# Malware Analysis Report

## WannaCry Ransomware

Dec 2023 | UnShad0wer | v1.0

# Table of Contents

# Executive Summary

| | |
|---|---|
| SHA256 hash | 24D004A104D4D54034DBCFFC2A4B19A11F39008A575AA614EA04703480B1022C |

WannaCry is a Ransomware sample first identified on May 12th, 2017. It is written in C++ Programing language that runs on Windows OS. The indicators of this worm are by encrypting the files on the targeted machine and changing the wallpaper after its successful launch. To decrypt the files, the victim must pay $300 in bitcoin, and it also leaves a note in order to guide the victim for payment process.

Additionally, this ransomware has worm capabilities trying to spread on the victim's network, and it has persistence mechanism.

This Ransomware includes a kill switch technique, which is a specific URL once the connection was succeed the malware won't execute and exits permanently, otherwise it will run its malicious payload.

YARA signature rules are attached in Appendix A.

# High-Level Technical Summary

WannaCry is a 32-bit executable file, and it requires administrative privilege to execute its malicious payload.

Once the malware executed it establishes a connection to the URL “**hxxp://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com**”, if the connection succeeds the malware will not execute its malicious payload, this is appearing to be the malware kill switch.

Otherwise, the malware will begin to execute its malicious payload and start encrypting the files, and it unpacks additional executables.

Right after its success execute, the files encrypted and “.wnry” extension added to the end of files, also the desktop wallpaper changes to an image to inform the victim what happened and guides the victim to follow the instructions in order to recover his/her files. It also installs a Decryptor program with GUI interface.

The malware has a worm capability that can be spread itself in the network through an SMB share and initiates network connection on port 445.

