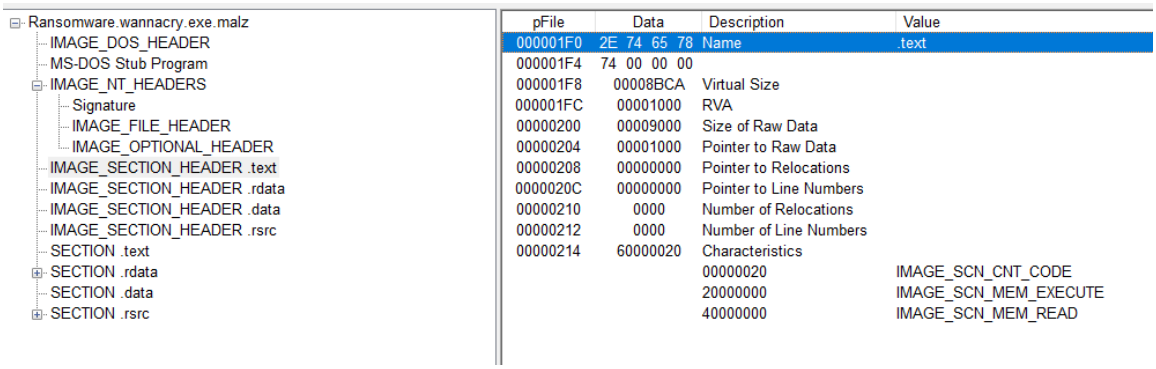
- **Additional related files hash values**

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**:



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@2ol7 r.wnry s.wnry t.wnry taskdl.exe taskse.exe u.wnry	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]
	Debugger Detection::Timing/Delay Check QueryPerformanceCounter [B0001.033]
ANTI-STATIC ANALYSIS	Disassembler Evasion::Argument Obfuscation [B0012.001]
COMMAND AND CONTROL	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

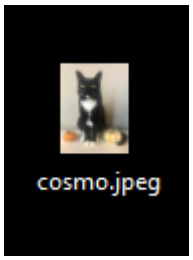
In conclusion, it can be inferred that the malware has cryptographic, anti-analysis, network communication and system manipulation (files, processes and services) capabilities. It indicates the general behavior of the malware while examining it dynamically.

Dynamic analysis

Activation of *wannacry.exe* – immediate visual symptoms

Executing the malware requires administrator authorizations.

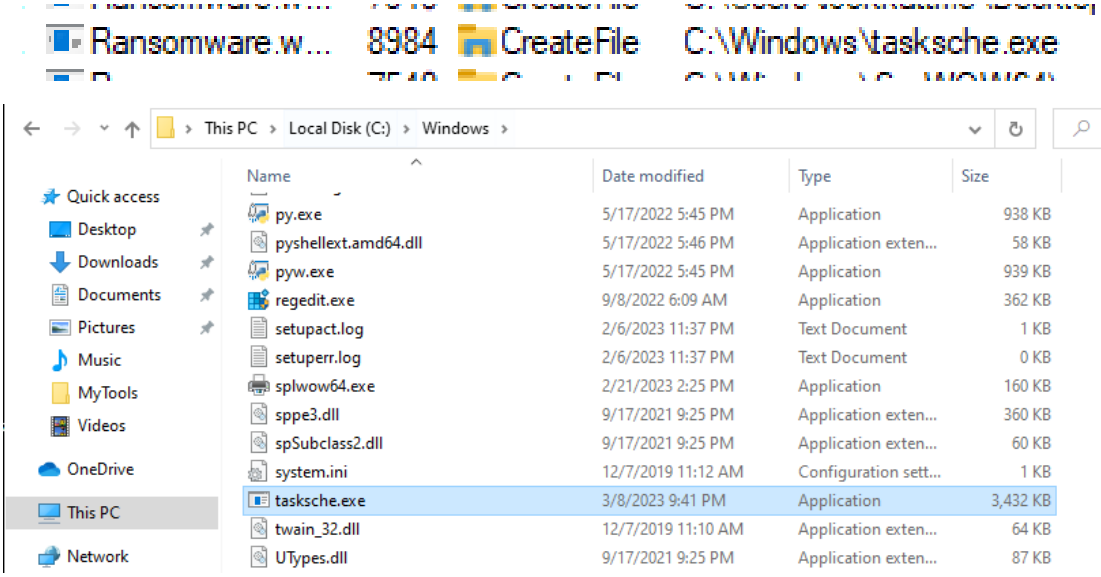
Firstly, it will run for few seconds and encrypt all the files with ".WNCRY" file extension, for example before (left) and after (right) the encryption:



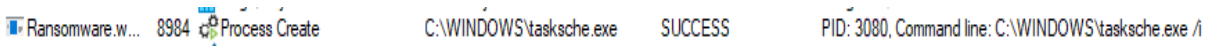
Then, after few more seconds It will switch the background and open a window:

Technical actions performed

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



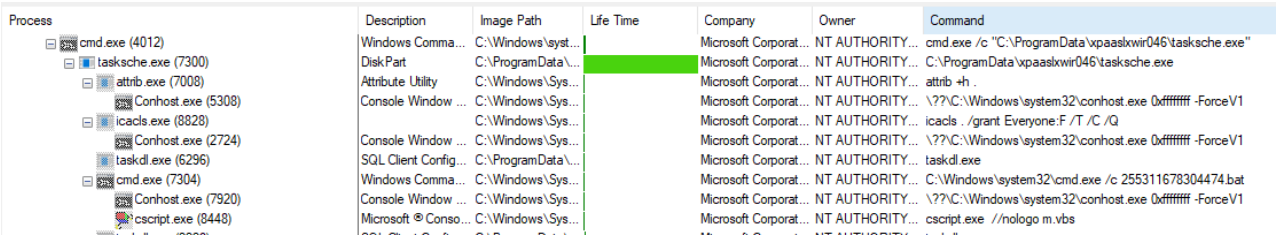
Which then runs as a separate process:



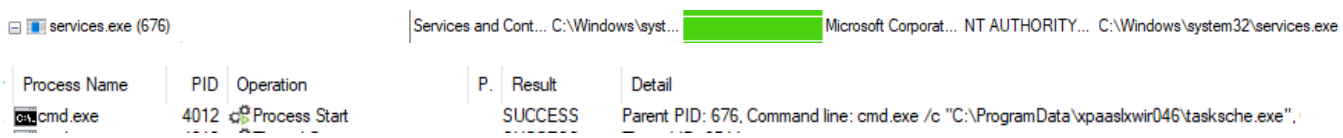
Then the ***tasksche.exe*** (process ID *3080)* creates a new directory:

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

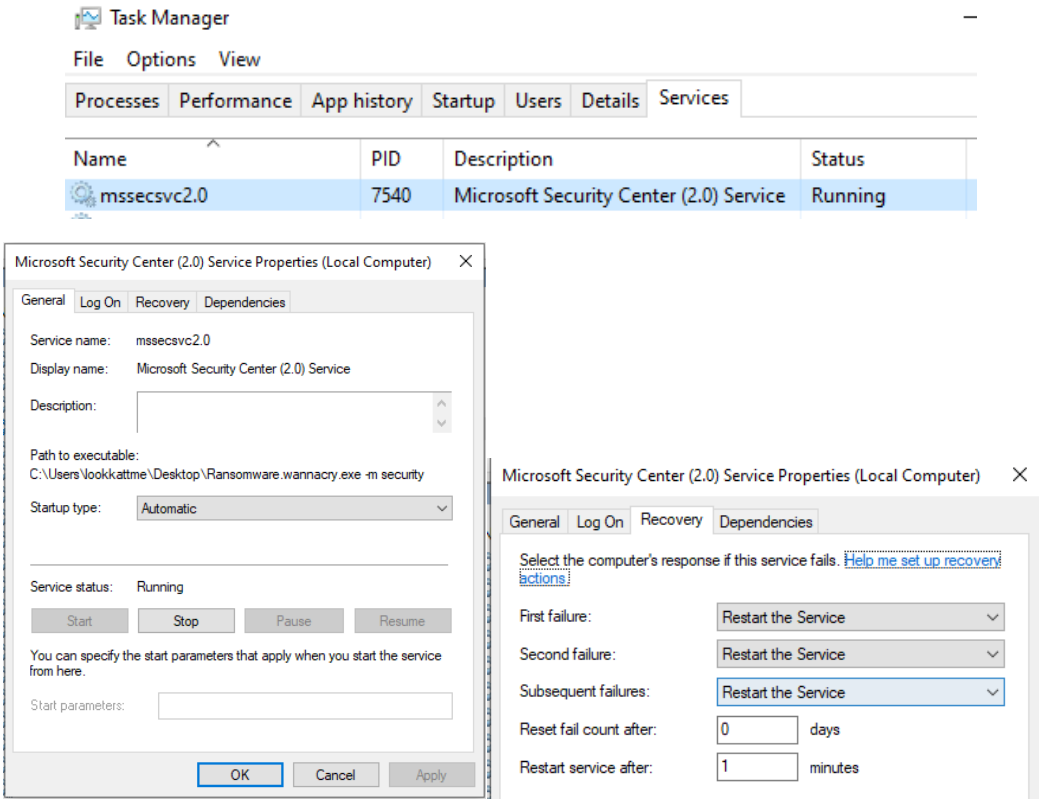
It executes ***attrib +h*** to hide the file and uses ***icacls*** to add all users full access (***/grant Everyone: F***) for all files in the directory and its subdirectories:



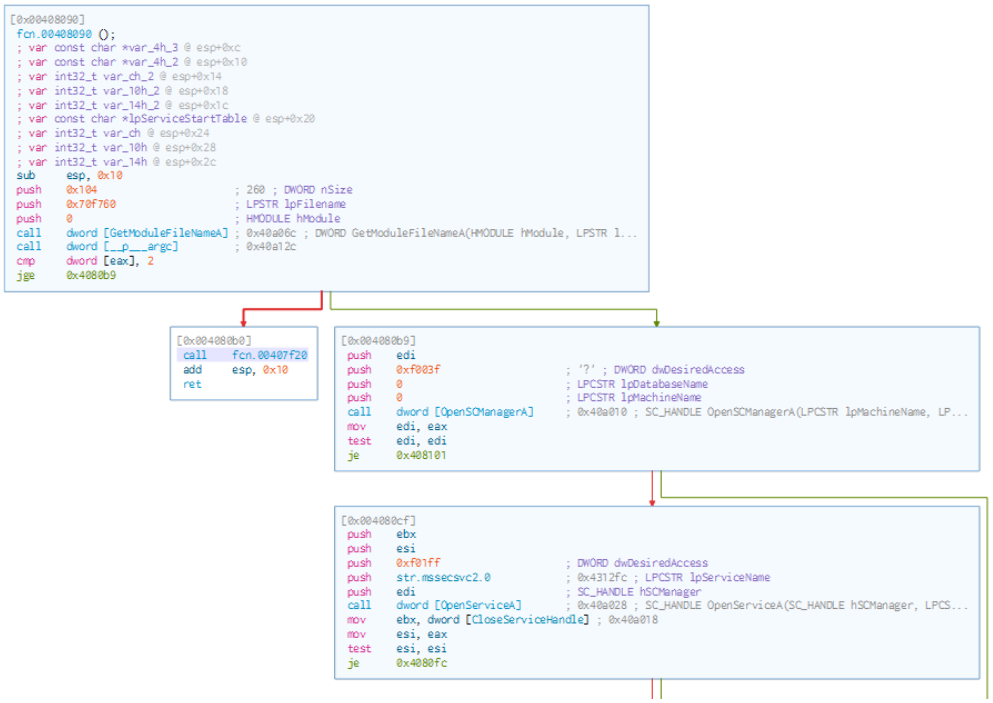
The ***cmd.exe*** command executed by ***services.exe:***



