WannaCry Ransomware Analysis Report

March 2024 | Doron Pesahov | v1.0

Table of Contents

Executive Summary 3

High-Level Technical Summary 4

Execution Diagram 5

Malware Composition 6

Static Analysis 8

Extracted strings 8

List of file extensions that can be encrypted 11

Binary imports & Suspicious Windows API imports 12

Image Secion Header sizes 14

Gathering more information regarding the binary using Capa 14

Debugging the binary into Assembly language level 17

Dynamic Analysis 20

Detonating with internet connection 20

Detonationg without internet connection 21

Host-Based indicators 22

Network-Based indicators 24

Malicious processes used by WannaCry 26

List of Indicators of Compromise (IOCs) 29

Yara Rules 30

Executive Summary

SHA256 Hash	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c

In the early summer of 2017, WannaCry was unleashed on the world. Widely considered to be one of the most devastating malware infections to date, WannaCry left a trail of destruction in its wake. It’s a ransomware CryptoWorm, which means it has the ability to not only encrypt individual hosts but also spread itself through networks all on its own, amplifying its destructive reach with every infected node it encountered.

WannaCry creators leveraged the EternalBlue Exploit which is a family of critical vulnerabilities in Microsoft SMBv1 server (CVE-2017-0143 to CVE-2017-0148) that helped them spreading this ransomware through networks. This technique allegedly developed by the NSA and was leaked by the “Shadow Brokers” in April 2017 along with other hacking tools that were developed by the NSA.

YARA signature rule is attached below.

High-Level Technical Summary

WannaCry is a 32-bit portable executable (PE) file, requiring administrative privileges for execution of its malicious payload. Upon execution, it attempts to establish a connection with a designated callback URL: "hxxp://www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com".
If a response is received from this URL, the malware refrains from executing its malicious payload, effectively acting as a kill-switch.
However, if there isn’t a connection to the specified URL, the malware proceeds with its destructive activities, which include:

- Encryption of files in the operating system with the ".WNCRY" file extension.
- Modification of the desktop background to display a black image containing information for the victim and instructions on how to recover their computer.
- Display of a window with a timer, demanding a Bitcoin payment to the attacker's Bitcoin wallet (WanaDecrypt0r 2.0).
- Unpacking additional second-stage executable files by the WannaCry PE, placing them in a dedicated directory (C:\ProgramData\gzfhbohbqt094), and establishing persistence.
- Attempting to propagate through the network via SMB shares (port 445) to infect additional hosts, expand its encryption capabilities, and maximize profitability.

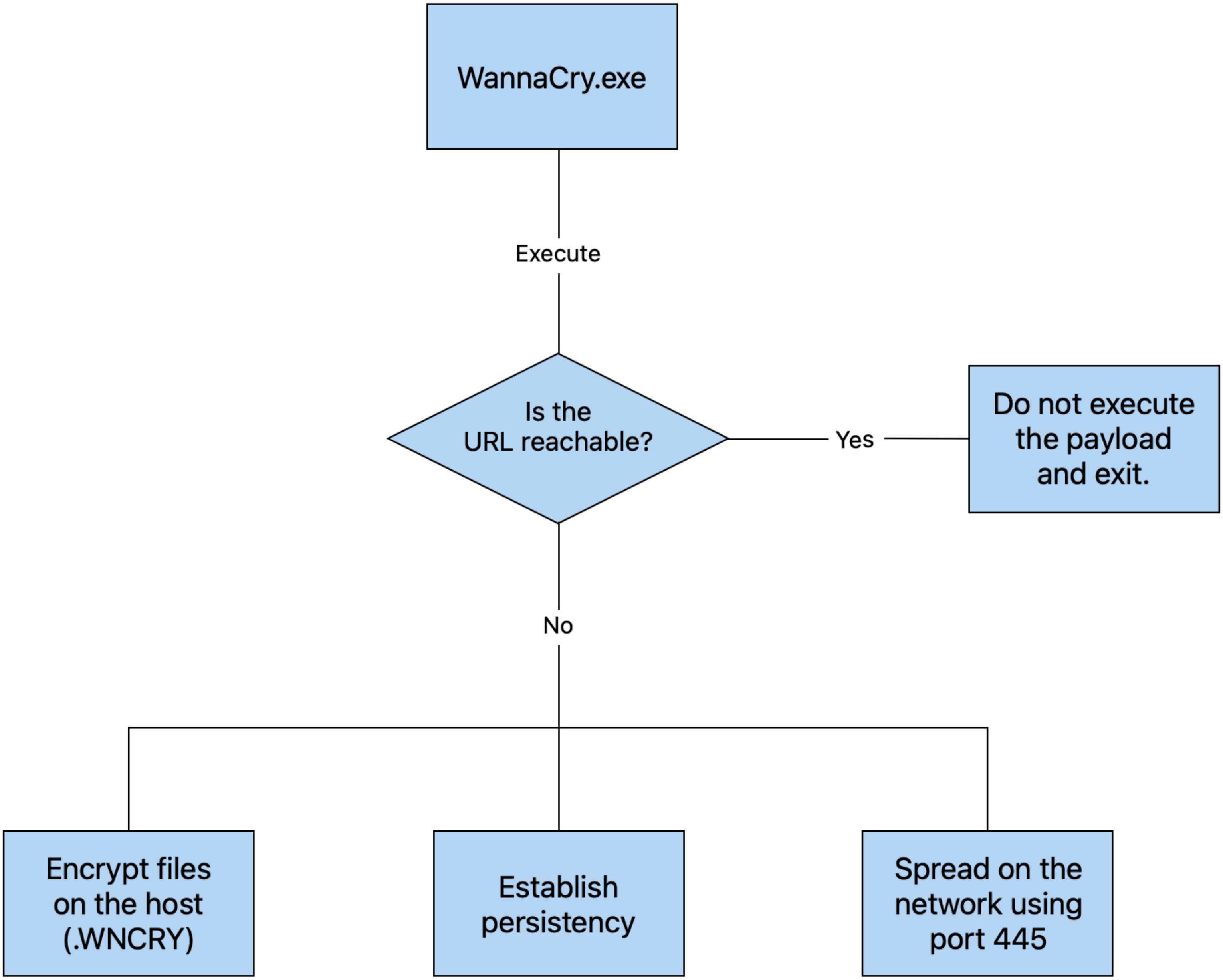

WannaCry.exe
Execute
Is the URL reachable?
Yes
Do not execute the payload and exit.
No
Encrypt files on the host (.WNCRY)
Establish persistency
Spread on the network using port 445

Figure 1 – Execution Diagram

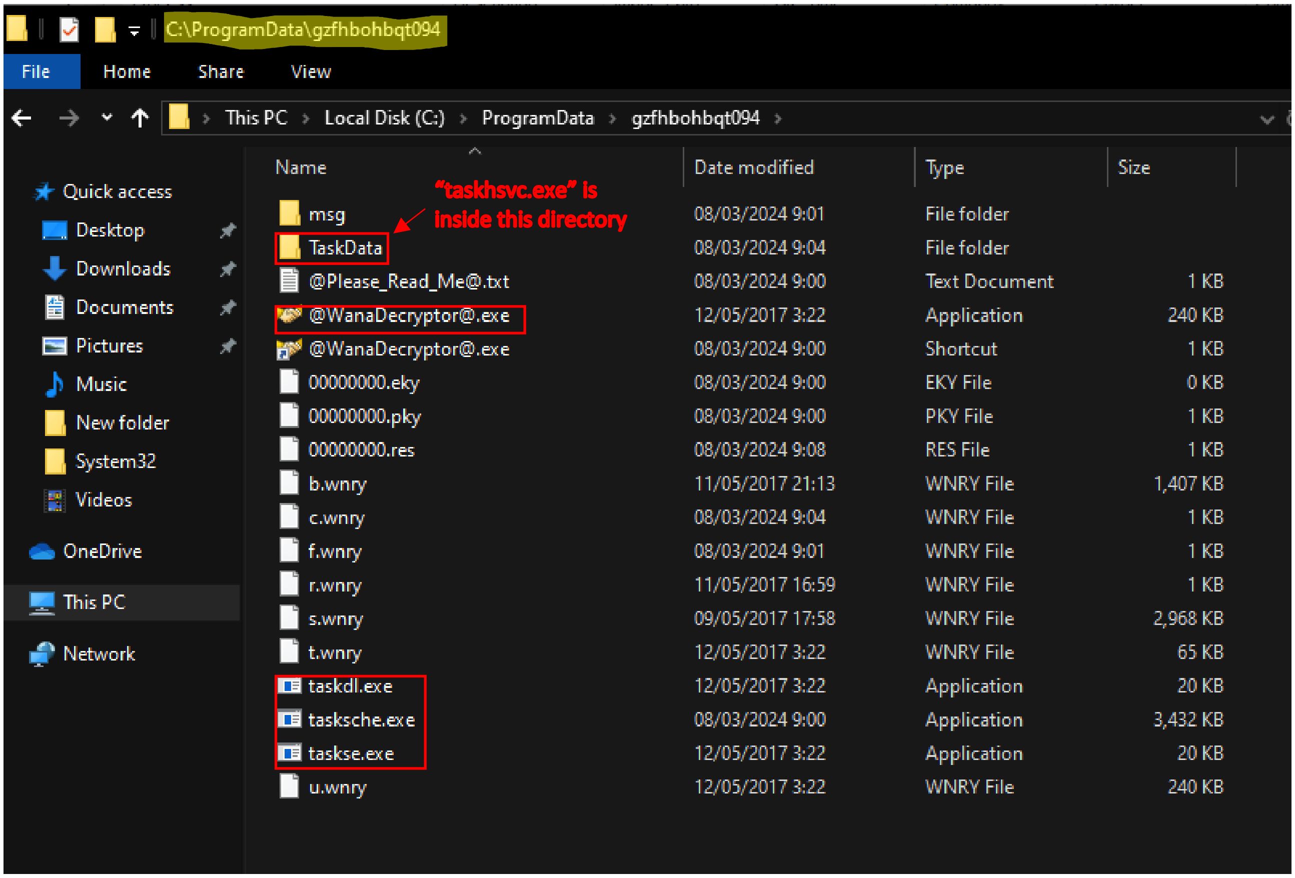
Malware Composition

Additional details on the sample:

SHA256 Hash	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
MD5 Hash	db349b97c37d22f5ea1d1841e3c89eb4
Architecture	32-bit
Programing Language	C++
Original File Name	lhdfrgui.exe

WannaCry.exe creates hidden directory in **C:\ProgramData\gzfhbohbqt094** which contains additional executables that were dropped after the initial detonation of the malware. This directory serves as the staging area for the WannaCry Ransomware.

File Name	SHA256 Hash
taskdl.exe	4a468603fdcb7a2eb5770705898cf9ef37aade532a7964642ecd705a74794b79
tasksche.exe	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
taskse.exe	2ca2d550e603d74dedda03156023135b38da3630cb014e3d00b1263358c5f00d
taskhsvc.exe	E48673680746FBE027E8982F62A83C298D6FB46AD9243DE8E79B7E5A24DCD4EB
@WanaDecryptor@.exe	B9C5D4339809E0AD9A00D4D3DD26FDF44A32819A54ABF846BB9B560D81391C25



C:\ProgramData\gzfhbohbqt094

"taskhsvc.exe" is inside this directory

Name	Date modified	Type	Size
msg	08/03/2024 9:01	File folder	
TaskData	08/03/2024 9:04	File folder	
@Please_Read_Me@.txt	08/03/2024 9:00	Text Document	1 KB
@WanaDecryptor@.exe	12/05/2017 3:22	Application	240 KB
@WanaDecryptor@.exe	08/03/2024 9:00	Shortcut	1 KB
00000000.eky	08/03/2024 9:00	EKY File	0 KB
00000000.pky	08/03/2024 9:00	PKY File	1 KB
00000000.res	08/03/2024 9:08	RES File	1 KB
b.wnry	11/05/2017 21:13	WNRY File	1,407 KB
c.wnry	08/03/2024 9:04	WNRY File	1 KB
f.wnry	08/03/2024 9:01	WNRY File	1 KB
r.wnry	11/05/2017 16:59	WNRY File	1 KB
s.wnry	09/05/2017 17:58	WNRY File	2,968 KB
t.wnry	12/05/2017 3:22	WNRY File	65 KB
taskdl.exe	12/05/2017 3:22	Application	20 KB
tasksche.exe	08/03/2024 9:00	Application	3,432 KB
taskse.exe	12/05/2017 3:22	Application	20 KB
u.wnry	12/05/2017 3:22	WNRY File	240 KB

Figure 2 – Staging Area

taksche.exe

This executable will be initiated in the second stage right after initiaing WannaCry ransomware and is resposible for initiating additional scripts and processes that will grant permissions, set the current directory to hidden, and ensuring persistence within the system (detailed below in figure 23).

taskdl.exe

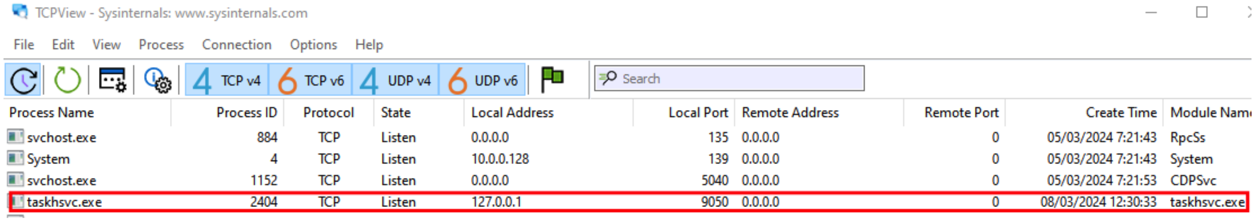
Support tool for removing temporary files.

taskse.exe

Support tool for launch Decryption Tool.

taskhsvc.exe

opens port 9050 to a LISTENING state and attempts to connect to non-private remote addresses over HTTPS, attempts to contact the configured C2 hidden services.



Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Nam
svchost.exe	884	TCP	Listen	0.0.0.0	135	0.0.0.0	0	05/03/2024 7:21:43	RpcSs
System	4	TCP	Listen	10.0.0.128	139	0.0.0.0	0	05/03/2024 7:21:43	System
svchost.exe	1152	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	05/03/2024 7:21:53	CDPSvc
taskhsvc.exe	2404	TCP	Listen	127.0.0.1	9050	0.0.0.0	0	08/03/2024 12:30:33	taskhsvc.exe

Figure 3 – taskhsvc.exe open listening port

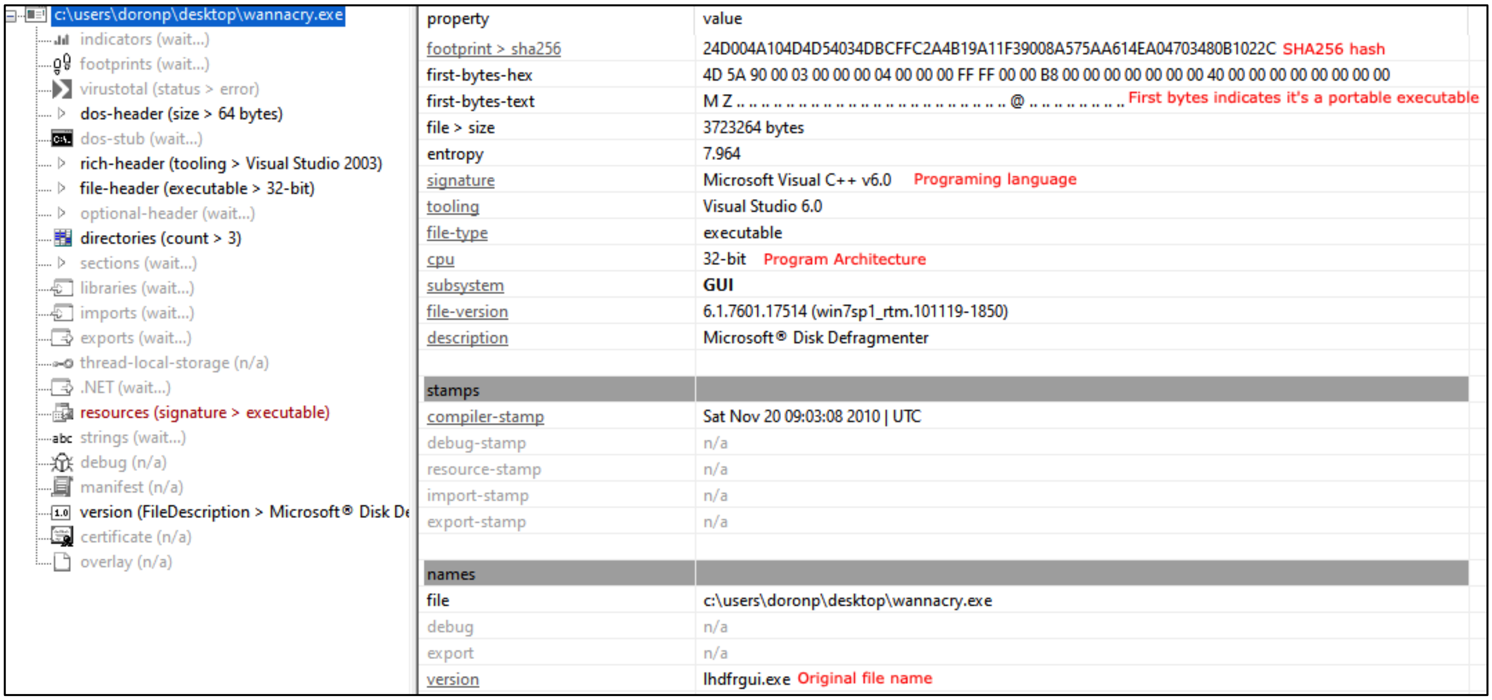
taskhsvc.exe

opens port 9050 to a LISTENING state and attempts to connect to non-private remote addresses over HTTPS, attempts to contact the configured C2 hidden services.