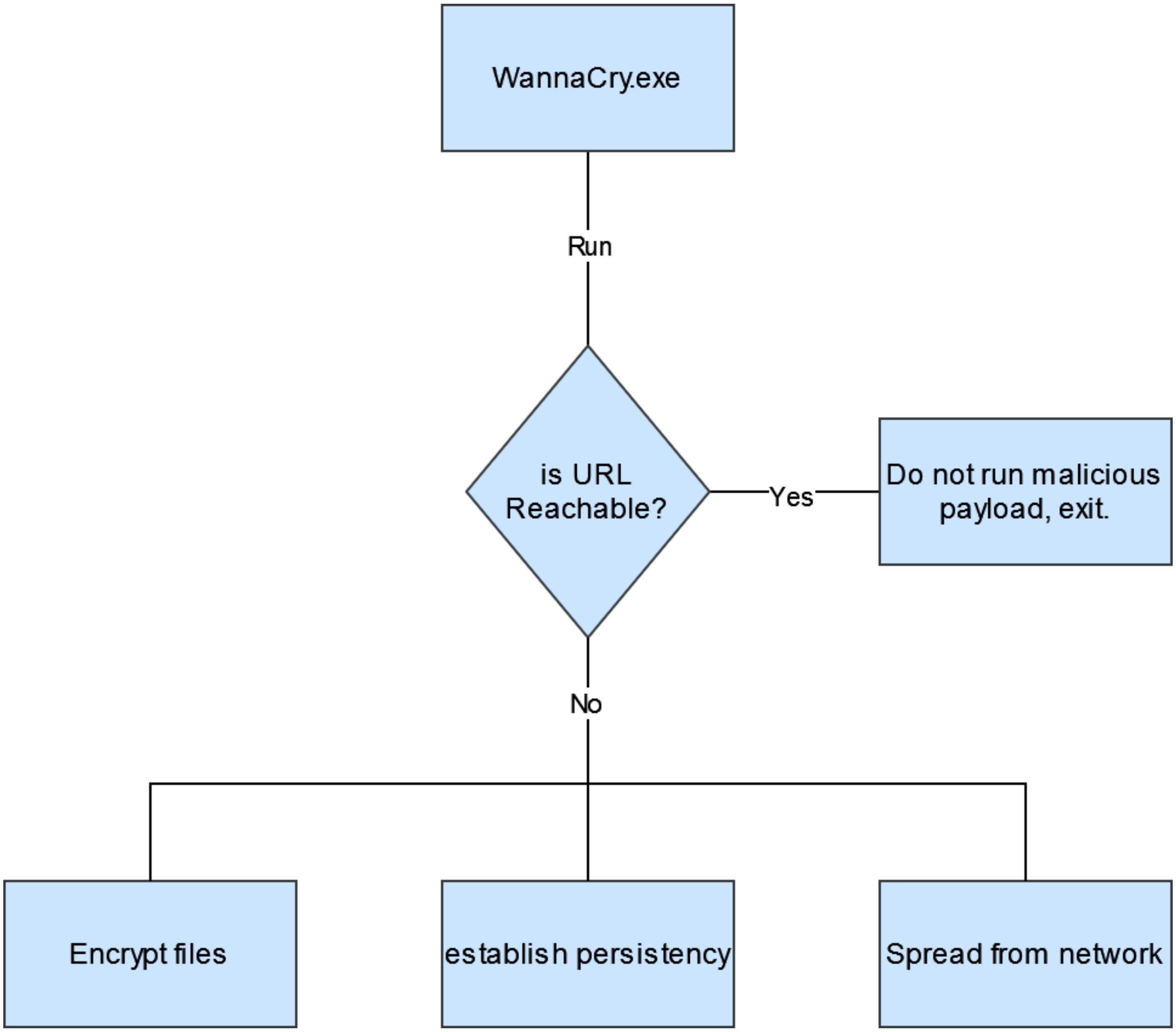


*Figure 1 execution diagram*

# Malware Composition

WannaCry.exe creates a hidden directory and it contains five executable files, perhaps this is the staging area of the WannaCry Ransomware.

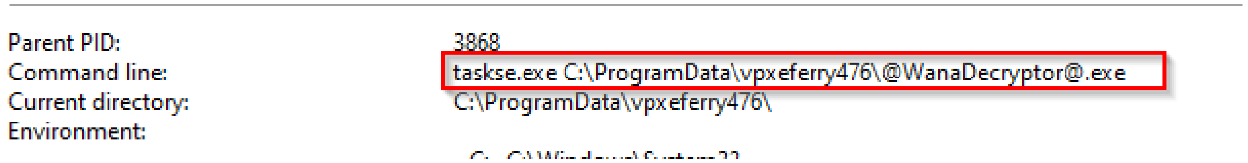
| File Name | SHA256 Hash |
|---|---|
| **tasksche.exe** | ED01EBFBC9EB5BBEA545AF4D01BF5F1071661840480439C6E5BABE8E080E41AA |
| **taskdl.exe** | 4A468603FDCB7A2EB5770705898CF9EF37AADE532A7964642ECD705A74794B79 |
| **taskse.exe** | 2CA2D550E603D74DEDDA03156023135B38DA3630CB014E3D00B1263358C5F00D |
| **taskhsvc.exe** | E48673680746FBE027E8982F62A83C298D6FB46AD9243DE8E79B7E5A24DCD4EB |
| **@WanaDecryptor@.exe** | B9C5D4339809E0AD9A00D4D3DD26FDF44A32819A54ABF846BB9B560D81391C25 |

## tasksche.exe

this executable is in C:\ProgramData\vpxefrry476, this file is initial run file after succeeding of wannacry.exe run, and this executable will handle other executable files added to the table above.

## taskse.exe:

This executable appears to be a scheduler for running WannaDecryptor.exe, it will execute WannaDecryptor.exe continuously every 10-20 seconds.



```
Parent PID:          3868
Command line:        taskse.exe C:\ProgramData\vpxeferry476\@WanaDecryptor@.exe
Current directory:   C:\ProgramData\vpxeferry476\
Environment:
```