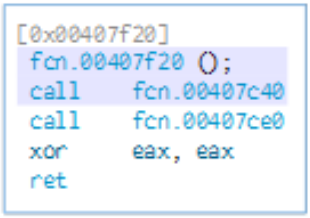
2) Under ***Services*** at the ***Task Manager***, we can notice a new service called ***mssecsvc2.0*** :



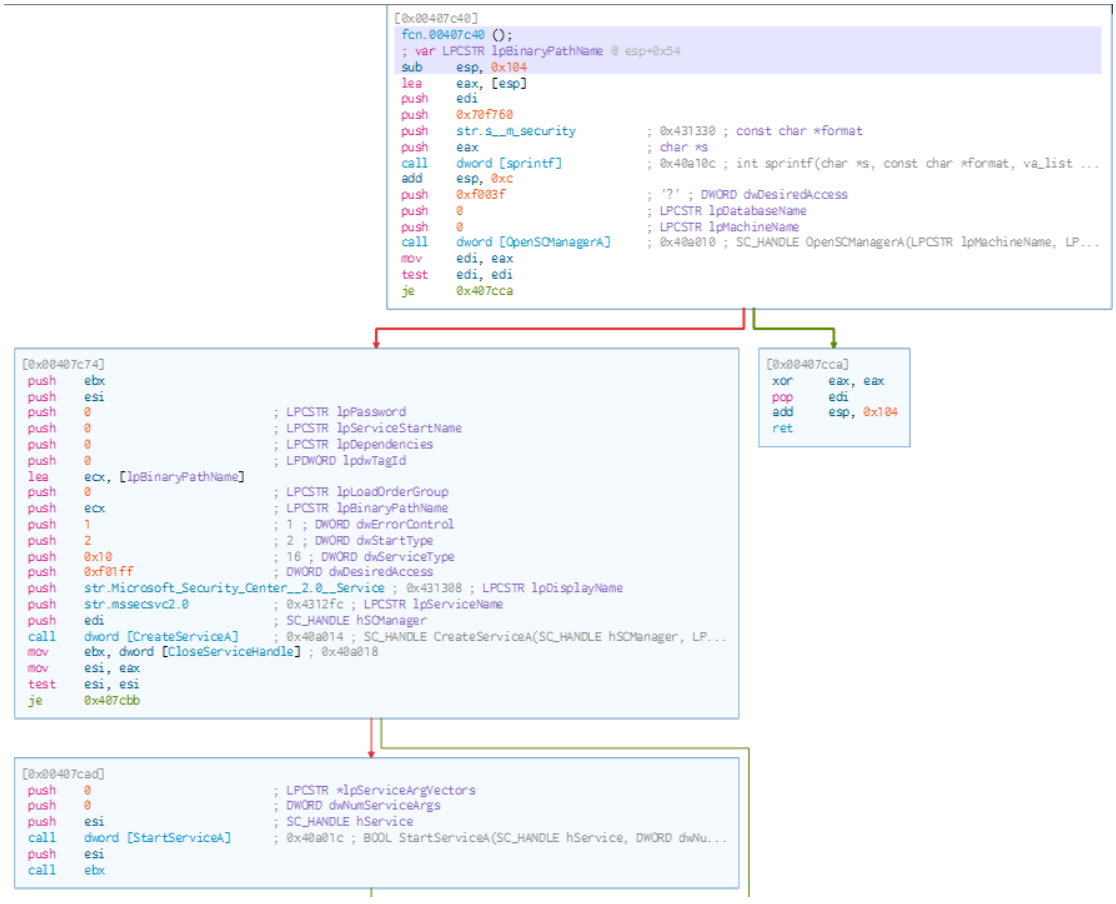
The service is created as the malware starts, checks the number of arguments – if there is only one argument (which means it executed for first time) performs the ***fcn.*0040f20** function – the left branch**.** Otherwise, it has more than one argument, means the service already exists (the service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