@WannaDecryptor@.exe:

This executable features a graphical user interface (GUI) and appears in the center of the screen upon successful completion of the encryption process. Its primary function is to facilitate the decryption of the victim's files subsequent to their Bitcoin payment.

Static Analysis

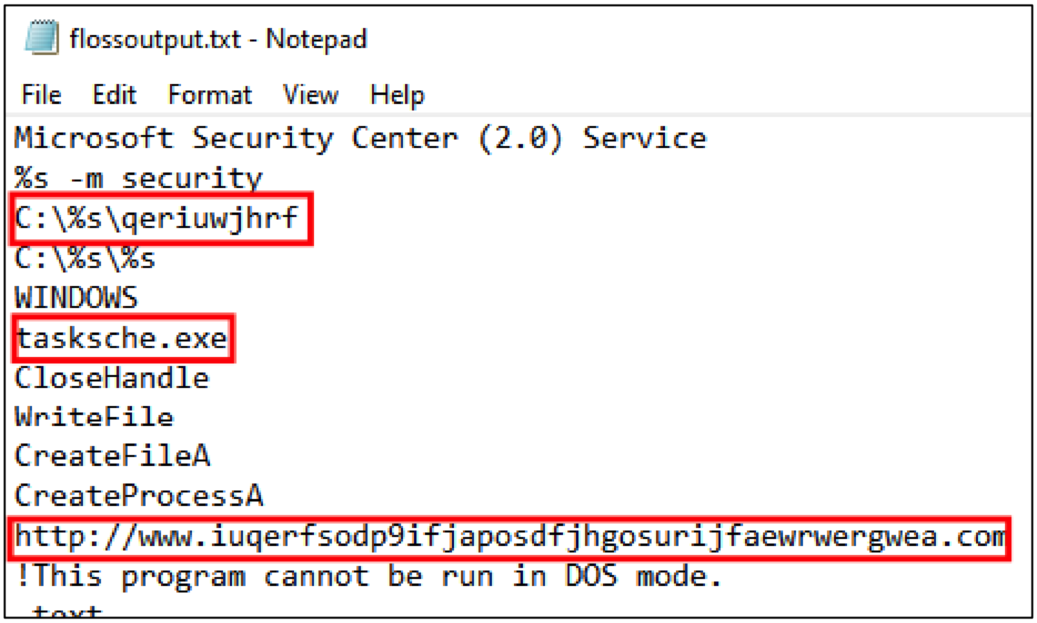


```
c:\users\doronp\desktop\wannacry.exe
  indicators (wait...)
  footprints (wait...)
  virustotal (status > error)
  dos-header (size > 64 bytes)
  dos-stub (wait...)
  rich-header (tooling > Visual Studio 2003)
  file-header (executable > 32-bit)
  optional-header (wait...)
  directories (count > 3)
  sections (wait...)
  libraries (wait...)
  imports (wait...)
  exports (wait...)
  thread-local-storage (n/a)
  .NET (wait...)
  resources (signature > executable)
  strings (wait...)
  debug (n/a)
  manifest (n/a)
  version (FileDescription > Microsoft® Disk De
  certificate (n/a)
  overlay (n/a)
```

property	value
footprint > sha256	24D004A104D4D54034DBCFFC2A4B19A11F39008A575AA614EA04703480B1022C SHA256 hash
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00
first-bytes-text	M Z .. .. @ .. .. First bytes indicates it's a portable executable
file > size	3723264 bytes
entropy	7.964
signature	Microsoft Visual C++ v6.0 Programing language
tooling	Visual Studio 6.0
file-type	executable
cpu	32-bit Program Architecture
subsystem	**GUI**
file-version	6.1.7601.17514 (win7sp1_rtm.101119-1850)
description	Microsoft® Disk Defragmenter
stamps	
compiler-stamp	Sat Nov 20 09:03:08 2010 | UTC
debug-stamp	n/a
resource-stamp	n/a
import-stamp	n/a
export-stamp	n/a
names	
file	c:\users\doronp\desktop\wannacry.exe
debug	n/a
export	n/a
version	lhdfrgui.exe Original file name

Figure 4 – PEStudio basic information

List of some of the interesting strings that were extraced from the PE:

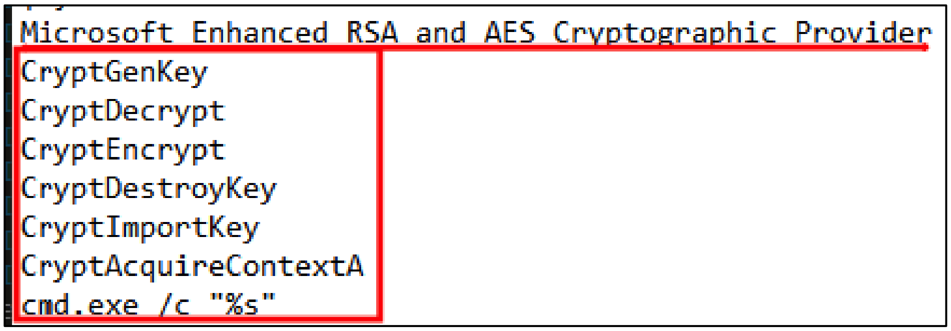


```
Microsoft Security Center (2.0) Service
%s -m security
C:\%s\qeriuwjhrf
C:\%s\%s
WINDOWS
tasksche.exe
CloseHandle
WriteFile
CreateFileA
CreateProcessA
http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
!This program cannot be run in DOS mode.
.text
```

Figure 5 – Floss Output (1)

When examining the strings inside the PE, we can identify right away file path in the C:\ partition with "%s" in it, the "tasksche.exe" that was described earlier, which is an executable that will be dropped to the OS once detonating the malware, and long URL string that the malware will probably communicate with at some point.

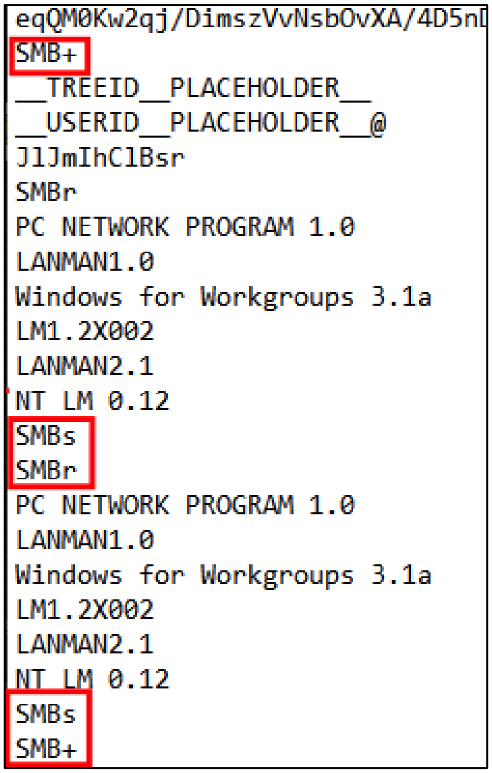
- the "%s" in the file path is a placeholder typically used in programming/scripting languages to represent a variable or placeholder that will be replaced with a specific value at runtime.



```
Microsoft Enhanced RSA and AES Cryptographic Provider
CryptGenKey
CryptDecrypt
CryptEncrypt
CryptDestroyKey
CryptImportKey
CryptAcquireContextA
cmd.exe /c "%s"
```

Figure 6 – Floss Output (2)

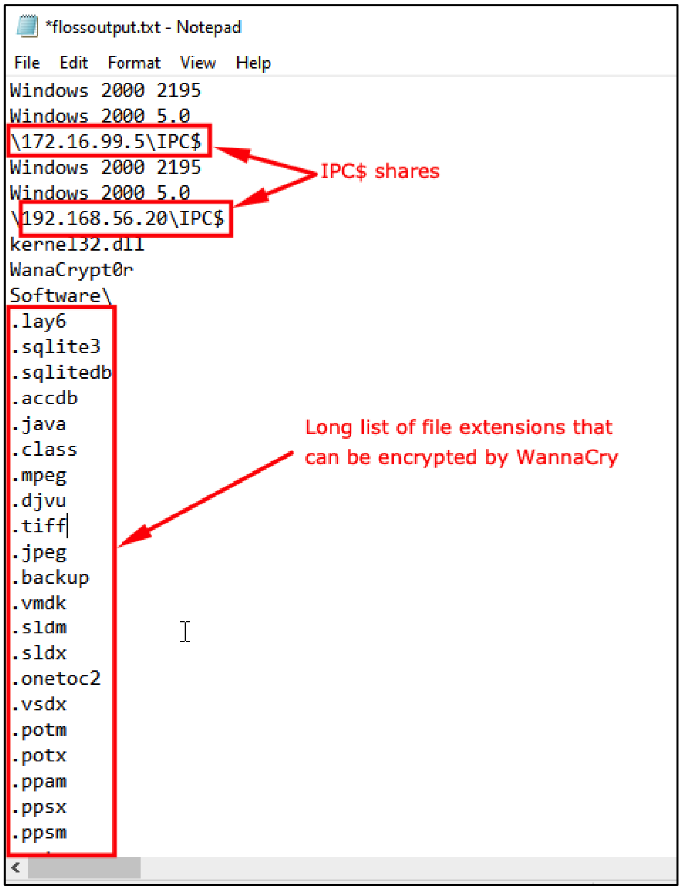
It looks like this malware is using cryptographic functions from the header wincrypt.h, probably to encrypt files. Additionaly there is a cmd command, again with "%s".



```
eqQM0Kw2qj/DimszVvNsbOvXA/4D5n
SMB+
__TREEID__PLACEHOLDER__
__USERID__PLACEHOLDER__@
J1JmIhClBsr
SMBr
PC NETWORK PROGRAM 1.0
LANMAN1.0
Windows for Workgroups 3.1a
LM1.2X002
LANMAN2.1
NT LM 0.12
SMBs
SMBr
PC NETWORK PROGRAM 1.0
LANMAN1.0
Windows for Workgroups 3.1a
LM1.2X002
LANMAN2.1
NT LM 0.12
SMBs
SMB+
```

strings that are related to the usage of the SMB (*Server Message Block* | *445*) protocol which allows sharing resources (files and directories) through the local network between Windows machines.

Figure 5 – Floss Output (3)



```
Windows 2000 2195
Windows 2000 5.0
\172.16.99.5\IPC$
Windows 2000 2195
Windows 2000 5.0
\192.168.56.20\IPC$
kernel32.dll
WanaCrypt0r
Software\
.lay6
.sqlite3
.sqlitedb
.accdb
.java
.class
.mpeg
.djvu
.tiff
.jpeg
.backup
.vmdk
.sldm
.sldx
.onetoc2
.vsdx
.potm
.potx
.ppam
.ppsx
.ppsm
```

IPC$ shares

Long list of file extensions that can be encrypted by WannaCry

Figure 7 – Floss Output (4)

In this screenshot we can see two internal IP addresses with “IPC$” at the end.
IPC$ share is also known as a null session connection. By using this session, Windows lets anonymous users perform certain activities, such as enumerating the names of domain accounts and network shares.
Additionally, we can see a long list of file extensions that can be encrypted by WannaCry ransomware.

Full list of the file extensions that the WannaCry Ransomware is capable of encrypting:

.docx
.docb
.docm
.dot
.dotm
.dotx
.xls
.xlsm
.xlsb
.xlw
.xlt
.xlm
.xlc
.xltx
.xltm
.ppt
.pptx
.pptm
.pot
.pps
.ppsm
.ppsx

.ppam
.potx
.potm
.pst
.ost
.msg
.eml
.vsd
.vsdx
.txt
.csv
.rtf
.123
.wks
.wk1
.pdf
.dwg
.onetoc2
.snt
.hwp
.602
.sxi

.sti
.sldx
.sldm
.sldm
.vdi
.vmdk
.vmx
.aes
.ARC
.PAQ
.bz2
.tbk
.bak
.tar
.tgz
.gz
.7z
.rar
.zip
.backup
.iso

.vcd
.jpeg
.jpg
.bmp
.png
.gif
.raw
.tif
.tiff
.nef
.psd
.ai
.svg
.djvu
.m4u
.m3u
.mid
.wma
.flv
.3g2
.mkv

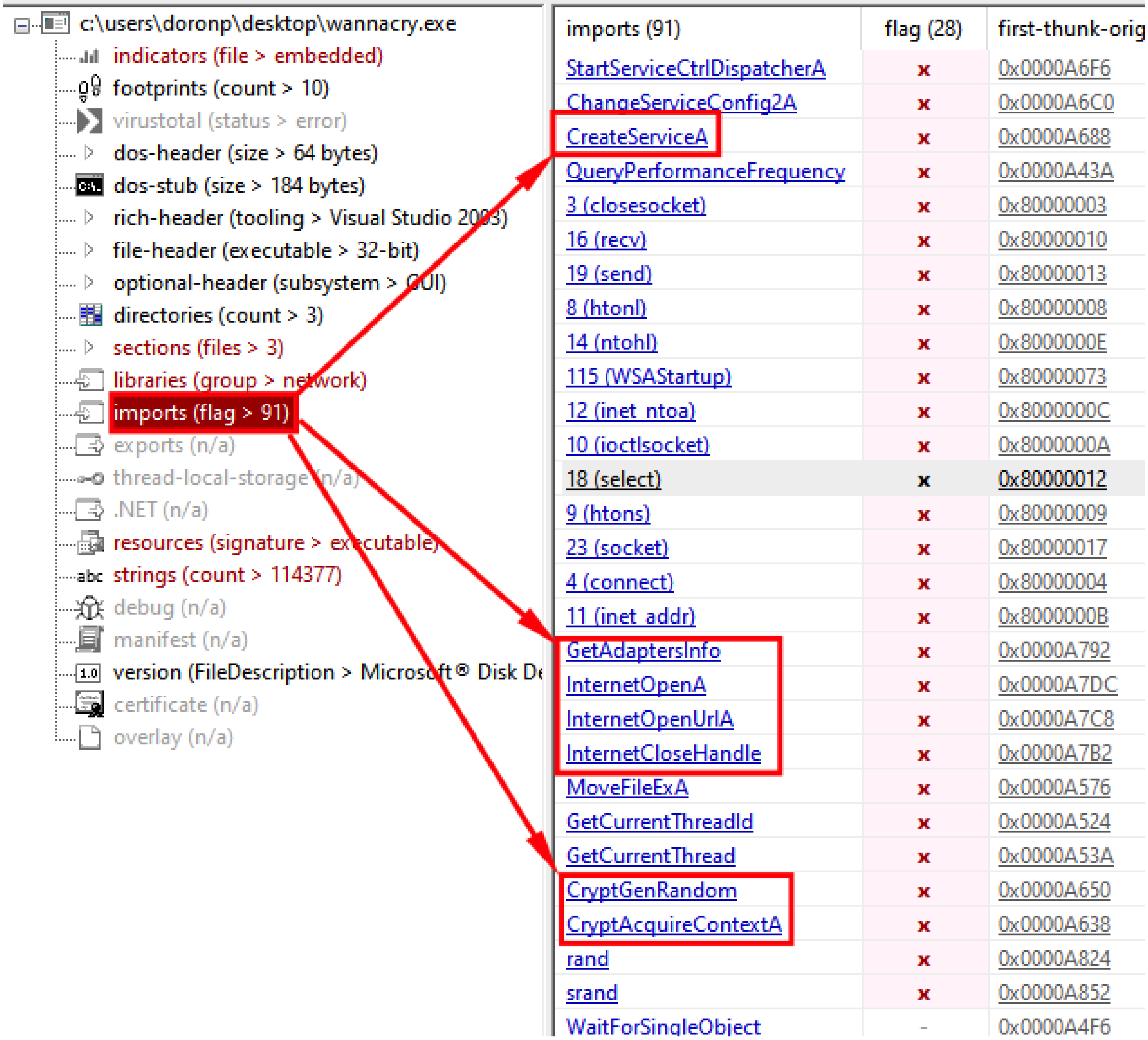
.3gp
.mp4
.mov
.avi
.asf
.mpeg
.vob
.wmv
.fla
.swf
.wav
.mp3
.sh
.class
.jar
.java
.rb
.asp
.php
.jsp
.brd

.sch
.dch
.dip
.pl
.vb
.vbs
.ps1
.cmd
.js
.asm
.h
.pas
.cpp
.c
.cs
.suo
.sln
.ldf
.mdf
.ibd
.myi

.myd
.frm
.odb
.dbf
.db
.mdb
.accdb
.sqlitedb
.sqlite3
.asc
.lay6
.lay
.mml
.sxm
.otg
.odg
.uop
.std
.sxd
.otp
.odp

.wb2
.slk
.dif
.stc
.sxc
.ots
.ods
.max
.3ds
.uot
.stw
.sxw
.ott
.odt
.pem
.p12
.csr
.crt
.key
.pfx
.der

Inspecting the Import Address Table (IAT) of the WannaCry binary:



c:\users\doronp\desktop\wannacry.exe
- indicators (file > embedded)
- footprints (count > 10)
- virustotal (status > error)
- dos-header (size > 64 bytes)
- dos-stub (size > 184 bytes)
- rich-header (tooling > Visual Studio 2008)
- file-header (executable > 32-bit)
- optional-header (subsystem > GUI)
- directories (count > 3)
- sections (files > 3)
- libraries (group > network)
- imports (flag > 91)
- exports (n/a)
- thread-local-storage (n/a)
- .NET (n/a)
- resources (signature > executable)
- strings (count > 114377)
- debug (n/a)
- manifest (n/a)
- version (FileDescription > Microsoft® Disk De
- certificate (n/a)
- overlay (n/a)

imports (91)	flag (28)	first-thunk-orig
StartServiceCtrlDispatcherA	x	0x0000A6F6
ChangeServiceConfig2A	x	0x0000A6C0
CreateServiceA	x	0x0000A688
QueryPerformanceFrequency	x	0x0000A43A
3 (closesocket)	x	0x80000003
16 (recv)	x	0x80000010
19 (send)	x	0x80000013
8 (htonl)	x	0x80000008
14 (ntohl)	x	0x8000000E
115 (WSAStartup)	x	0x80000073
12 (inet_ntoa)	x	0x8000000C
10 (ioctlsocket)	x	0x8000000A
18 (select)	x	0x80000012
9 (htons)	x	0x80000009
23 (socket)	x	0x80000017
4 (connect)	x	0x80000004
11 (inet_addr)	x	0x8000000B
GetAdaptersInfo	x	0x0000A792
InternetOpenA	x	0x0000A7DC
InternetOpenUrlA	x	0x0000A7C8
InternetCloseHandle	x	0x0000A7B2
MoveFileExA	x	0x0000A576
GetCurrentThreadId	x	0x0000A524
GetCurrentThread	x	0x0000A53A
CryptGenRandom	x	0x0000A650
CryptAcquireContextA	x	0x0000A638
rand	x	0x0000A824
srand	x	0x0000A852
WaitForSingleObject	-	0x0000A4F6

Figure 8 – Binary imports

There are 91 imports used by this binary whilst **28 of them flagged as suspicious**. We won't describe all of them but the most suspicious, which are also related to the strings we found earlier.