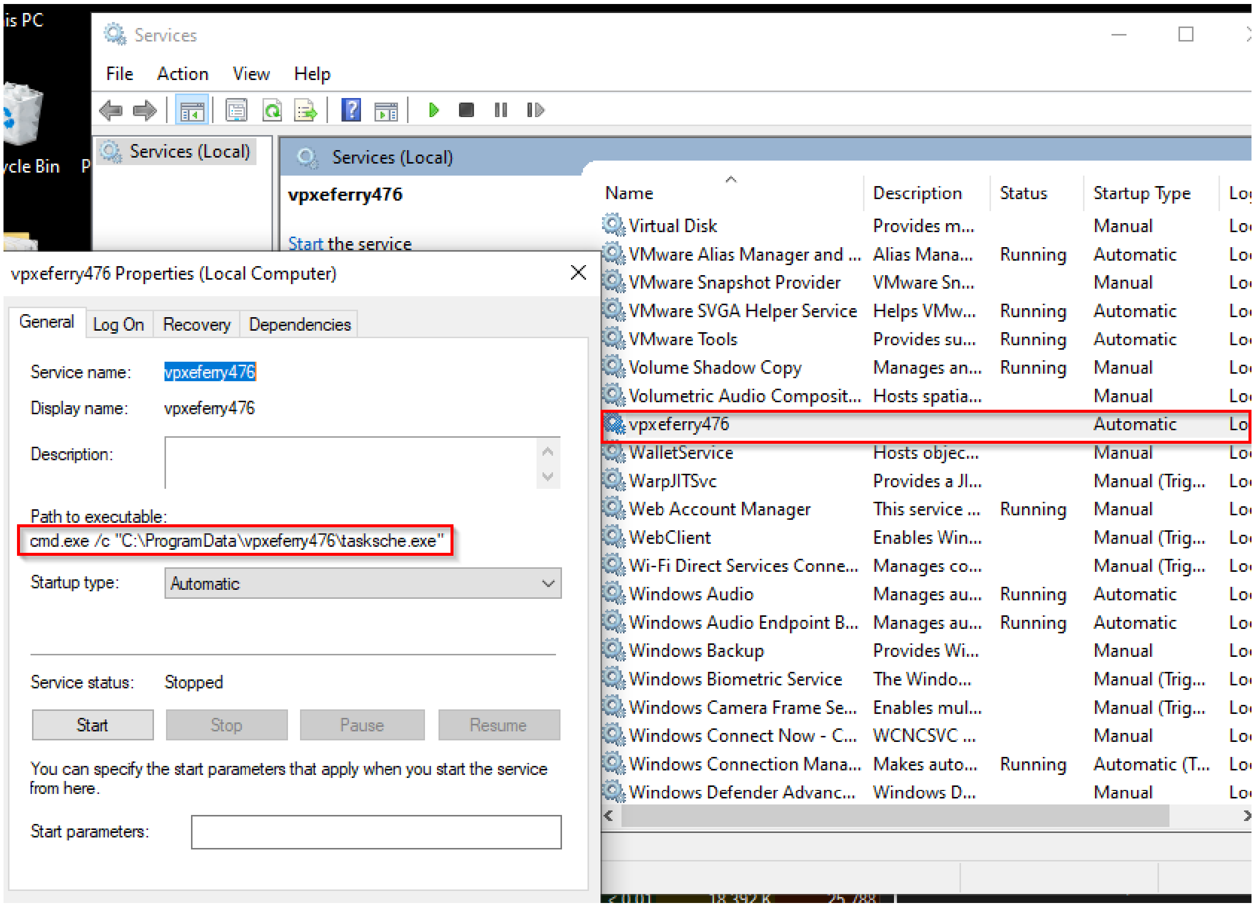
*Figure 2 command to run WanaDecryptor*

## taskse.exe:

this executable will store and deletes WannaCry.exe logs in C:\Windows\Temp and the files ends with ".WNCRYT" extension.

## taskhsvc.exe:

This executable will create a service to stay persistent of the ransomware after rebooting the system and detecting USB while attached to the computer, then propagate.



Service name: vpxeferry476

Display name: vpxeferry476

Description:

Path to executable:
cmd.exe /c "C:\ProgramData\vpxeferry476\tasksche.exe"

Startup type: Automatic

Service status: Stopped

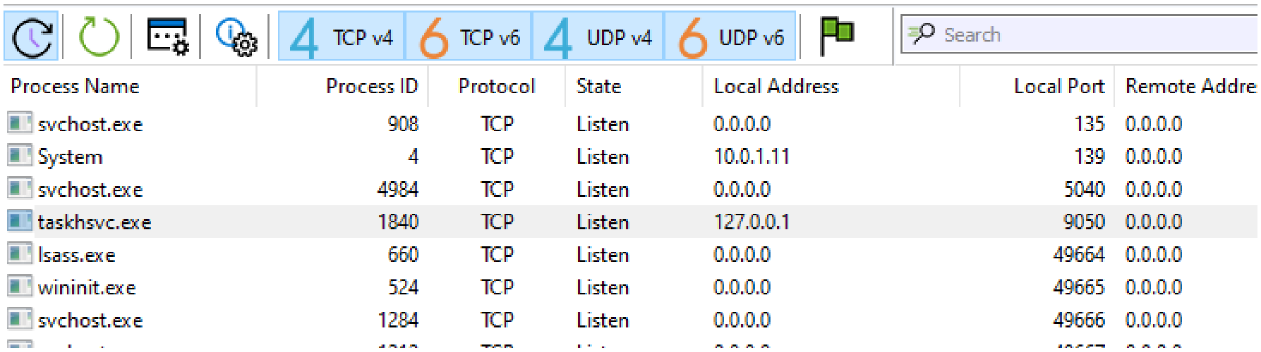
You can specify the start parameters that apply when you start the service from here.