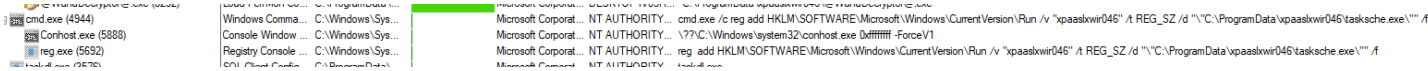
First time execution will get the left branch (since no other arguments → argc = 1):



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 ***Registery***:



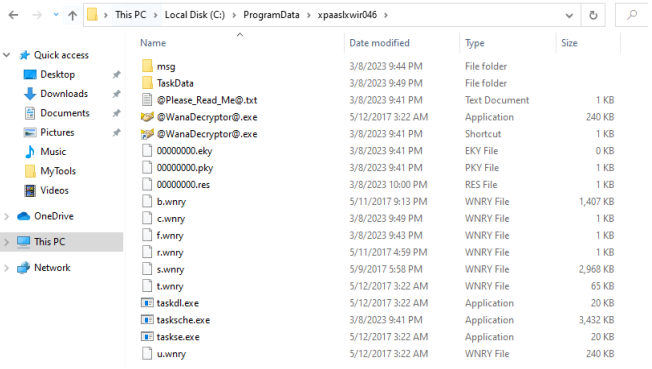
In conclusion, the service keeps the persistence of the malware by recovering it - if the machine is restarted or any failure caused while the process is running.

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\xpaaslxwir046\tasksche.exe", (

Which is creating files inside ***C:\ProgramData\xpaaslxwir046*** and executes them:

Process Name	PID	Operation	Path	Result
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\b.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\c.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\msg\m_bulgarian.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\msg\m_chinese (simplified).wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\msg\m_chinese (traditional).wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\msg\m_croatian.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\msg\m_czech.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\msg\m_danish.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\msg\m_dutch.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\msg\m_english.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\msg\m_filipino.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\msg\m_finnish.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\msg\m_french.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\msg\m_german.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\msg\m_greek.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\msg\m_indonesian.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\msg\m_italian.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\msg\m_japanese.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\msg\m_korean.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\msg\m_latvian.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\msg\m_norwegian.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\msg\m_polish.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\msg\m_portuguese.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\msg\m_romanian.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\msg\m_russian.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\msg\m_slovak.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\msg\m_spanish.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\msg\m_swedish.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\msg\m_turkish.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\msg\m_vietnamese.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\r.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\s.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\t.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\taskdl.exe	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\taskse.exe	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\u.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\c.wnry	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\00000000.pky	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\00000000.eky	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\00000000.res	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\00000000.res	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\255311678304474.bat	SUCCESS
tasksche.exe	7300	CreateFile	C:\ProgramData\xpaaslxwir046\@Please_Read_Me@.txt	SUCCESS



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

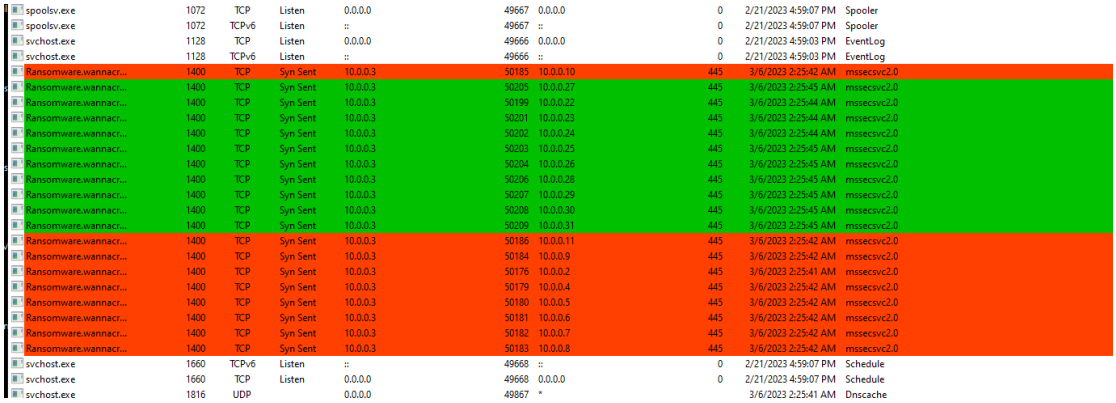
5) The ***@wanaDecrypter@.exe*** executes command to prevent the recovery of the infected system:

The full command:

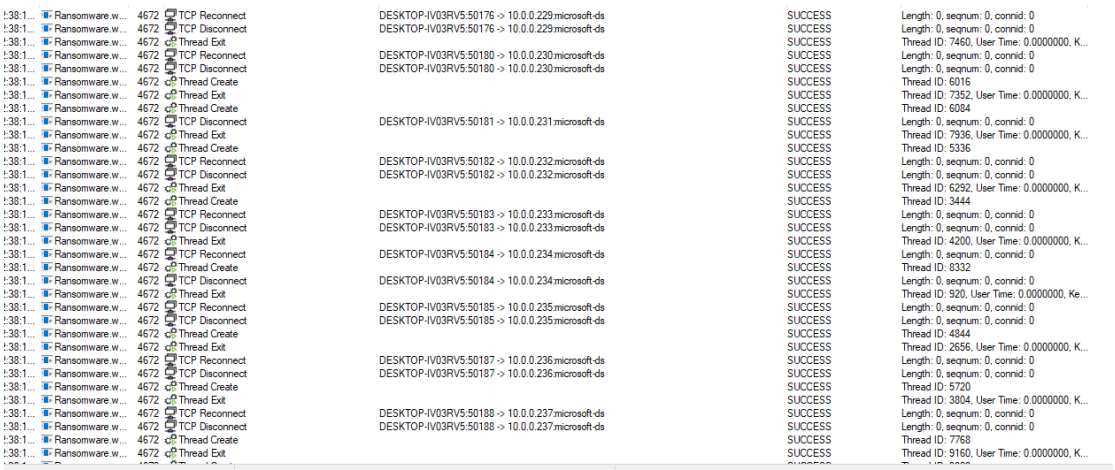
```
cmd.exe /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete
& bcdedit /set {default} bootstatuspolicy ignoreallfailures
& bcdedit /set {default} recoveryenabled no & wbadmin delete catalog -quiet
```

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:



ProcMon:



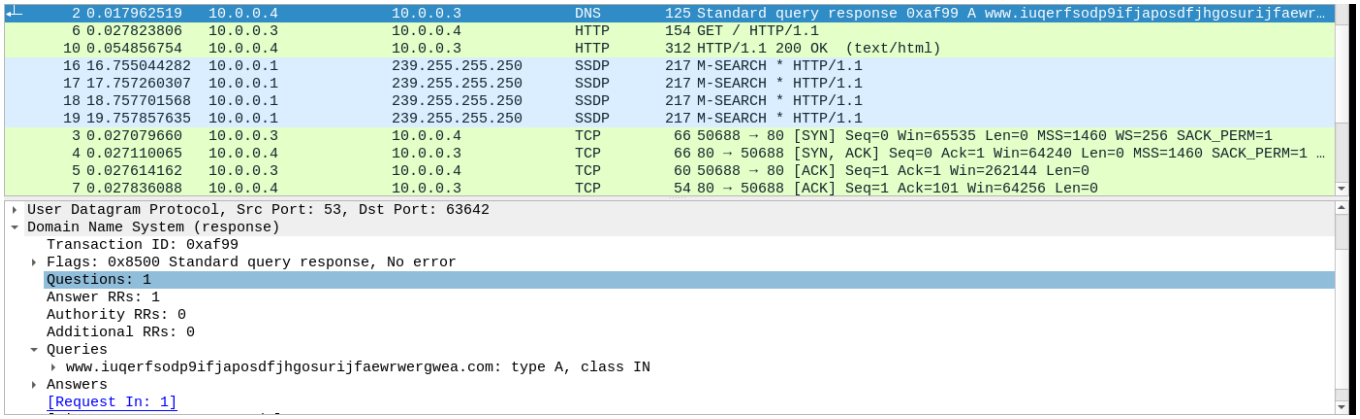
***Wannacry.exe* kill switch**

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

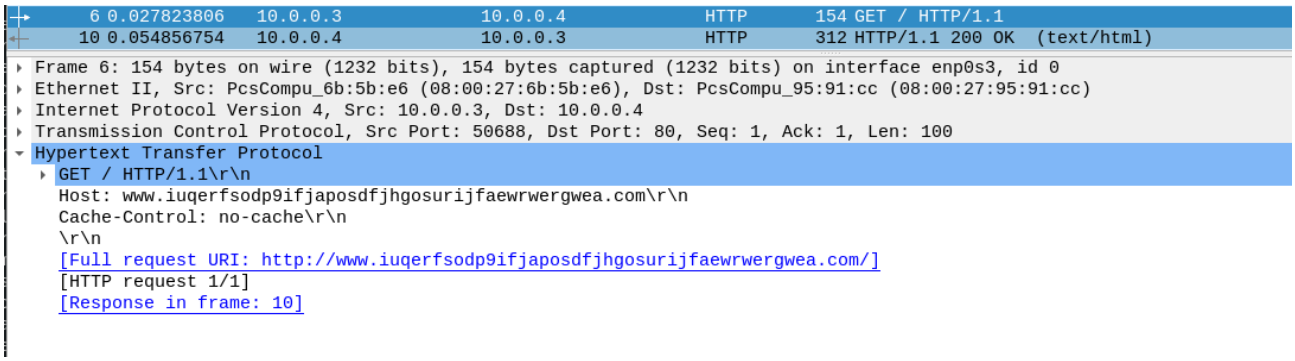
Wannacry.exe sends a ***HTTP*** request to domain name – ***[http]://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com/***

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

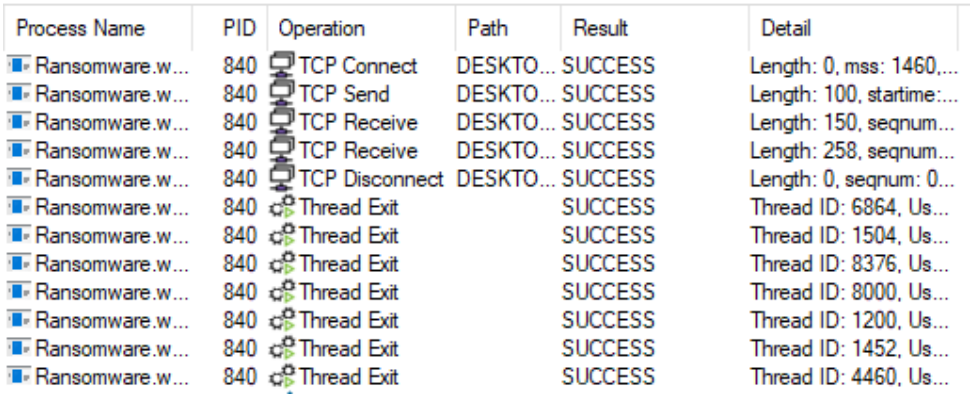
1) The ***DNS*** query for the domain name:



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



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

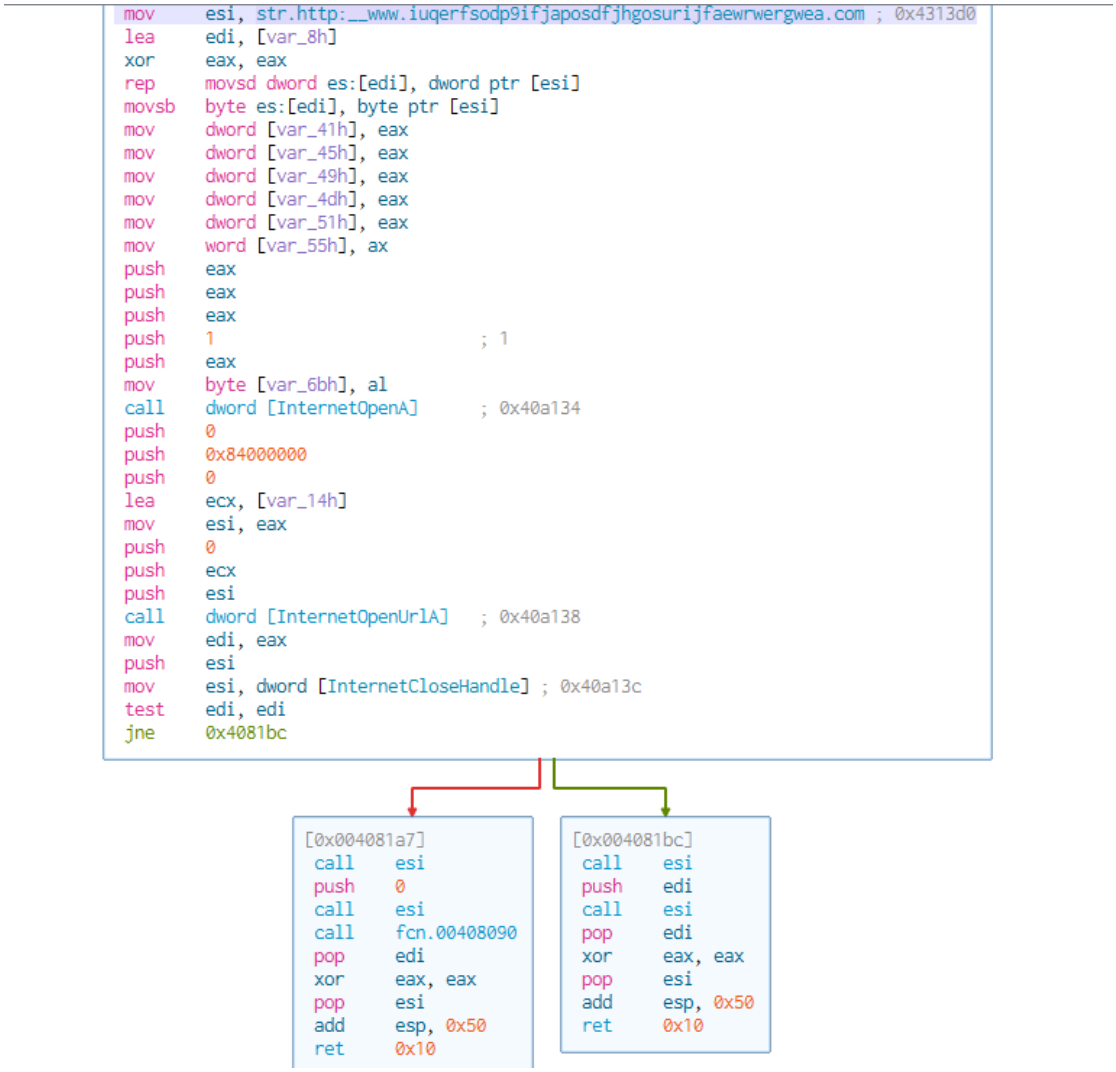


Process Name	PID	Operation	Path	Result	Detail
Ransomware.w…	840	TCP Connect	DESKTO…	SUCCESS	Length: 0, mss: 1460,…
Ransomware.w…	840	TCP Send	DESKTO…	SUCCESS	Length: 100, startime:…
Ransomware.w…	840	TCP Receive	DESKTO…	SUCCESS	Length: 150, seqnum…
Ransomware.w…	840	TCP Receive	DESKTO…	SUCCESS	Length: 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"***.



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-cryto-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_icacls = "icacls . /grand Everyone:F /T /C /Q" ascii
        $add_attrib_h = "attib +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_icacls, $add_attrib_h, $encryption_capabilities,
        $tasksche_exe, $taskhsvc_exe, $taskdl_exe, $taskse_exe, $mssecsvc_2_0, $wana_decrypt, $wnry_ext)
}
```