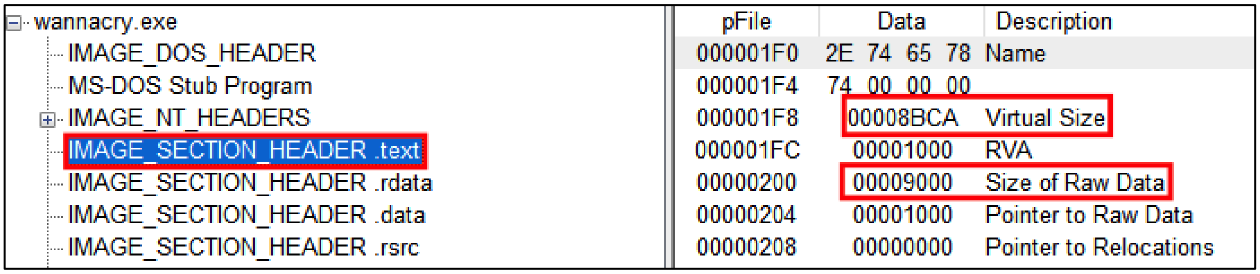
Windows API Import	Description	Library	Associated Attack
InternetOpenA	used to initialize the use of WinINet functions.	Wininet.dll	Malicious Internet Activity
InternetOpenUrlA	used to open a resource specified by a complete FTP or HTTP URL.	Wininet.dll	Malicious Internet Activity
InternetCloseHandle	used to close an internet handle.	Wininet.dll	Malicious Internet Activity
GetAdaptersInfo	used to obtain information about the network adapters on the system. This function is commonly used by malware for enumeration purposes.	Iphlpapi.dll	Enumeration
CryptAcquireContextA	used to acquire a handle to a particular key container within a particular cryptographic service provider (CSP).	Advapi32.dll	Ransomware
CryptGenRandom	used to fill a buffer with cryptographically random bytes.	Advapi32.dll	Ransomware
CreateServiceA	Used to create a service object and adds it to the specified service control manager database. This function is commonly used by malware for persistence.	Advapi32.dll	Helper
LocalAlloc	used for heap allocation and manipulation.	Kernel32.dll	Injection

- The first three internet functions (InternetOpenA, InternetOpenUrlA, InternetCloseHandle) can be used to download malicious files, exfiltration or to interact with a C2. In our case it’s related to the long URL string which will be used for communication and as a kill-switch.

- The GetAdaptersInfo function is commonly used by malware for enumeration tasks. Its usage is associated with certain strings previously identified, such as the IPC$ share.

- CryptGenRandom, CryptAcquireContextA are standard cryptographic functions commonly utilized by ransomware, primarily for encrypting various types of files.

- CreateServiceA is frequently utilized by malware for establishing persistence. Essentially, its purpose is to generate a service.



- wannacry.exe
  - IMAGE_DOS_HEADER
  - MS-DOS Stub Program
  - IMAGE_NT_HEADERS
  - IMAGE_SECTION_HEADER .text
  - IMAGE_SECTION_HEADER .rdata
  - IMAGE_SECTION_HEADER .data
  - IMAGE_SECTION_HEADER .rsrc

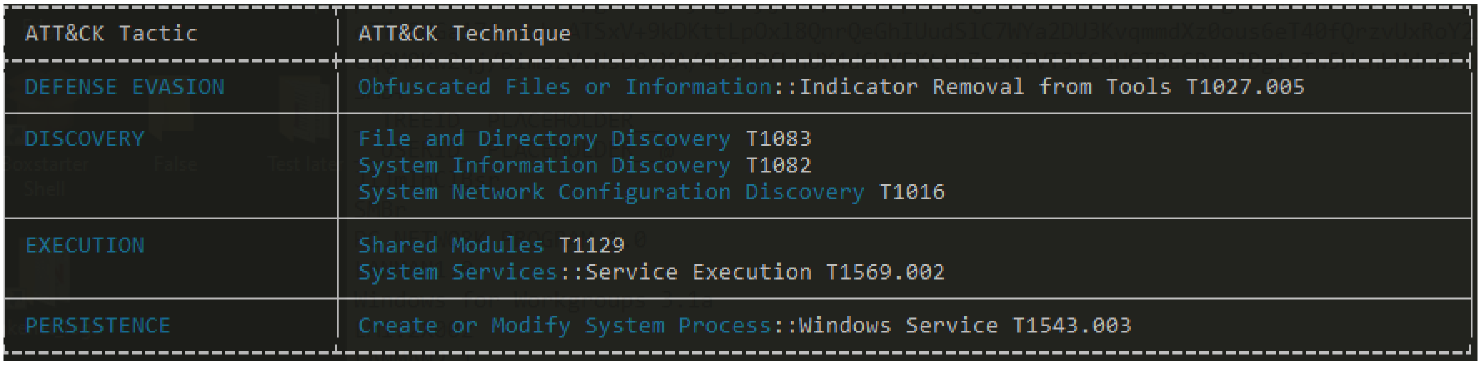
pFile	Data	Description
000001F0	2E 74 65 78	Name
000001F4	74 00 00 00	
000001F8	00008BCA	Virtual Size
000001FC	00001000	RVA
00000200	00009000	Size of Raw Data
00000204	00001000	Pointer to Raw Data
00000208	00000000	Pointer to Relocations

Figure 9 – PEView Header Size

	Size in Hexadecimal	Size in Decimal
Virtual Size	00008BCA	35,786
Size of Raw Data	00009000	36,864
Size Difference	436	1,078

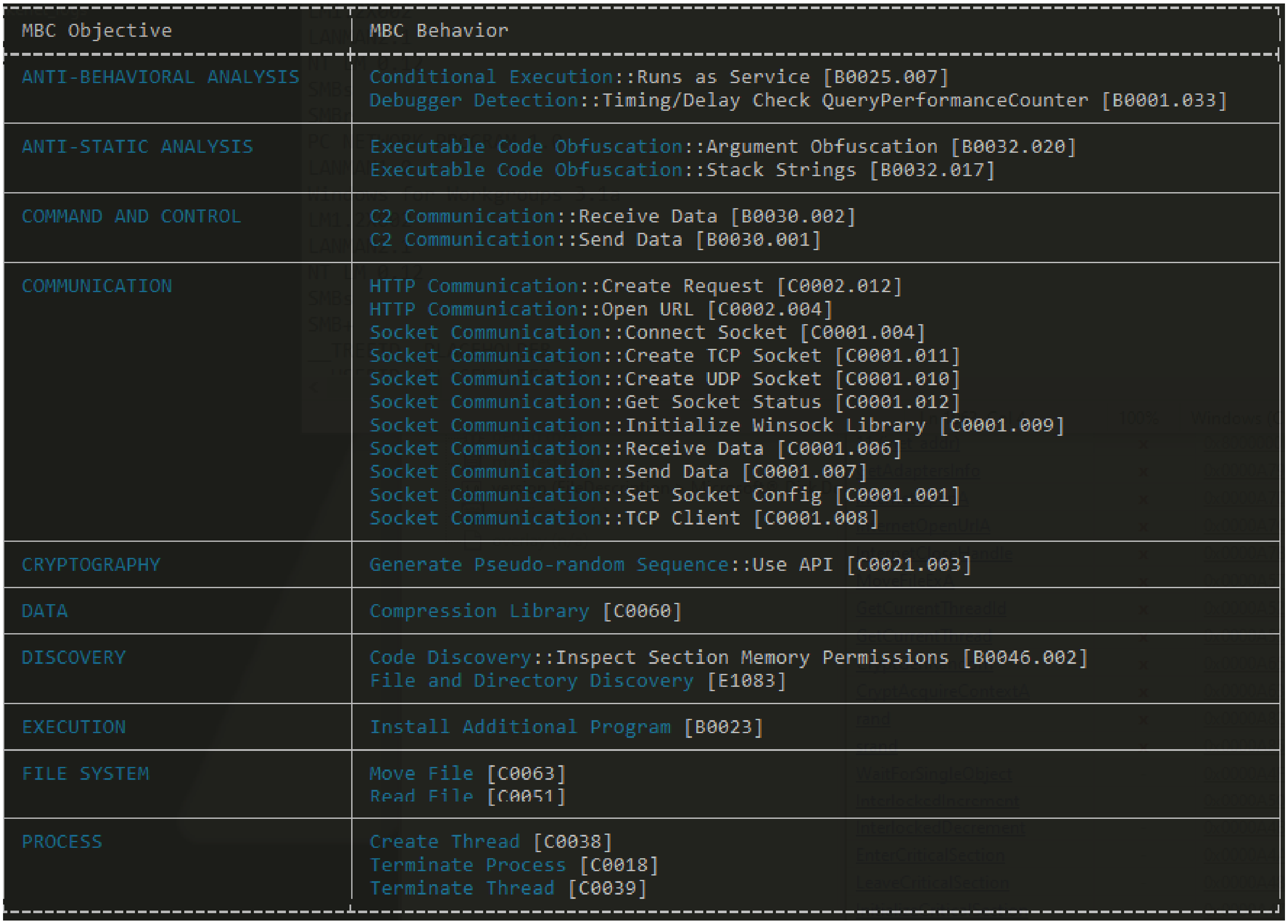
Upon examining the sizes of the Image Secion Header, there's a minimal difference between the Virtual Size and the Raw Data Size, indicating that the binary is likely unpacked.

Inspecting the binary malicious capabilities using Capa:



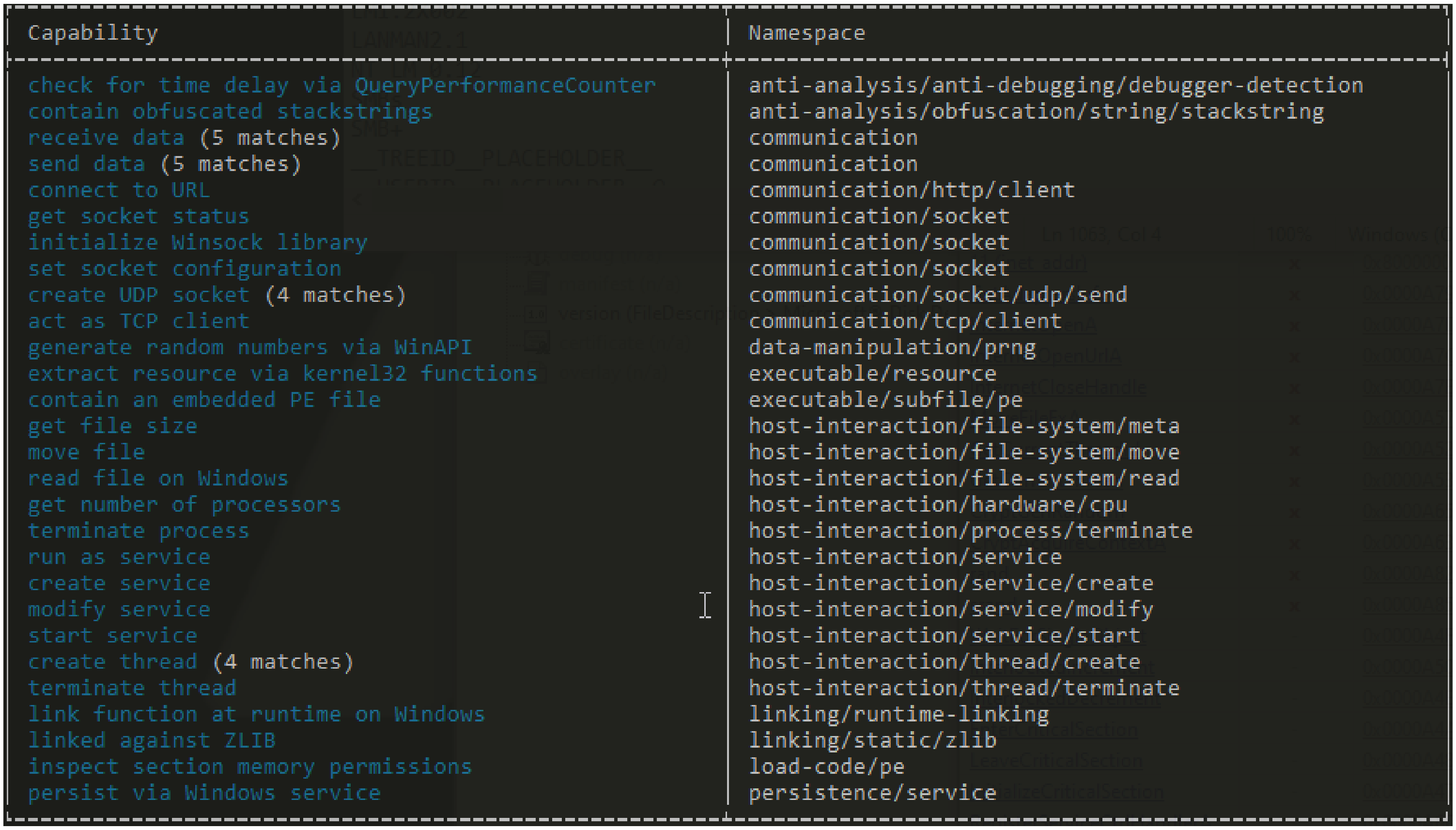
```
ATT&CK Tactic      | ATT&CK Technique
-------------------+------------------------------------------------------------------
DEFENSE EVASION    | Obfuscated Files or Information::Indicator Removal from Tools T1027.005
DISCOVERY          | File and Directory Discovery T1083
                   | System 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
```

Figure 10 – ATT&CK Details by Capa



```
+--------------------------+--------------------------------------------------------------------------+
| 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     | Executable Code Obfuscation::Argument Obfuscation [B0032.020]            |
|                          | Executable Code Obfuscation::Stack Strings [B0032.017]                   |
|--------------------------|--------------------------------------------------------------------------|
| 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]           |
|                          | File and Directory Discovery [E1083]                                     |
|--------------------------|--------------------------------------------------------------------------|
| EXECUTION                | Install Additional Program [B0023]                                       |
|--------------------------|--------------------------------------------------------------------------|
| FILE SYSTEM              | Move File [C0063]                                                        |
|                          | Read File [C0051]                                                        |
|--------------------------|--------------------------------------------------------------------------|
| PROCESS                  | Create Thread [C0038]                                                    |
|                          | Terminate Process [C0018]                                                |
|                          | Terminate Thread [C0039]                                                 |
+--------------------------+--------------------------------------------------------------------------+
```

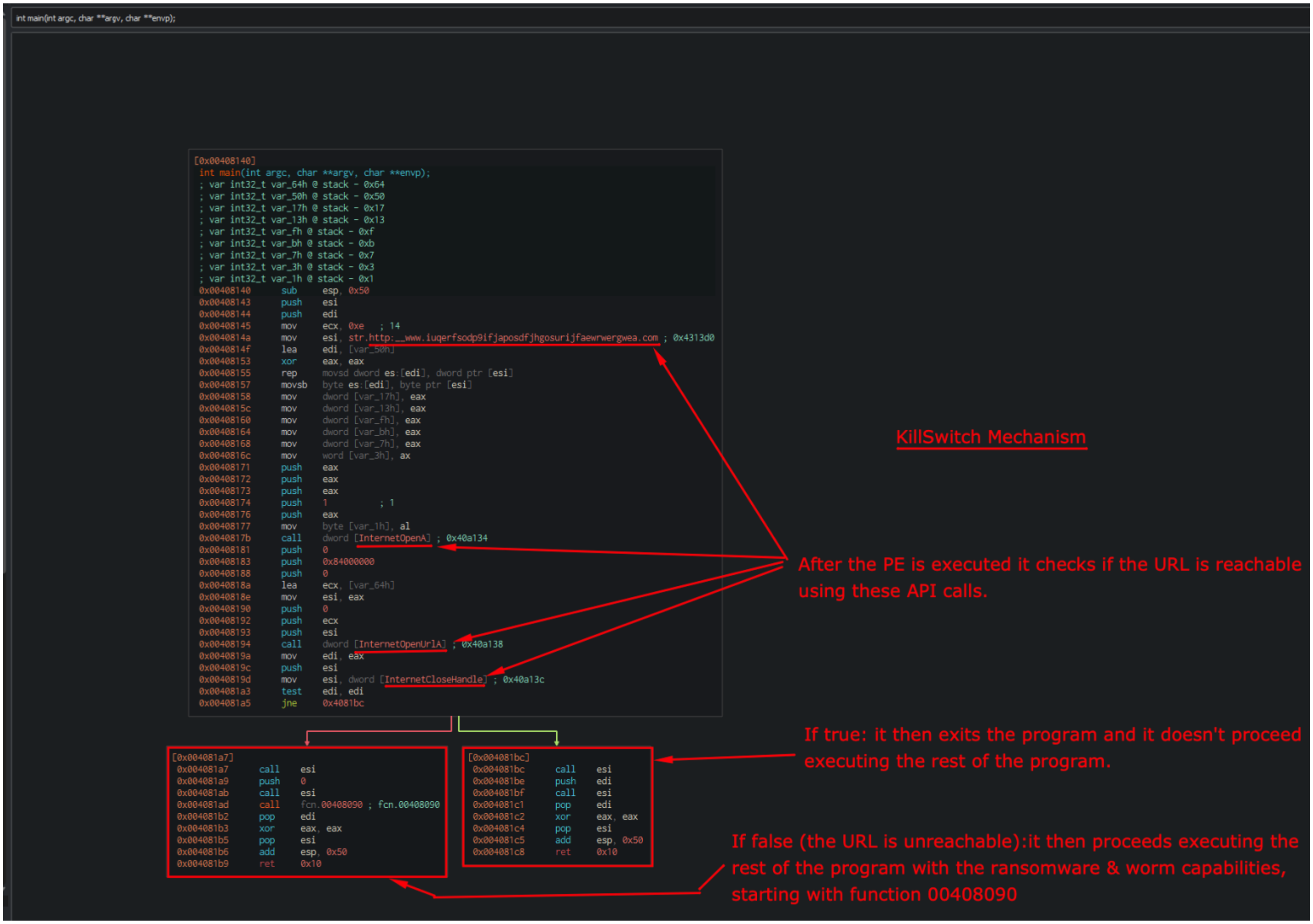
Figure 11 – Malware Behavior Catalog Details by Capa



```
+----------------------------------------------------+------------------------------------------------------+
| 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                               |
| 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                                  |
+----------------------------------------------------+------------------------------------------------------+
```