Start parameters:

| Name | Description | Status | Startup Type | Lo |
|---|---|---|---|---|
| Virtual Disk | Provides m... | | Manual | Lo |
| VMware Alias Manager and ... | Alias Mana... | Running | Automatic | Lo |
| VMware Snapshot Provider | VMware Sn... | | Manual | Lo |
| VMware SVGA Helper Service | Helps VMw... | Running | Automatic | Lo |
| VMware Tools | Provides su... | Running | Automatic | Lo |
| Volume Shadow Copy | Manages an... | Running | Manual | Lo |
| Volumetric Audio Composit... | Hosts spatia... | | Manual | Lo |
| vpxeferry476 | | | Automatic | Lo |
| WalletService | Hosts objec... | | Manual | Lo |
| WarpJITSvc | Provides a JI... | | Manual (Trig... | Lo |
| Web Account Manager | This service ... | Running | Manual | Lo |
| WebClient | Enables Win... | | Manual (Trig... | Lo |
| Wi-Fi Direct Services Conne... | Manages co... | | Manual (Trig... | Lo |
| Windows Audio | Manages au... | Running | Automatic | Lo |
| Windows Audio Endpoint B... | Manages au... | Running | Automatic | Lo |
| Windows Backup | Provides Wi... | | Manual | Lo |
| Windows Biometric Service | The Windo... | | Manual (Trig... | Lo |
| Windows Camera Frame Se... | Enables mul... | | Manual (Trig... | Lo |
| Windows Connect Now - C... | WCNCSVC ... | | Manual | Lo |
| Windows Connection Mana... | Makes auto... | Running | Automatic (T... | Lo |
| Windows Defender Advanc... | Windows D... | | Manual | Lo |

*Figure 3 command to run malicious service.*

Meanwhile this executable opens TCP/9050 port and listens on all interfaces with localhost address.



| Process Name | Process ID | Protocol | State | Local Address | Local Port | Remote Addre |
|---|---|---|---|---|---|---|
| svchost.exe | 908 | TCP | Listen | 0.0.0.0 | 135 | 0.0.0.0 |
| System | 4 | TCP | Listen | 10.0.1.11 | 139 | 0.0.0.0 |
| svchost.exe | 4984 | TCP | Listen | 0.0.0.0 | 5040 | 0.0.0.0 |
| taskhsvc.exe | 1840 | TCP | Listen | 127.0.0.1 | 9050 | 0.0.0.0 |
| lsass.exe | 660 | TCP | Listen | 0.0.0.0 | 49664 | 0.0.0.0 |
| wininit.exe | 524 | TCP | Listen | 0.0.0.0 | 49665 | 0.0.0.0 |
| svchost.exe | 1284 | TCP | Listen | 0.0.0.0 | 49666 | 0.0.0.0 |

*Figure 4 listen port*

## @WannaDecryptor@.exe:

This executable has a GUI and pops up in the middle of the screen after encryption process succeeded, the main purpose of this executable is for decrypting victim’s files after they have paid with bitcoin.

# Basic Static Analysis

In this phase information extracted without executing the sample, conducted with multiple tools (E.g. FIOSS, capa, PEStudio, PEView).

| | |
|---|---|
| CPU | 32-bit |
| Written Language | C++ |
| Original file name | lhdfrgui.exe |

Strings Extracted:

| Strings | Description |
|---|---|
| hxxp://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com | Kill switch URL |
| cmd.exe /c "%s" | A command with terminating the CMD window using /c |
| tasksche.exe<br>diskpart.exe | Another executable file |
| icacls . /grant Everyone:F /T /C /Q | A command to grant permission for the files, directories, and subdirectories to everyone |
| \\172.16.99.5\IPC$<br>\\192.168.56.20\IPC$ | A network path with a \IPC$ which is a window hidden administrative share folder |
| WanaCrypt0r | File name |
| C:\%s\qeriuwjhrf | A malicious file path |
| attrib +h . | A command that hides the current directory |