Figure 12 – Capabilities Details by Capa

Statically debugging the binary into Assembly language level:



```
int main(int argc, char **argv, char **envp);
```

```
[0x00408140]
 int main(int argc, char **argv, char **envp);
 ; var int32_t var_64h @ stack - 0x64
 ; var int32_t var_50h @ stack - 0x50
 ; var int32_t var_17h @ stack - 0x17
 ; var int32_t var_13h @ stack - 0x13
 ; var int32_t var_fh @ stack - 0xf
 ; var int32_t var_bh @ stack - 0xb
 ; var int32_t var_7h @ stack - 0x7
 ; var int32_t var_3h @ stack - 0x3
 ; var int32_t var_1h @ stack - 0x1
 0x00408140      sub     esp, 0x50
 0x00408143      push    esi
 0x00408144      push    edi
 0x00408145      mov     ecx, 0xe   ; 14
 0x0040814a      mov     esi, str.http:__www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com ; 0x4313d0
 0x0040814f      lea     edi, [var_50h]
 0x00408153      xor     eax, eax
 0x00408155      rep     movsd dword es:[edi], dword ptr [esi]
 0x00408157      movsb   byte es:[edi], byte ptr [esi]
 0x00408158      mov     dword [var_17h], eax
 0x0040815c      mov     dword [var_13h], eax
 0x00408160      mov     dword [var_fh], eax
 0x00408164      mov     dword [var_bh], eax
 0x00408168      mov     dword [var_7h], eax
 0x0040816c      mov     word [var_3h], ax
 0x00408171      push    eax
 0x00408172      push    eax
 0x00408173      push    eax
 0x00408174      push    1          ; 1
 0x00408176      push    eax
 0x00408177      mov     byte [var_1h], al
 0x0040817b      call    dword [InternetOpenA] ; 0x40a134
 0x00408181      push    0
 0x00408183      push    0x84000000
 0x00408188      push    0
 0x0040818a      lea     ecx, [var_64h]
 0x0040818e      mov     esi, eax
 0x00408190      push    0
 0x00408192      push    ecx
 0x00408193      push    esi
 0x00408194      call    dword [InternetOpenUrlA] ; 0x40a138
 0x0040819a      mov     edi, eax
 0x0040819c      push    esi
 0x0040819d      mov     esi, dword [InternetCloseHandle] ; 0x40a13c
 0x004081a3      test    edi, edi
 0x004081a5      jne     0x4081bc
```

```
[0x004081a7]
 0x004081a7      call    esi
 0x004081a9      push    0
 0x004081ab      call    esi
 0x004081ad      call    fcn.00408090 ; fcn.00408090
 0x004081b2      pop     edi
 0x004081b3      xor     eax, eax
 0x004081b5      pop     esi
 0x004081b6      add     esp, 0x50
 0x004081b9      ret     0x10
```

```
[0x004081bc]
 0x004081bc      call    esi
 0x004081be      push    edi
 0x004081bf      call    esi
 0x004081c1      pop     edi
 0x004081c2      xor     eax, eax
 0x004081c4      pop     esi
 0x004081c5      add     esp, 0x50
 0x004081c8      ret     0x10
```

KillSwitch Mechanism

After the PE is executed it checks if the URL is reachable using these API calls.

If true: it then exits the program and it doesn't proceed executing the rest of the program.

If false (the URL is unreachable):it then proceeds executing the rest of the program with the ransomware & worm capabilities, starting with function 00408090

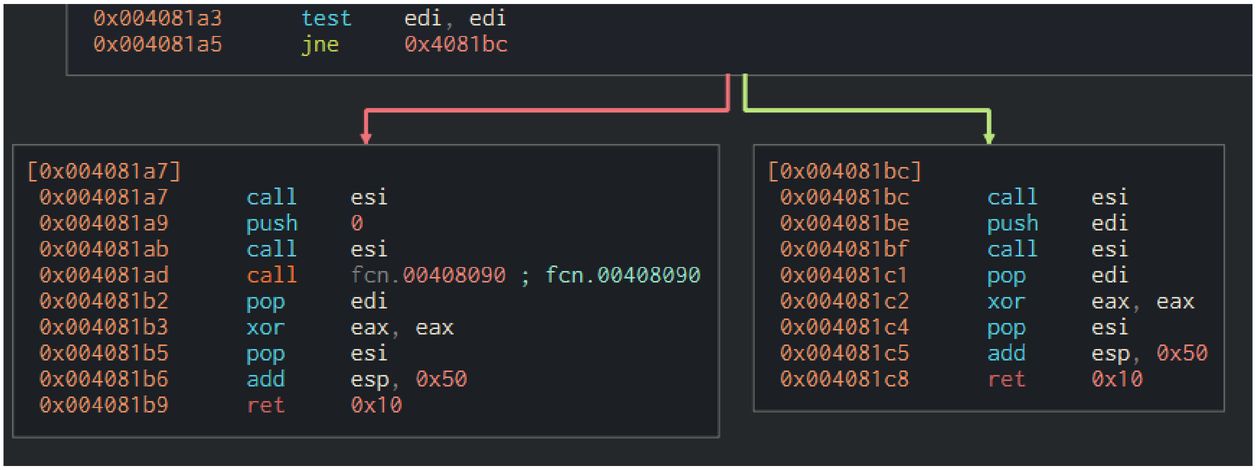
Figure 13 – The Main Function of The Binary

The **main** fundtion of the malware binary's primary function acts as a kill-switch, which includes a long URL string, Windows API calls to establish an internet connection and access the specified URL. It then saves the result of reaching the malicious URL, and based on the result, it determines whether to activate the malicious payload or not.

If the connection is successful, it will stop and exit itself, and if there **ins't** a connection it will proceed executing the rest of the program and move to function 00408090.

More in depth:

- The string of the killswitch URL is moved into ECX.
- The arguments for InternetOpenA are pushed onto the stack. The boolean result of InternetOpenA is moved into EAX.
- The arguments for InternetOpenUrlA are pushed onto the stack, including the killswitch URL.
  The result of InternetOpenUrlA is moved into EAX. Then, this result is also moved into EDI.
- The handle is closed and the program evaluates the value of EDI.
- If the value is 0x0 (i.e, NULL), WannaCry makes a call to the first function (00408090) in the payload.
- Else, WannaCry exits without triggering the payload.



```
0x004081a3      test    edi, edi
0x004081a5      jne     0x4081bc
```

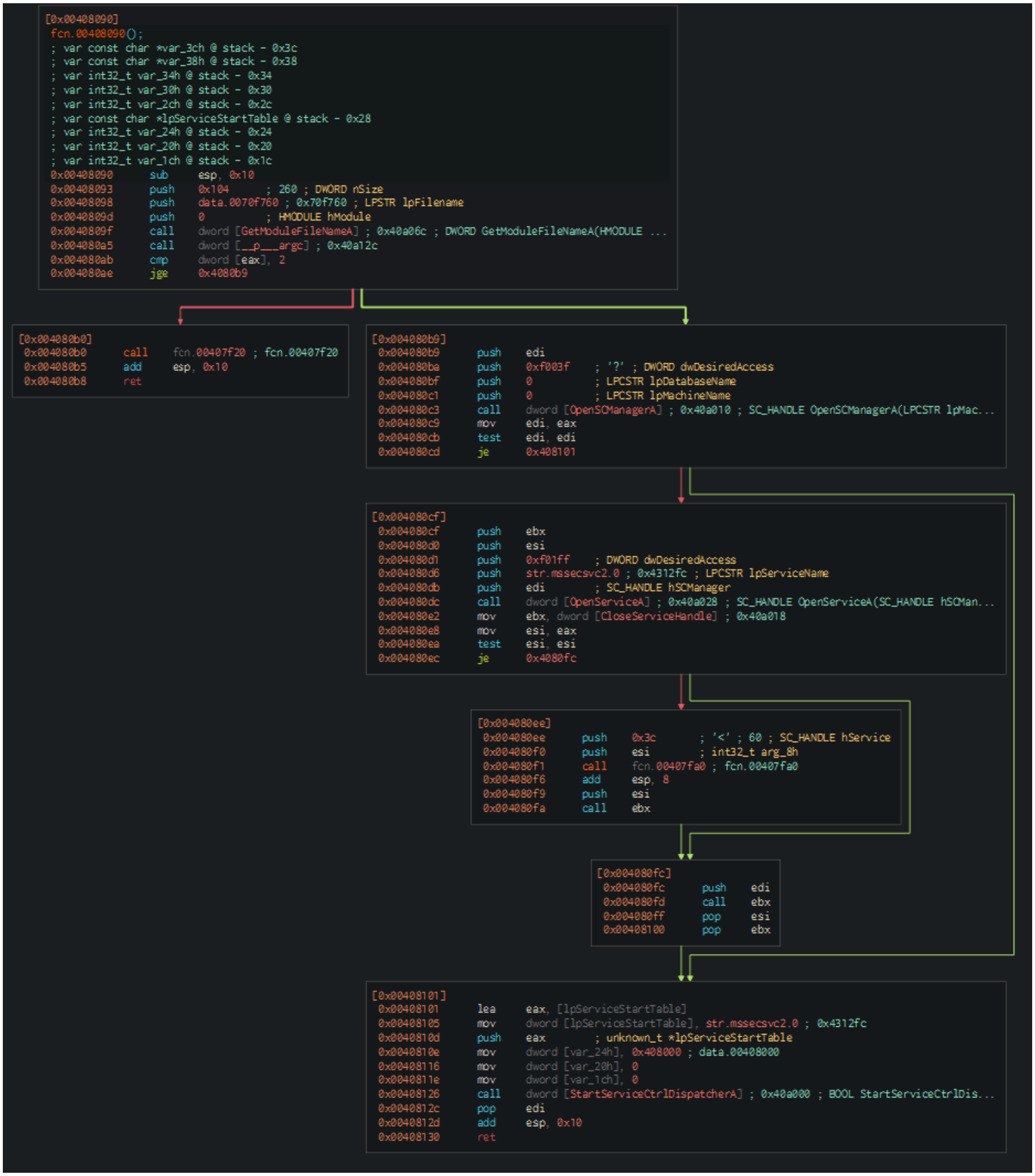
```
[0x004081a7]
 0x004081a7      call    esi
 0x004081a9      push    0
 0x004081ab      call    esi
 0x004081ad      call    fcn.00408090 ; fcn.00408090
 0x004081b2      pop     edi
 0x004081b3      xor     eax, eax
 0x004081b5      pop     esi
 0x004081b6      add     esp, 0x50
 0x004081b9      ret     0x10
```

```
[0x004081bc]
 0x004081bc      call    esi
 0x004081be      push    edi
 0x004081bf      call    esi
 0x004081c1      pop     edi
 0x004081c2      xor     eax, eax
 0x004081c4      pop     esi
 0x004081c5      add     esp, 0x50
 0x004081c8      ret     0x10
```

Figure 14 – Kill Switch

The result of wether the long URL is accessible or not will be saved (edi), and then in the test function, the edi value will test it against it self (edi, edi).
Based on that, if the value is **True** (the URL is accessible) the JNE (Jump Not Equal) will jump to the memory address 0x4081bc and exit the program.
If the value is **False** (there isn't a connection witht the specified URL), it will proceed to function 00408090 and executes the payload.

Function 00408090, the starting point of the payload, has been called after a successful execution, which then starts modifying files in the currently running process and begins the attack.



```
[0x00408090]
 fcn.00408090();
 ; var const char *var_3ch @ stack - 0x3c
 ; var const char *var_38h @ stack - 0x38
 ; var int32_t var_34h @ stack - 0x34
 ; var int32_t var_30h @ stack - 0x30
 ; var int32_t var_2ch @ stack - 0x2c
 ; var const char *lpServiceStartTable @ stack - 0x28
 ; var int32_t var_24h @ stack - 0x24
 ; var int32_t var_20h @ stack - 0x20
 ; var int32_t var_1ch @ stack - 0x1c
 0x00408090      sub     esp, 0x10
 0x00408093      push    0x104       ; 260 ; DWORD nSize
 0x00408098      push    data.0070f760 ; 0x70f760 ; LPSTR lpFilename
 0x0040809d      push    0           ; HMODULE hModule
 0x0040809f      call    dword [GetModuleFileNameA] ; 0x40a06c ; DWORD GetModuleFileNameA(HMODULE ...
 0x004080a5      call    dword [__p___argc] ; 0x40a12c
 0x004080ab      cmp     dword [eax], 2
 0x004080ae      jge     0x4080b9
```

```
[0x004080b0]
 0x004080b0      call    fcn.00407f20 ; fcn.00407f20
 0x004080b5      add     esp, 0x10
 0x004080b8      ret
```

```
[0x004080b9]
 0x004080b9      push    edi
 0x004080ba      push    0xf003f     ; '?' ; DWORD dwDesiredAccess
 0x004080bf      push    0           ; LPCSTR lpDatabaseName
 0x004080c1      push    0           ; LPCSTR lpMachineName
 0x004080c3      call    dword [OpenSCManagerA] ; 0x40a010 ; SC_HANDLE OpenSCManagerA(LPCSTR lpMac...
 0x004080c9      mov     edi, eax
 0x004080cb      test    edi, edi
 0x004080cd      je      0x408101
```

```
[0x004080cf]
 0x004080cf      push    ebx
 0x004080d0      push    esi
 0x004080d1      push    0xf01ff     ; DWORD dwDesiredAccess
 0x004080d6      push    str.mssecsvc2.0 ; 0x4312fc ; LPCSTR lpServiceName
 0x004080db      push    edi         ; SC_HANDLE hSCManager
 0x004080dc      call    dword [OpenServiceA] ; 0x40a028 ; SC_HANDLE OpenServiceA(SC_HANDLE hSCMan...
 0x004080e2      mov     ebx, dword [CloseServiceHandle] ; 0x40a018
 0x004080e8      mov     esi, eax
 0x004080ea      test    esi, esi
 0x004080ec      je      0x4080fc
```

```
[0x004080ee]
 0x004080ee      push    0x3c         ; '<' ; 60 ; SC_HANDLE hService
 0x004080f0      push    esi          ; int32_t arg_8h
 0x004080f1      call    fcn.00407fa0 ; fcn.00407fa0
 0x004080f6      add     esp, 8
 0x004080f9      push    esi
 0x004080fa      call    ebx
```

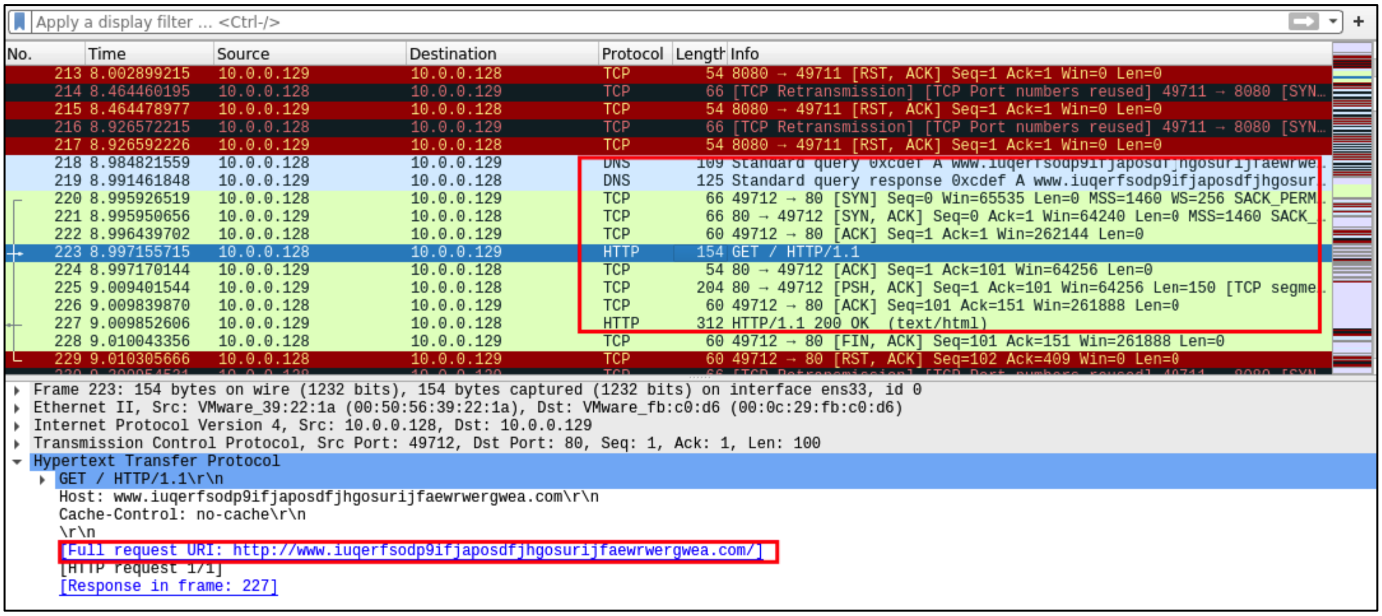
```
[0x004080fc]
 0x004080fc      push    edi
 0x004080fd      call    ebx
 0x004080ff      pop     esi
 0x00408100      pop     ebx
```

```
[0x00408101]
 0x00408101      lea     eax, [lpServiceStartTable]
 0x00408105      mov     dword [lpServiceStartTable], str.mssecsvc2.0 ; 0x4312fc
 0x0040810d      push    eax         ; unknown_t *lpServiceStartTable
 0x0040810e      mov     dword [var_24h], 0x408000 ; data.00408000
 0x00408116      mov     dword [var_20h], 0
 0x0040811e      mov     dword [var_1ch], 0
 0x00408126      call    dword [StartServiceCtrlDispatcherA] ; 0x40a000 ; BOOL StartServiceCtrlDis...
 0x0040812c      pop     edi
 0x0040812d      add     esp, 0x10
 0x00408130      ret
```

Figure 15 – fcn.00408090

Dynamic Analysis

Detonation with internet connection:
In this phase, we'll detonate the malware while using InetSim to simulate an active internet connection.



```
Apply a display filter ... <Ctrl-/>

No.   Time         Source       Destination  Protocol Length Info
  213 8.002899215  10.0.0.129   10.0.0.128   TCP        54 8080 → 49711 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  214 8.464460195  10.0.0.128   10.0.0.129   TCP        66 [TCP Retransmission] [TCP Port numbers reused] 49711 → 8080 [SYN…
  215 8.464478977  10.0.0.129   10.0.0.128   TCP        54 8080 → 49711 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  216 8.926572215  10.0.0.128   10.0.0.129   TCP        66 [TCP Retransmission] [TCP Port numbers reused] 49711 → 8080 [SYN…
  217 8.926592226  10.0.0.129   10.0.0.128   TCP        54 8080 → 49711 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  218 8.984821559  10.0.0.128   10.0.0.129   DNS       109 Standard query 0xcdef A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwe…
  219 8.991461848  10.0.0.129   10.0.0.128   DNS       125 Standard query response 0xcdef A www.iuqerfsodp9ifjaposdfjhgosur…
  220 8.995926519  10.0.0.128   10.0.0.129   TCP        66 49712 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM…
  221 8.995950656  10.0.0.129   10.0.0.128   TCP        66 80 → 49712 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_…
  222 8.996439702  10.0.0.128   10.0.0.129   TCP        60 49712 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
  223 8.997155715  10.0.0.128   10.0.0.129   HTTP      154 GET / HTTP/1.1
  224 8.997170144  10.0.0.129   10.0.0.128   TCP        54 80 → 49712 [ACK] Seq=1 Ack=101 Win=64256 Len=0
  225 9.009401544  10.0.0.129   10.0.0.128   TCP       204 80 → 49712 [PSH, ACK] Seq=1 Ack=101 Win=64256 Len=150 [TCP segme…
  226 9.009839870  10.0.0.128   10.0.0.129   TCP        60 49712 → 80 [ACK] Seq=101 Ack=151 Win=261888 Len=0
  227 9.009852606  10.0.0.129   10.0.0.128   HTTP      312 HTTP/1.1 200 OK  (text/html)
  228 9.010043356  10.0.0.128   10.0.0.129   TCP        60 49712 → 80 [FIN, ACK] Seq=101 Ack=151 Win=261888 Len=0
  229 9.010305666  10.0.0.128   10.0.0.129   TCP        60 49712 → 80 [RST, ACK] Seq=102 Ack=409 Win=0 Len=0

▸ Frame 223: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) on interface ens33, id 0
▸ Ethernet II, Src: VMware_39:22:1a (00:50:56:39:22:1a), Dst: VMware_fb:c0:d6 (00:0c:29:fb:c0:d6)
▸ Internet Protocol Version 4, Src: 10.0.0.128, Dst: 10.0.0.129
▸ Transmission Control Protocol, Src Port: 49712, 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: 227]
```

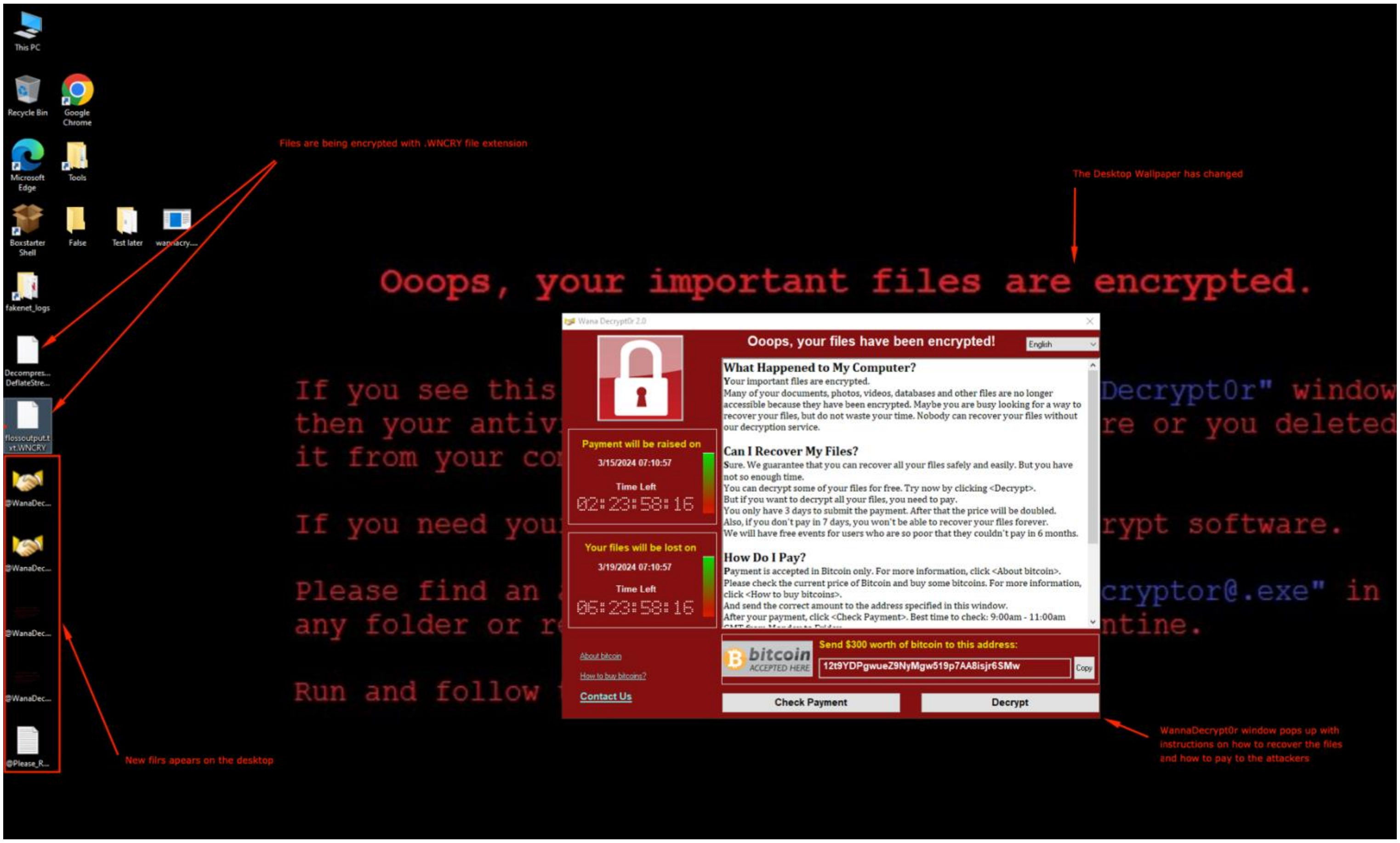
Figure 16 – Wireshark Network Traffic

Upon inspecting the network traffic after the initial detonation of the malware while there is an active internet connection, we can see that after the DNS request and TCP 3-Way Handshake, there's an HTTP traffic with GET response to the long URL that we saw earlier:
hxxp://www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com

Right after that, we see another HTTP traffic with status code of "200 OK" which indicates that the request has succeeded and the malware was able to reach this URL.

In this case, the malware will exit itself and won't proceed with executing the payload.

Detonating without internet connection:



Files are being encrypted with .WNCRY file extension

The Desktop Wallpaper has changed

Ooops, your important files are encrypted.

If you see this … Decrypt0r" window
then your antiv… re or you deleted
it from your co…

If you need you… rypt software.

Please find an … cryptor@.exe" in
any folder or r… ntine.

Run and follow …

Ooops, your files have been encrypted!

Payment will be raised on
3/15/2024 07:10:57
Time Left
02:23:58:16

Your files will be lost on
3/19/2024 07:10:57
Time Left
06:23:58:16

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

New filrs apears on the desktop

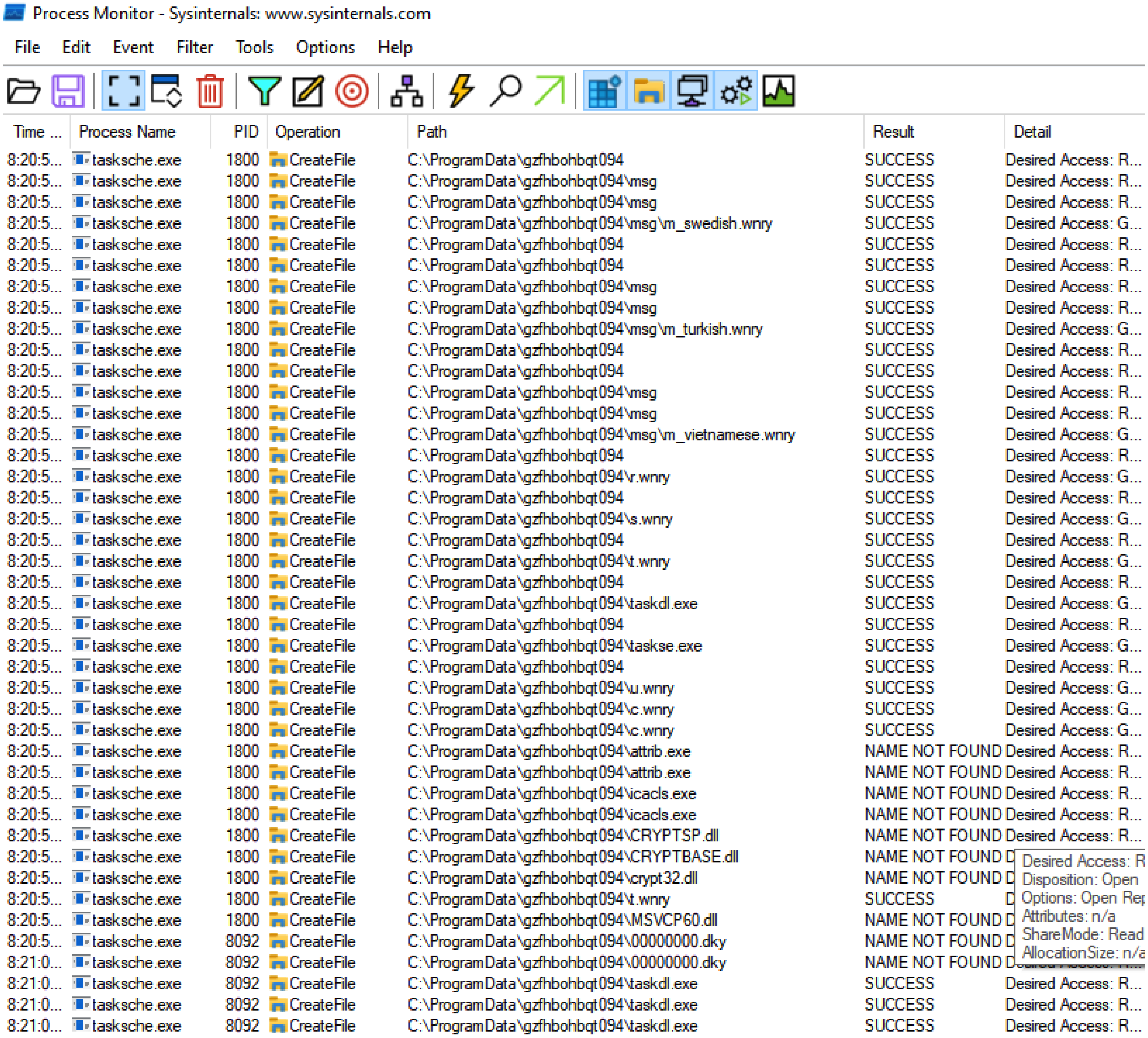
WannaDecrypt0r window pops up with instructions on how to recover the files and how to pay to the attackers

Figure 17 – WannaCry initial Detonation

Few seconds after detonating the the malware, we can some of the symptoms of the malware:

- Files are getting encrypted with ".WNCRY" file extension.
- The desktop’s wallpaper has been changed from the original wallpaper to black image with instructions to the victim on how to act in order to get his data back.
- The WannaDecrypt0r.exe pops up with a timer and instructions on how to pay the attackers’ wallet with Bitcoin.
- Appearance of new files on the desktop related to the WannaCry Ransomware.
    - .bmp image files, which replaced the original desktop’s wallpaper.
    - WannaDecrypt0r.exe which is shown on the center of the screen.
    - Text file with instructions on how to recover the files and how to pay to the attackers.

While inspecting the host-based indicators and filtering for file creation, we can see a lot of files are being created and located in “C:\ProgramData\gzfhbohbqt094”, mainly by the process “tasksche.exe” (also shown in figure 2).

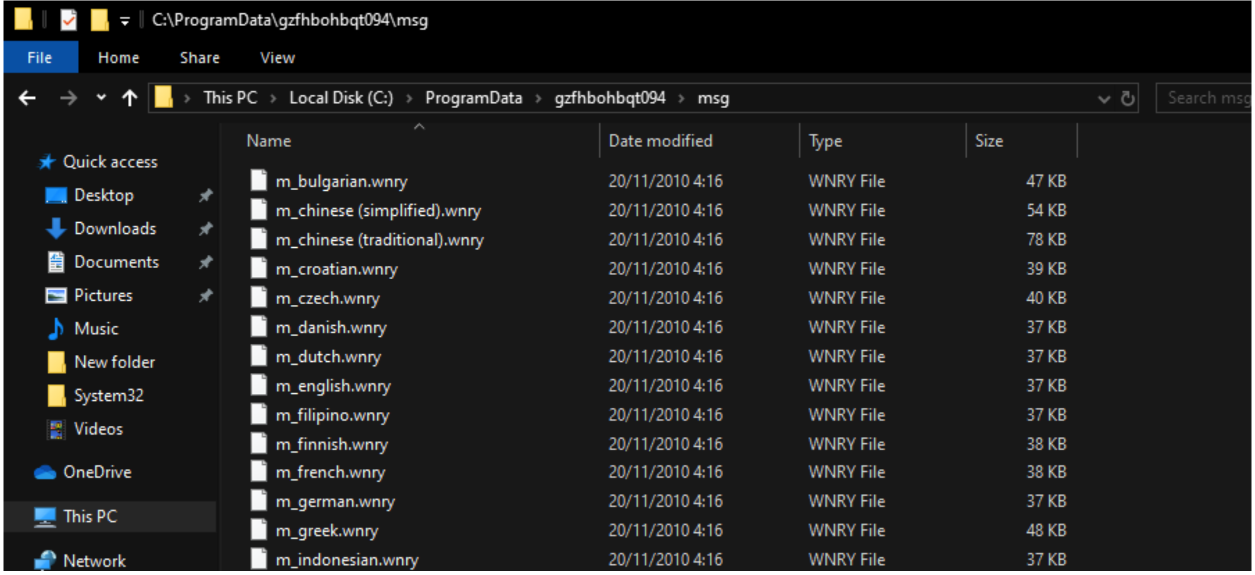


Time ...	Process Name	PID	Operation	Path	Result	Detail
8:20:5...	tasksche.exe	1800	CreateFile	C:\ProgramData\gzfhbohbqt094	SUCCESS	Desired Access: R...
8:20:5...	tasksche.exe	1800	CreateFile	C:\ProgramData\gzfhbohbqt094\msg	SUCCESS	Desired Access: R...
8:20:5...	tasksche.exe	1800	CreateFile	C:\ProgramData\gzfhbohbqt094\msg	SUCCESS	Desired Access: R...
8:20:5...	tasksche.exe	1800	CreateFile	C:\ProgramData\gzfhbohbqt094\msg\m_swedish.wnry	SUCCESS	Desired Access: G...
8:20:5...	tasksche.exe	1800	CreateFile	C:\ProgramData\gzfhbohbqt094	SUCCESS	Desired Access: R...
8:20:5...	tasksche.exe	1800	CreateFile	C:\ProgramData\gzfhbohbqt094	SUCCESS	Desired Access: R...
8:20:5...	tasksche.exe	1800	CreateFile	C:\ProgramData\gzfhbohbqt094\msg	SUCCESS	Desired Access: R...
8:20:5...	tasksche.exe	1800	CreateFile	C:\ProgramData\gzfhbohbqt094\msg	SUCCESS	Desired Access: R...
8:20:5...	tasksche.exe	1800	CreateFile	C:\ProgramData\gzfhbohbqt094\msg\m_turkish.wnry	SUCCESS	Desired Access: G...
8:20:5...	tasksche.exe	1800	CreateFile	C:\ProgramData\gzfhbohbqt094	SUCCESS	Desired Access: R...
8:20:5...	tasksche.exe	1800	CreateFile	C:\ProgramData\gzfhbohbqt094	SUCCESS	Desired Access: R...
8:20:5...	tasksche.exe	1800	CreateFile	C:\ProgramData\gzfhbohbqt094\msg	SUCCESS	Desired Access: R...
8:20:5...	tasksche.exe	1800	CreateFile	C:\ProgramData\gzfhbohbqt094\msg	SUCCESS	Desired Access: R...
8:20:5...	tasksche.exe	1800	CreateFile	C:\ProgramData\gzfhbohbqt094\msg\m_vietnamese.wnry	SUCCESS	Desired Access: G...
8:20:5...	tasksche.exe	1800	CreateFile	C:\ProgramData\gzfhbohbqt094	SUCCESS	Desired Access: R...
8:20:5...	tasksche.exe	1800	CreateFile	C:\ProgramData\gzfhbohbqt094\r.wnry	SUCCESS	Desired Access: G...
8:20:5...	tasksche.exe	1800	CreateFile	C:\ProgramData\gzfhbohbqt094	SUCCESS	Desired Access: R...
8:20:5...	tasksche.exe	1800	CreateFile	C:\ProgramData\gzfhbohbqt094\s.wnry	SUCCESS	Desired Access: G...
8:20:5...	tasksche.exe	1800	CreateFile	C:\ProgramData\gzfhbohbqt094	SUCCESS	Desired Access: R...
8:20:5...	tasksche.exe	1800	CreateFile	C:\ProgramData\gzfhbohbqt094\t.wnry	SUCCESS	Desired Access: G...
8:20:5...	tasksche.exe	1800	CreateFile	C:\ProgramData\gzfhbohbqt094	SUCCESS	Desired Access: R...
8:20:5...	tasksche.exe	1800	CreateFile	C:\ProgramData\gzfhbohbqt094\taskdl.exe	SUCCESS	Desired Access: G...
8:20:5...	tasksche.exe	1800	CreateFile	C:\ProgramData\gzfhbohbqt094	SUCCESS	Desired Access: R...
8:20:5...	tasksche.exe	1800	CreateFile	C:\ProgramData\gzfhbohbqt094\taskse.exe	SUCCESS	Desired Access: G...
8:20:5...	tasksche.exe	1800	CreateFile	C:\ProgramData\gzfhbohbqt094	SUCCESS	Desired Access: R...
8:20:5...	tasksche.exe	1800	CreateFile	C:\ProgramData\gzfhbohbqt094\u.wnry	SUCCESS	Desired Access: G...
8:20:5...	tasksche.exe	1800	CreateFile	C:\ProgramData\gzfhbohbqt094\c.wnry	SUCCESS	Desired Access: G...
8:20:5...	tasksche.exe	1800	CreateFile	C:\ProgramData\gzfhbohbqt094\c.wnry	SUCCESS	Desired Access: G...
8:20:5...	tasksche.exe	1800	CreateFile	C:\ProgramData\gzfhbohbqt094\attrib.exe	NAME NOT FOUND	Desired Access: R...
8:20:5...	tasksche.exe	1800	CreateFile	C:\ProgramData\gzfhbohbqt094\attrib.exe	NAME NOT FOUND	Desired Access: R...
8:20:5...	tasksche.exe	1800	CreateFile	C:\ProgramData\gzfhbohbqt094\icacls.exe	NAME NOT FOUND	Desired Access: R...
8:20:5...	tasksche.exe	1800	CreateFile	C:\ProgramData\gzfhbohbqt094\icacls.exe	NAME NOT FOUND	Desired Access: R...
8:20:5...	tasksche.exe	1800	CreateFile	C:\ProgramData\gzfhbohbqt094\CRYPTSP.dll	NAME NOT FOUND	Desired Access: R...
8:20:5...	tasksche.exe	1800	CreateFile	C:\ProgramData\gzfhbohbqt094\CRYPTBASE.dll	NAME NOT FOUND	D
8:20:5...	tasksche.exe	1800	CreateFile	C:\ProgramData\gzfhbohbqt094\crypt32.dll	NAME NOT FOUND	D
8:20:5...	tasksche.exe	1800	CreateFile	C:\ProgramData\gzfhbohbqt094\t.wnry	SUCCESS	D
8:20:5...	tasksche.exe	1800	CreateFile	C:\ProgramData\gzfhbohbqt094\MSVCP60.dll	NAME NOT FOUND	D
8:20:5...	tasksche.exe	8092	CreateFile	C:\ProgramData\gzfhbohbqt094\00000000.dky	NAME NOT FOUND	D
8:21:0...	tasksche.exe	8092	CreateFile	C:\ProgramData\gzfhbohbqt094\00000000.dky	NAME NOT FOUND	D
8:21:0...	tasksche.exe	8092	CreateFile	C:\ProgramData\gzfhbohbqt094\taskdl.exe	SUCCESS	Desired Access: R...
8:21:0...	tasksche.exe	8092	CreateFile	C:\ProgramData\gzfhbohbqt094\taskdl.exe	SUCCESS	Desired Access: R...
8:21:0...	tasksche.exe	8092	CreateFile	C:\ProgramData\gzfhbohbqt094\taskdl.exe	SUCCESS	Desired Access: R...

Desired Access: R
Disposition: Open
Options: Open Rep
Attributes: n/a
ShareMode: Read
AllocationSize: n/a

Figure 18 – File Creation with Procmon

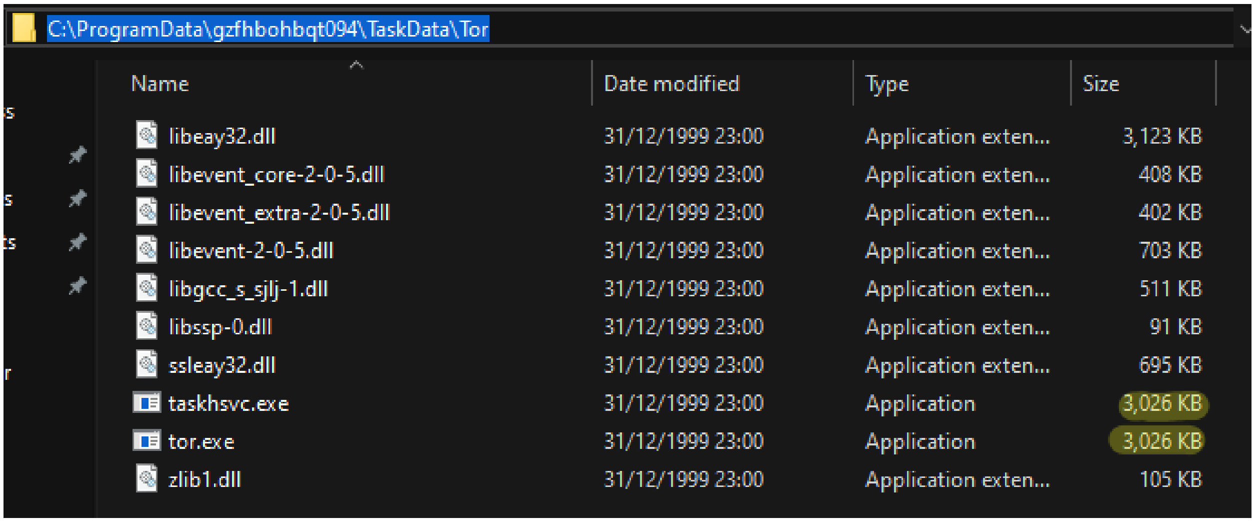
Another folder within the “gzfhbohbqt094” folder is the “msg” folder that contains .wnry files. These files are RTF files containing the ransomware information in different languages.



Name	Date modified	Type	Size
m_bulgarian.wnry	20/11/2010 4:16	WNRY File	47 KB
m_chinese (simplified).wnry	20/11/2010 4:16	WNRY File	54 KB
m_chinese (traditional).wnry	20/11/2010 4:16	WNRY File	78 KB
m_croatian.wnry	20/11/2010 4:16	WNRY File	39 KB
m_czech.wnry	20/11/2010 4:16	WNRY File	40 KB
m_danish.wnry	20/11/2010 4:16	WNRY File	37 KB
m_dutch.wnry	20/11/2010 4:16	WNRY File	37 KB
m_english.wnry	20/11/2010 4:16	WNRY File	37 KB
m_filipino.wnry	20/11/2010 4:16	WNRY File	37 KB
m_finnish.wnry	20/11/2010 4:16	WNRY File	38 KB
m_french.wnry	20/11/2010 4:16	WNRY File	38 KB
m_german.wnry	20/11/2010 4:16	WNRY File	37 KB
m_greek.wnry	20/11/2010 4:16	WNRY File	48 KB
m_indonesian.wnry	20/11/2010 4:16	WNRY File	37 KB

Figure 19 – msg Folder

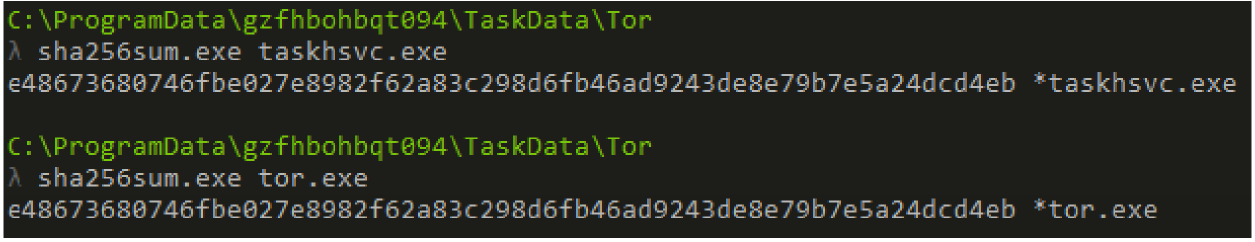
Additional folder is the“Tor” folder that’s located in “C:\ProgramData\gzfhbohbqt094\TaskData\Tor” and contains two executables: “taskhsvc.exe” & “tor.exe” which have similar file size. “taskhsvc.exe” appears to be a copy of “tor.exe”, probably to hide itself and be less easier to spot.



Name	Date modified	Type	Size
libeay32.dll	31/12/1999 23:00	Application exten...	3,123 KB
libevent_core-2-0-5.dll	31/12/1999 23:00	Application exten...	408 KB
libevent_extra-2-0-5.dll	31/12/1999 23:00	Application exten...	402 KB
libevent-2-0-5.dll	31/12/1999 23:00	Application exten...	703 KB
libgcc_s_sjlj-1.dll	31/12/1999 23:00	Application exten...	511 KB
libssp-0.dll	31/12/1999 23:00	Application exten...	91 KB
ssleay32.dll	31/12/1999 23:00	Application exten...	695 KB
taskhsvc.exe	31/12/1999 23:00	Application	3,026 KB
tor.exe	31/12/1999 23:00	Application	3,026 KB
zlib1.dll	31/12/1999 23:00	Application exten...	105 KB

Figure 20 – Tor Folder

I've also extracted the file hash for both of them and these appears to be the same file.



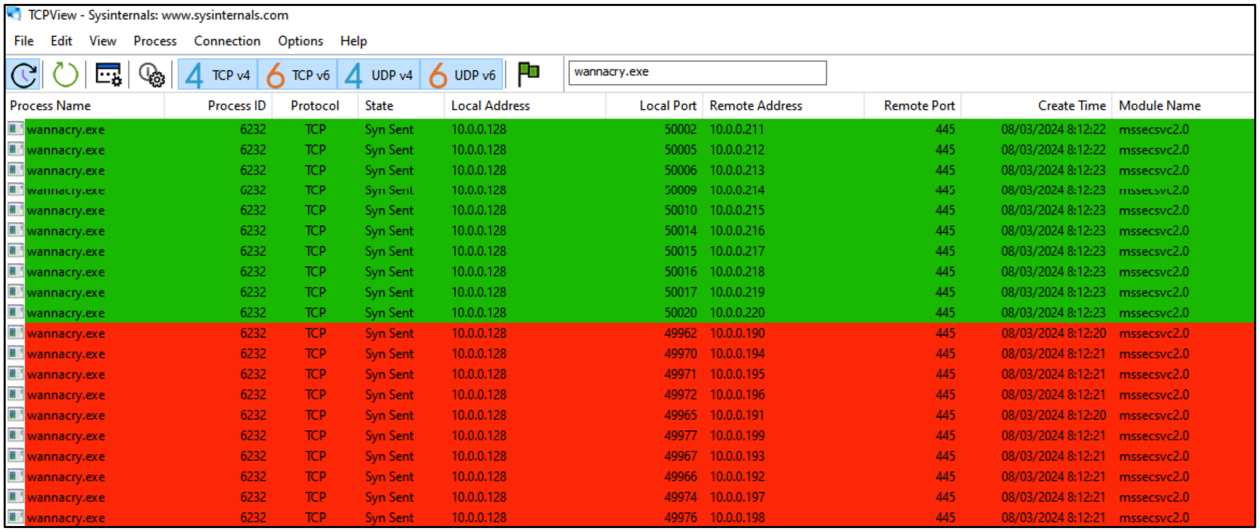
```
C:\ProgramData\gzfhbohbqt094\TaskData\Tor
λ sha256sum.exe taskhsvc.exe
e48673680746fbe027e8982f62a83c298d6fb46ad9243de8e79b7e5a24dcd4eb *taskhsvc.exe

C:\ProgramData\gzfhbohbqt094\TaskData\Tor
λ sha256sum.exe tor.exe
e48673680746fbe027e8982f62a83c298d6fb46ad9243de8e79b7e5a24dcd4eb *tor.exe
```

Figure 21 – Same Hash for both of the files

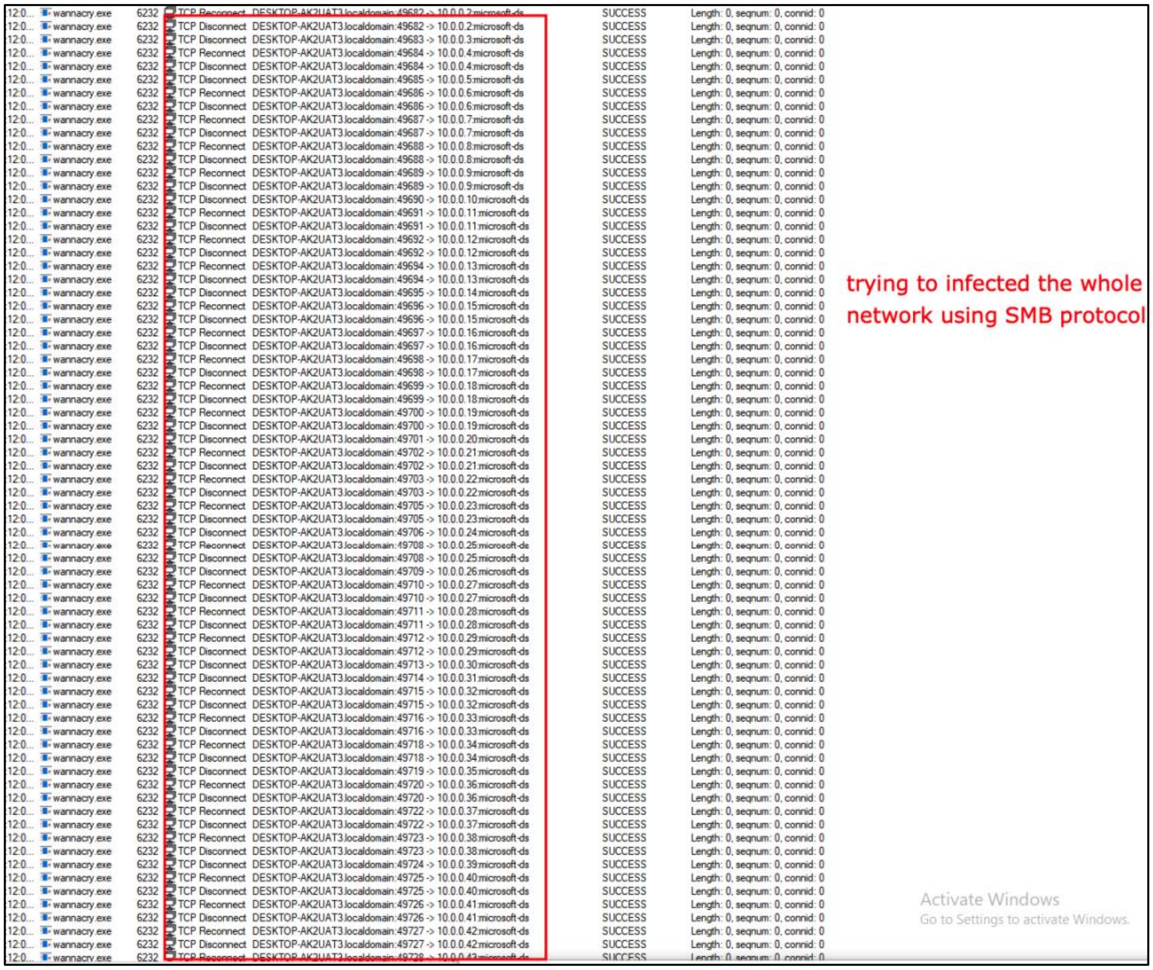
Upon looking for network indicators, we've seen that the "taskhsvc.exe" process opens port 9050 to a LISTENING state (as shown above in figure 3) which belong to "tor-socks" service (www.torproject.org) and attempts to connect to non-private remote addresses over HTTPS, attempts to contact the configured C2 hidden services.

In order to find more network indicators, I also used TCPView as and Procmon and noticed that WannaCry was sending TCP Syn requests on port 445 to every IP address that's in the subnet of the infected machine (10.0.0.0/24).
What the malware is trying to do is to infect other machines through the use of the SMB protocol, leveraging the EternalBlue Exploit developed by the NSA. We can see that WannaCry is not only Ransomware but also has Worm capabilities.



Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
wannacry.exe	6232	TCP	Syn Sent	10.0.0.128	50002	10.0.0.211	445	08/03/2024 8:12:22	mssecsvc2.0
wannacry.exe	6232	TCP	Syn Sent	10.0.0.128	50005	10.0.0.212	445	08/03/2024 8:12:22	mssecsvc2.0
wannacry.exe	6232	TCP	Syn Sent	10.0.0.128	50006	10.0.0.213	445	08/03/2024 8:12:23	mssecsvc2.0
wannacry.exe	6232	TCP	Syn Sent	10.0.0.128	50009	10.0.0.214	445	08/03/2024 8:12:23	mssecsvc2.0
wannacry.exe	6232	TCP	Syn Sent	10.0.0.128	50010	10.0.0.215	445	08/03/2024 8:12:23	mssecsvc2.0
wannacry.exe	6232	TCP	Syn Sent	10.0.0.128	50014	10.0.0.216	445	08/03/2024 8:12:23	mssecsvc2.0
wannacry.exe	6232	TCP	Syn Sent	10.0.0.128	50015	10.0.0.217	445	08/03/2024 8:12:23	mssecsvc2.0
wannacry.exe	6232	TCP	Syn Sent	10.0.0.128	50016	10.0.0.218	445	08/03/2024 8:12:23	mssecsvc2.0
wannacry.exe	6232	TCP	Syn Sent	10.0.0.128	50017	10.0.0.219	445	08/03/2024 8:12:23	mssecsvc2.0
wannacry.exe	6232	TCP	Syn Sent	10.0.0.128	50020	10.0.0.220	445	08/03/2024 8:12:23	mssecsvc2.0
wannacry.exe	6232	TCP	Syn Sent	10.0.0.128	49962	10.0.0.190	445	08/03/2024 8:12:20	mssecsvc2.0
wannacry.exe	6232	TCP	Syn Sent	10.0.0.128	49970	10.0.0.194	445	08/03/2024 8:12:21	mssecsvc2.0
wannacry.exe	6232	TCP	Syn Sent	10.0.0.128	49971	10.0.0.195	445	08/03/2024 8:12:21	mssecsvc2.0
wannacry.exe	6232	TCP	Syn Sent	10.0.0.128	49972	10.0.0.196	445	08/03/2024 8:12:21	mssecsvc2.0
wannacry.exe	6232	TCP	Syn Sent	10.0.0.128	49965	10.0.0.191	445	08/03/2024 8:12:20	mssecsvc2.0
wannacry.exe	6232	TCP	Syn Sent	10.0.0.128	49977	10.0.0.199	445	08/03/2024 8:12:21	mssecsvc2.0
wannacry.exe	6232	TCP	Syn Sent	10.0.0.128	49967	10.0.0.193	445	08/03/2024 8:12:21	mssecsvc2.0
wannacry.exe	6232	TCP	Syn Sent	10.0.0.128	49966	10.0.0.192	445	08/03/2024 8:12:21	mssecsvc2.0
wannacry.exe	6232	TCP	Syn Sent	10.0.0.128	49974	10.0.0.197	445	08/03/2024 8:12:21	mssecsvc2.0
wannacry.exe	6232	TCP	Syn Sent	10.0.0.128	49976	10.0.0.198	445	08/03/2024 8:12:21	mssecsvc2.0

Figure 21 – SMB Connections by TCPView

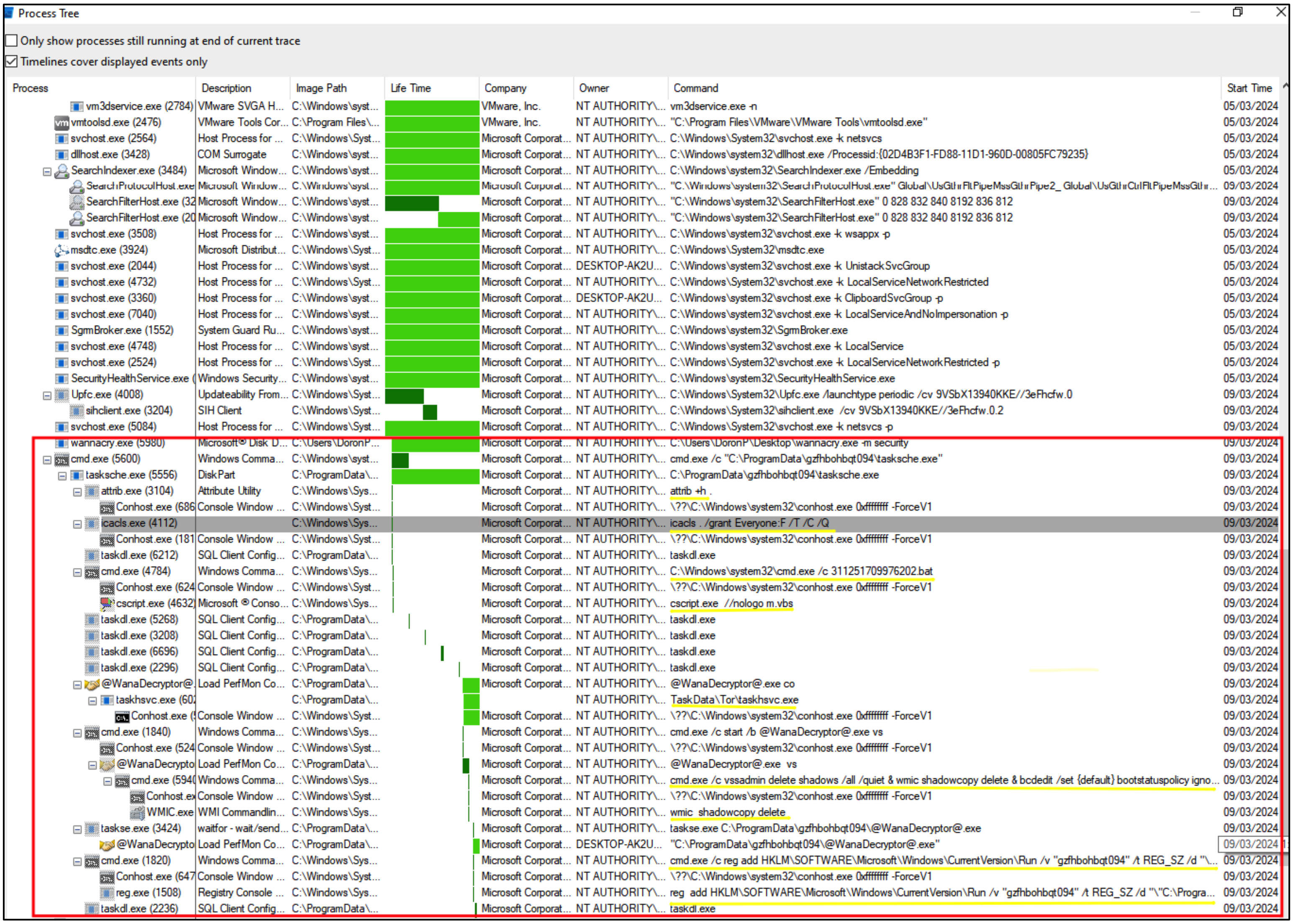


```
12:0...  wannacry.exe  6232  TCP Reconnect   DESKTOP-AK2UAT3.localdomain:49682 -> 10.0.0.2:microsoft-ds   SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49682 -> 10.0.0.2:microsoft-ds   SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49683 -> 10.0.0.3:microsoft-ds   SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Reconnect   DESKTOP-AK2UAT3.localdomain:49684 -> 10.0.0.4:microsoft-ds   SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49684 -> 10.0.0.4:microsoft-ds   SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49685 -> 10.0.0.5:microsoft-ds   SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Reconnect   DESKTOP-AK2UAT3.localdomain:49686 -> 10.0.0.6:microsoft-ds   SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49686 -> 10.0.0.6:microsoft-ds   SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Reconnect   DESKTOP-AK2UAT3.localdomain:49687 -> 10.0.0.7:microsoft-ds   SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49687 -> 10.0.0.7:microsoft-ds   SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Reconnect   DESKTOP-AK2UAT3.localdomain:49688 -> 10.0.0.8:microsoft-ds   SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49688 -> 10.0.0.8:microsoft-ds   SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Reconnect   DESKTOP-AK2UAT3.localdomain:49689 -> 10.0.0.9:microsoft-ds   SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49689 -> 10.0.0.9:microsoft-ds   SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49690 -> 10.0.0.10:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Reconnect   DESKTOP-AK2UAT3.localdomain:49691 -> 10.0.0.11:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49691 -> 10.0.0.11:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Reconnect   DESKTOP-AK2UAT3.localdomain:49692 -> 10.0.0.12:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49692 -> 10.0.0.12:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Reconnect   DESKTOP-AK2UAT3.localdomain:49694 -> 10.0.0.13:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49694 -> 10.0.0.13:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49695 -> 10.0.0.14:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Reconnect   DESKTOP-AK2UAT3.localdomain:49696 -> 10.0.0.15:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49696 -> 10.0.0.15:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Reconnect   DESKTOP-AK2UAT3.localdomain:49697 -> 10.0.0.16:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49697 -> 10.0.0.16:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Reconnect   DESKTOP-AK2UAT3.localdomain:49698 -> 10.0.0.17:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49698 -> 10.0.0.17:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Reconnect   DESKTOP-AK2UAT3.localdomain:49699 -> 10.0.0.18:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49699 -> 10.0.0.18:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Reconnect   DESKTOP-AK2UAT3.localdomain:49700 -> 10.0.0.19:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49700 -> 10.0.0.19:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49701 -> 10.0.0.20:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Reconnect   DESKTOP-AK2UAT3.localdomain:49702 -> 10.0.0.21:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49702 -> 10.0.0.21:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Reconnect   DESKTOP-AK2UAT3.localdomain:49703 -> 10.0.0.22:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49703 -> 10.0.0.22:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Reconnect   DESKTOP-AK2UAT3.localdomain:49705 -> 10.0.0.23:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49705 -> 10.0.0.23:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49706 -> 10.0.0.24:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Reconnect   DESKTOP-AK2UAT3.localdomain:49708 -> 10.0.0.25:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49708 -> 10.0.0.25:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49709 -> 10.0.0.26:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Reconnect   DESKTOP-AK2UAT3.localdomain:49710 -> 10.0.0.27:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49710 -> 10.0.0.27:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Reconnect   DESKTOP-AK2UAT3.localdomain:49711 -> 10.0.0.28:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49711 -> 10.0.0.28:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Reconnect   DESKTOP-AK2UAT3.localdomain:49712 -> 10.0.0.29:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49712 -> 10.0.0.29:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49713 -> 10.0.0.30:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49714 -> 10.0.0.31:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Reconnect   DESKTOP-AK2UAT3.localdomain:49715 -> 10.0.0.32:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49715 -> 10.0.0.32:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Reconnect   DESKTOP-AK2UAT3.localdomain:49716 -> 10.0.0.33:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49716 -> 10.0.0.33:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Reconnect   DESKTOP-AK2UAT3.localdomain:49718 -> 10.0.0.34:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49718 -> 10.0.0.34:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49719 -> 10.0.0.35:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Reconnect   DESKTOP-AK2UAT3.localdomain:49720 -> 10.0.0.36:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49720 -> 10.0.0.36:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Reconnect   DESKTOP-AK2UAT3.localdomain:49722 -> 10.0.0.37:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49722 -> 10.0.0.37:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Reconnect   DESKTOP-AK2UAT3.localdomain:49723 -> 10.0.0.38:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49723 -> 10.0.0.38:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49724 -> 10.0.0.39:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Reconnect   DESKTOP-AK2UAT3.localdomain:49725 -> 10.0.0.40:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49725 -> 10.0.0.40:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Reconnect   DESKTOP-AK2UAT3.localdomain:49726 -> 10.0.0.41:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49726 -> 10.0.0.41:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Reconnect   DESKTOP-AK2UAT3.localdomain:49727 -> 10.0.0.42:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Disconnect  DESKTOP-AK2UAT3.localdomain:49727 -> 10.0.0.42:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
12:0...  wannacry.exe  6232  TCP Reconnect   DESKTOP-AK2UAT3.localdomain:49728 -> 10.0.0.43:microsoft-ds  SUCCESS  Length: 0, seqnum: 0, connid: 0
```

trying to infected the whole network using SMB protocol

Figure 22 – SMB Connections by Procmon

During the review of the process tree to check the parent process and its subsequent child processes to gather more insights into the capabilities of this malware, I've observed the following:



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	Command	Start Time
vm3dservice.exe (2784)	VMware SVGA H...	C:\Windows\syst...		VMware, Inc.	NT AUTHORITY\...	vm3dservice.exe -n	05/03/2024
vmtoolsd.exe (2476)	VMware Tools Cor...	C:\Program Files\...		VMware, Inc.	NT AUTHORITY\...	"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"	05/03/2024
svchost.exe (2564)	Host Process for ...	C:\Windows\Syst...		Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\System32\svchost.exe -k netsvcs	05/03/2024
dllhost.exe (3428)	COM Surrogate	C:\Windows\syst...		Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\system32\dllhost.exe /Processid:{02D4B3F1-FD88-11D1-960D-00805FC79235}	05/03/2024
SearchIndexer.exe (3484)	Microsoft Window...	C:\Windows\syst...		Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\system32\SearchIndexer.exe /Embedding	05/03/2024
SearchProtocolHost.exe	Microsoft Window...	C:\Windows\syst...		Microsoft Corporat...	NT AUTHORITY\...	"C:\Windows\system32\SearchProtocolHost.exe" Global\UsGthrFltPipeMssGthrPipe2_ Global\UsGthrCtrlFltPipeMssGthr...	09/03/2024
SearchFilterHost.exe (32	Microsoft Window...	C:\Windows\syst...		Microsoft Corporat...	NT AUTHORITY\...	"C:\Windows\system32\SearchFilterHost.exe" 0 828 832 840 8192 836 812	09/03/2024
SearchFilterHost.exe (20	Microsoft Window...	C:\Windows\syst...		Microsoft Corporat...	NT AUTHORITY\...	"C:\Windows\system32\SearchFilterHost.exe" 0 828 832 840 8192 836 812	09/03/2024
svchost.exe (3508)	Host Process for ...	C:\Windows\syst...		Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\system32\svchost.exe -k wsappx -p	05/03/2024
msdtc.exe (3924)	Microsoft Distribut...	C:\Windows\Syst...		Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\System32\msdtc.exe	05/03/2024
svchost.exe (2044)	Host Process for ...	C:\Windows\syst...		Microsoft Corporat...	DESKTOP-AK2U...	C:\Windows\system32\svchost.exe -k UnistackSvcGroup	05/03/2024
svchost.exe (4732)	Host Process for ...	C:\Windows\Syst...		Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted	05/03/2024
svchost.exe (3360)	Host Process for ...	C:\Windows\syst...		Microsoft Corporat...	DESKTOP-AK2U...	C:\Windows\system32\svchost.exe -k ClipboardSvcGroup -p	05/03/2024
svchost.exe (7040)	Host Process for ...	C:\Windows\syst...		Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation -p	05/03/2024
SgrmBroker.exe (1552)	System Guard Ru...	C:\Windows\syst...		Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\system32\SgrmBroker.exe	05/03/2024
svchost.exe (4748)	Host Process for ...	C:\Windows\syst...		Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\system32\svchost.exe -k LocalService	05/03/2024
svchost.exe (2524)	Host Process for ...	C:\Windows\Syst...		Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p	05/03/2024
SecurityHealthService.exe (	Windows Security...	C:\Windows\syst...		Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\system32\SecurityHealthService.exe	05/03/2024
Upfc.exe (4008)	Updateability From...	C:\Windows\Syst...		Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\System32\Upfc.exe /launchtype periodic /cv 9VSbX13940KKE//3eFhcfw.0	09/03/2024
sihclient.exe (3204)	SIH Client	C:\Windows\Syst...		Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\System32\sihclient.exe /cv 9VSbX13940KKE//3eFhcfw.0.2	09/03/2024
svchost.exe (5084)	Host Process for ...	C:\Windows\Syst...		Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\System32\svchost.exe -k netsvcs -p	09/03/2024
wannacry.exe (5980)	Microsoft® Disk D...	C:\Users\DoronP...		Microsoft Corporat...	NT AUTHORITY\...	C:\Users\DoronP\Desktop\wannacry.exe -m security	09/03/2024
cmd.exe (5600)	Windows Comma...	C:\Windows\syst...		Microsoft Corporat...	NT AUTHORITY\...	cmd.exe /c "C:\ProgramData\gzfhbohbqt094\tasksche.exe"	09/03/2024
tasksche.exe (5556)	DiskPart	C:\ProgramData\...		Microsoft Corporat...	NT AUTHORITY\...	C:\ProgramData\gzfhbohbqt094\tasksche.exe	09/03/2024
attrib.exe (3104)	Attribute Utility	C:\Windows\Sys...		Microsoft Corporat...	NT AUTHORITY\...	attrib +h .	09/03/2024
Conhost.exe (686	Console Window ...	C:\Windows\Syst...		Microsoft Corporat...	NT AUTHORITY\...	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1	09/03/2024
icacls.exe (4112)		C:\Windows\Sys...		Microsoft Corporat...	NT AUTHORITY\...	icacls . /grant Everyone:F /T /C /Q	09/03/2024
Conhost.exe (181	Console Window ...	C:\Windows\Syst...		Microsoft Corporat...	NT AUTHORITY\...	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1	09/03/2024
taskdl.exe (6212)	SQL Client Config...	C:\ProgramData\...		Microsoft Corporat...	NT AUTHORITY\...	taskdl.exe	09/03/2024
cmd.exe (4784)	Windows Comma...	C:\Windows\Sys...		Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\system32\cmd.exe /c 311251709976202.bat	09/03/2024
Conhost.exe (624	Console Window ...	C:\Windows\Syst...		Microsoft Corporat...	NT AUTHORITY\...	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1	09/03/2024
cscript.exe (4632)	Microsoft ® Conso...	C:\Windows\Sys...		Microsoft Corporat...	NT AUTHORITY\...	cscript.exe //nologo m.vbs	09/03/2024
taskdl.exe (5268)	SQL Client Config...	C:\ProgramData\...		Microsoft Corporat...	NT AUTHORITY\...	taskdl.exe	09/03/2024
taskdl.exe (3208)	SQL Client Config...	C:\ProgramData\...		Microsoft Corporat...	NT AUTHORITY\...	taskdl.exe	09/03/2024
taskdl.exe (6696)	SQL Client Config...	C:\ProgramData\...		Microsoft Corporat...	NT AUTHORITY\...	taskdl.exe	09/03/2024
taskdl.exe (2296)	SQL Client Config...	C:\ProgramData\...		Microsoft Corporat...	NT AUTHORITY\...	taskdl.exe	09/03/2024
@WanaDecryptor@.	Load PerfMon Co...	C:\ProgramData\...		Microsoft Corporat...	NT AUTHORITY\...	@WanaDecryptor@.exe co	09/03/2024
taskhsvc.exe (60		C:\ProgramData\...			NT AUTHORITY\...	TaskData\Tor\taskhsvc.exe	09/03/2024
Conhost.exe (	Console Window ...	C:\Windows\Syst...		Microsoft Corporat...	NT AUTHORITY\...	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1	09/03/2024
cmd.exe (1840)	Windows Comma...	C:\Windows\Sys...		Microsoft Corporat...	NT AUTHORITY\...	cmd.exe /c start /b @WanaDecryptor@.exe vs	09/03/2024
Conhost.exe (524	Console Window ...	C:\Windows\Syst...		Microsoft Corporat...	NT AUTHORITY\...	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1	09/03/2024
@WanaDecrypto	Load PerfMon Co...	C:\ProgramData\...		Microsoft Corporat...	NT AUTHORITY\...	@WanaDecryptor@.exe vs	09/03/2024
cmd.exe (594	Windows Comma...	C:\Windows\Sys...		Microsoft Corporat...	NT AUTHORITY\...	cmd.exe /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy igno...	09/03/2024
Conhost.ex	Console Window ...	C:\Windows\Syst...		Microsoft Corporat...	NT AUTHORITY\...	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1	09/03/2024
WMIC.exe	WMI Commandlin...	C:\Windows\Sys...		Microsoft Corporat...	NT AUTHORITY\...	wmic shadowcopy delete	09/03/2024
taskse.exe (3424)	waitfor - wait/send...	C:\ProgramData\...		Microsoft Corporat...	NT AUTHORITY\...	taskse.exe C:\ProgramData\gzfhbohbqt094\@WanaDecryptor@.exe	09/03/2024
@WanaDecrypto	Load PerfMon Co...	C:\ProgramData\...		Microsoft Corporat...	DESKTOP-AK2U...	"C:\ProgramData\gzfhbohbqt094\@WanaDecryptor@.exe"	09/03/2024
cmd.exe (1820)	Windows Comma...	C:\Windows\Sys...		Microsoft Corporat...	NT AUTHORITY\...	cmd.exe /c reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "gzfhbohbqt094" /t REG_SZ /d "\...	09/03/2024
Conhost.exe (647	Console Window ...	C:\Windows\Syst...		Microsoft Corporat...	NT AUTHORITY\...	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1	09/03/2024
reg.exe (1508)	Registry Console ...	C:\Windows\Sys...		Microsoft Corporat...	NT AUTHORITY\...	reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "gzfhbohbqt094" /t REG_SZ /d "\"C:\Progra...	09/03/2024
taskdl.exe (2236)	SQL Client Config...	C:\ProgramData\...		Microsoft Corporat...	NT AUTHORITY\...	taskdl.exe	09/03/2024

Figure 23 – Process Tree

Below is the explanation of these processes and what they are exactly doing:

- **cmd.exe /c "C:\ProgramData\gzfhbohbqt094\tasksche.exe" C:\Windows\SysWOW64\attrib.exe attrib +h .**
    - Tasksche.exe was initiated after wannacry.exe's detonation which then set the directory it was initiated from to hidden using attrib.exe.

- **C:\Windows\SysWOW64\icacls.exe icacls . /grant Everyone:F /T /C /Q**
  - → tasksche.exe used icacls.exe (ACLs - Access Control Lists) to perform the following on the current directory (gzfhbohbqt094):
    - – "/grant Everyone:F": This part of the command grants full control (F) permissions to the "Everyone" group. This essentially allows all users, including guests and unauthenticated users, full control over the directory and its contents.
    - – "/T": This switch applies the specified permission changes to all subdirectories and files within the specified directory recursively.
    - – "/C": This switch continues the operation even if errors occur during processing.
    - – "/Q": This switch suppresses the display of success messages.

- **C:\Windows\SysWOW64\cmd.exe C:\Windows\system32\cmd.exe /c 311251709976202.bat**
  - → taskdl.exe executes a batch file named "311251709976202.bat" using command interpreter.
  - → "/c" flag tells cmd.exe to execute the command specified and then terminate.

- **cscript.exe //nologo m.vbs**
  - → Runs a VBScript file named "m.vbs" without displaying the Windows Script Host logo.
  - → "//nologo" is an argument used to suppress the Windows Script Host logo during script execution.

- **C:\ProgramData\gzfhbohbqt094\TaskData\Tor\taskhsvc.exe TaskData\Tor\taskhsvc.exe**
  - → taskhsvc.exe is executed which then opens port 9050 to a LISTENING state (screenshot above) and attempts to connect to non-private remote addresses over HTTPS.

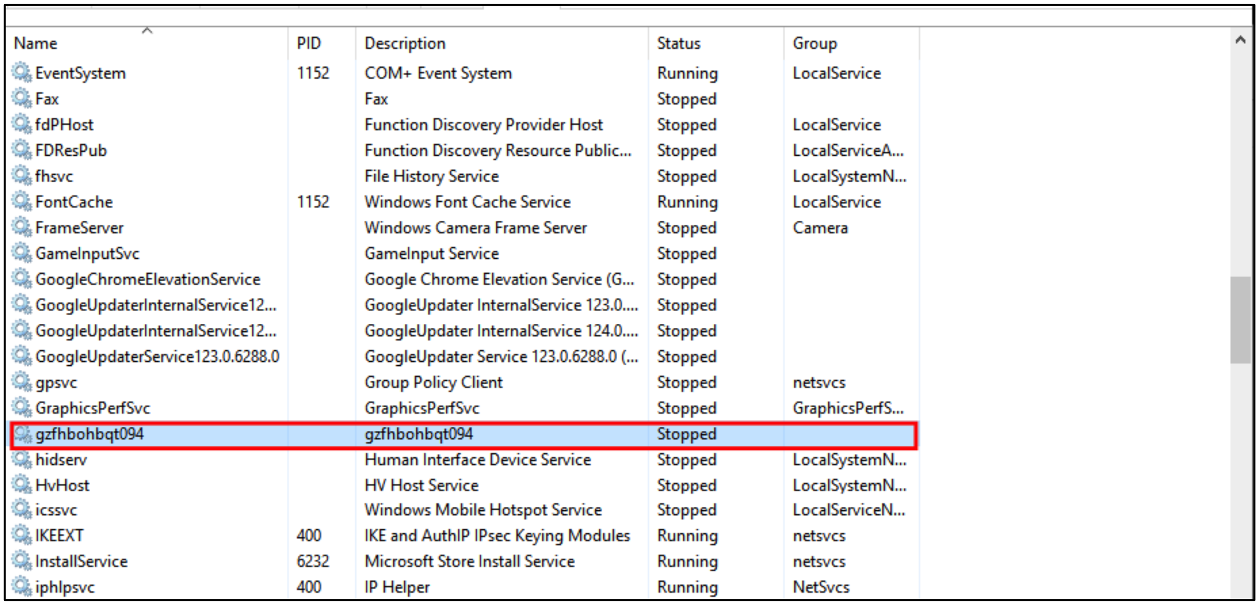
- **cmd.exe /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no & wbadmin delete catalog -quiet**
  - → vssadmin delete shadows /all /quiet: Deletes all Volume Shadow Copies quietly.
  - → wmic shadowcopy delete: Deletes all remaining shadow copies using Windows Management Instrumentation Command-line (WMIC).
  - → bcdedit /set {default} bootstatuspolicy ignoreallfailures: Sets the boot status policy to ignore all failures.
  - → bcdedit /set {default} recoveryenabled no: Disables recovery options for the default boot entry.
  - → wbadmin delete catalog -quiet: Deletes the backup catalog quietly.

  This command sequence is designed to remove or tamper with system backup and recovery mechanisms, possibly to cover tracks or hinder recovery efforts.

- **cmd.exe /c reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "gzfhbohbqt094" /t REG_SZ /d "\"C:\ProgramData\gzfhbohbqt094\tasksche.exe\"" /f**
  - → cmd.exe /c: Initiates a command shell and executes the specified command before terminating.
  - → reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run: Adds a new entry under the "Run" registry key, which specifies programs that should run automatically when the system starts.
  - → /v "gzfhbohbqt094": Specifies the name of the registry value to be created.
  - → /t REG_SZ: Specifies the data type of the registry value as a string (REG_SZ).
  - → /d "\"C:\ProgramData\gzfhbohbqt094\tasksche.exe\"": Specifies the data to be stored in the registry value, which is the path to an executable file ("C:\ProgramData\gzfhbohbqt094\tasksche.exe"). The double quotes around the path are escaped with backslashes.
  - → /f: Forces the creation of the registry entry without prompting for confirmation.

  This command is likely attempting to add a new entry to the Windows registry to ensure that a specific executable (tasksche.exe) is executed every time the system starts (Persistence Mechanism).
  The executable path indicates that it resides in the C:\ProgramData\gzfhbohbqt094\ directory.

We can also see the persistence mechanism while reviewing the service manager within the OS and the new service that was created “gzfhbohbqt094” which will load whenever the system boots up.



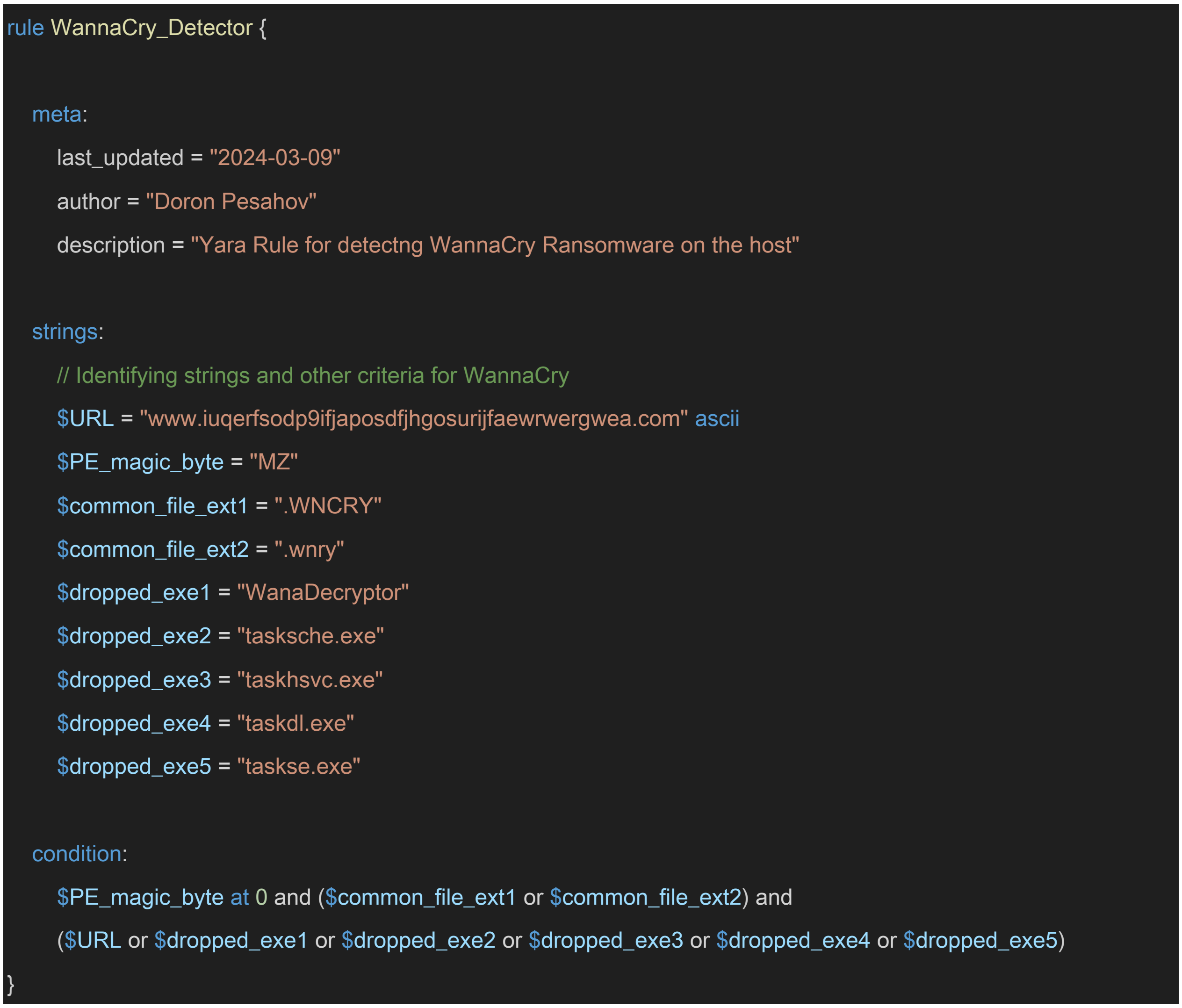
Name	PID	Description	Status	Group
EventSystem	1152	COM+ Event System	Running	LocalService
Fax		Fax	Stopped	
fdPHost		Function Discovery Provider Host	Stopped	LocalService
FDResPub		Function Discovery Resource Public...	Stopped	LocalServiceA...
fhsvc		File History Service	Stopped	LocalSystemN...
FontCache	1152	Windows Font Cache Service	Running	LocalService
FrameServer		Windows Camera Frame Server	Stopped	Camera
GameInputSvc		GameInput Service	Stopped	
GoogleChromeElevationService		Google Chrome Elevation Service (G...	Stopped	
GoogleUpdaterInternalService12...		GoogleUpdater InternalService 123.0....	Stopped	
GoogleUpdaterInternalService12...		GoogleUpdater InternalService 124.0....	Stopped	
GoogleUpdaterService123.0.6288.0		GoogleUpdater Service 123.0.6288.0 (...	Stopped	
gpsvc		Group Policy Client	Stopped	netsvcs
GraphicsPerfSvc		GraphicsPerfSvc	Stopped	GraphicsPerfS...
gzfhbohbqt094		gzfhbohbqt094	Stopped	
hidserv		Human Interface Device Service	Stopped	LocalSystemN...
HvHost		HV Host Service	Stopped	LocalSystemN...
icssvc		Windows Mobile Hotspot Service	Stopped	LocalServiceN...
IKEEXT	400	IKE and AuthIP IPsec Keying Modules	Running	netsvcs
InstallService	6232	Microsoft Store Install Service	Running	netsvcs
iphlpsvc	400	IP Helper	Running	NetSvcs

Figure 24 – New Service Indicating Persistency

List of Indicators of Compromise (IOCs)

Domain	hxxp://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
Strings	WNcry@2o17
	tasksche.exe
	taskse.exed
	taskdl.exe
	C:\%s\%s
	C:\%s\qeriuwjhrf
	\172.16.99.5\IPC$
	\192.168.56.20\IPC$
	icacls . /grant Everyone:F /T /C /Q
	.wncry
	.wnry
Hashes	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
	4a468603fdcb7a2eb5770705898cf9ef37aade532a7964642ecd705a74794b79
	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
	2ca2d550e603d74dedda03156023135b38da3630cb014e3d00b1263358c5f00d
	E48673680746FBE027E8982F62A83C298D6FB46AD9243DE8E79B7E5A24DCD4EB
	B9C5D4339809E0AD9A00D4D3DD26FDF44A32819A54ABF846BB9B560D81391C25

Yara Rules



```
rule WannaCry_Detector {

  meta:
    last_updated = "2024-03-09"
    author = "Doron Pesahov"
    description = "Yara Rule for detectng WannaCry Ransomware on the host"

  strings:
    // Identifying strings and other criteria for WannaCry
    $URL = "www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com" ascii
    $PE_magic_byte = "MZ"
    $common_file_ext1 = ".WNCRY"
    $common_file_ext2 = ".wnry"
    $dropped_exe1 = "WanaDecryptor"
    $dropped_exe2 = "tasksche.exe"
    $dropped_exe3 = "taskhsvc.exe"
    $dropped_exe4 = "taskdl.exe"
    $dropped_exe5 = "taskse.exe"

  condition:
    $PE_magic_byte at 0 and ($common_file_ext1 or $common_file_ext2) and
    ($URL or $dropped_exe1 or $dropped_exe2 or $dropped_exe3 or $dropped_exe4 or $dropped_exe5)
}
```