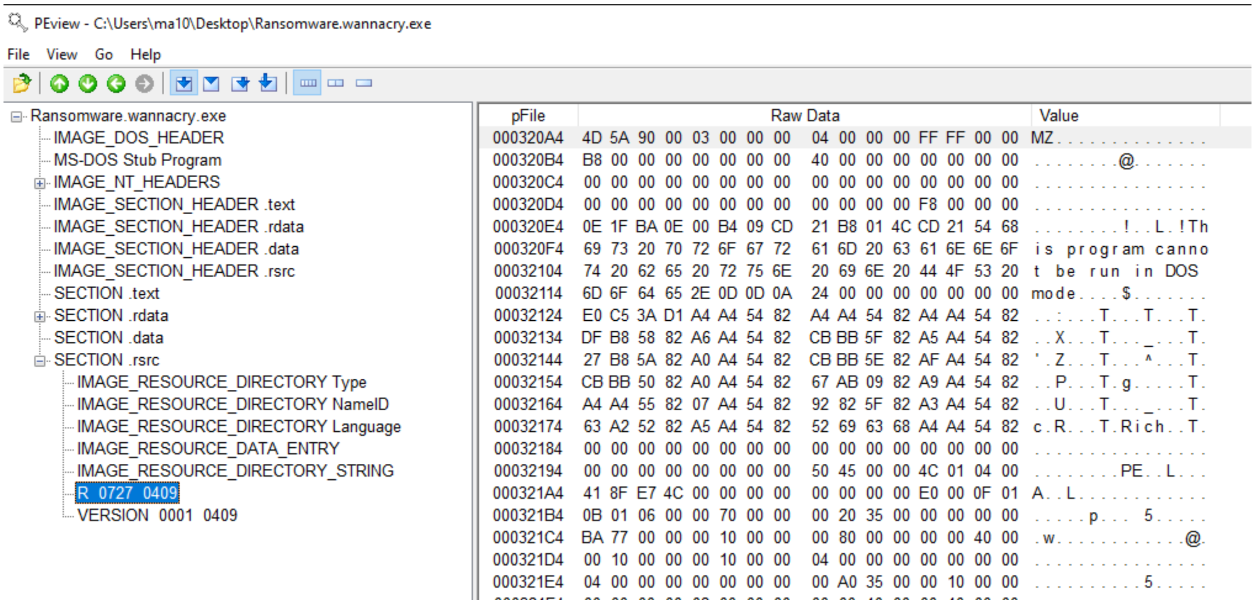
Windows API imports:

| Imports | Descriptions |
|---|---|
| 4 (connect) | The connect function establishes a connection to a specified socket. |
| 23 (socket) | The socket function creates a socket that is bound to a specific transport service provider. |
| 11 (inet_addr) | The inet_addr function converts a string containing an IPv4 dotted-decimal address into a proper address for the IN_ADDR structure. |
| GetAdaptersInfo | Used to obtain information about the network adapters on the system. This function is commonly used by malware for enumeration purposes. |
| InternetOpenA | Used to initialize the use of WinINet functions. |
| InternetOpenUrlA | Used to open a resource specified by a complete FTP or HTTP URL. |
| CryptGenRandom | Used to fill a buffer with cryptographically random bytes. |
| CryptAcquireContextA | Used to acquire a handle to a particular key container within a particular cryptographic service provider (CSP) |
| rand | Generates a pseudorandom number |
| Srand | Sets the starting seed value for the pseudorandom number generator used by the rand function. |
| 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. |
| MoveFileExA | Used to move an existing file or a directory, including its children. |

File types to encrypt:

.der .pfx .key .crt .csr .p12 .pem .odt .ott .sxw .stw .uot
.3ds .max .3dm .ods .ots .sxc .stc .dif .slk .wb2 .odp .otp
.sxd .std .uop .odg .otg .sxm .mml .lay .lay6 .asc .sqlite3
.sqlitedb .sql .accdb .mdb .dbf .odb .frm .myd .myi .ibd .mdf
.ldf .sln .suo .cpp .pas .asm .cmd .bat .ps1 .vbs .dip .dch
.sch .brd .jsp .php .asp .java .jar .class .mp3 .wav .swf .fla
.wmv .mpg .vob .mpeg .asf .avi .mov .mp4 .3gp .mkv .3g2 .flv
.wma .mid .m3u .m4u .djvu .svg .psd .nef .tiff .tif .cgm .raw
.gif .png .bmp .jpg .jpeg .vcd .iso .backup .zip .rar .tgz
.tar .bak .tbk .bz2 .PAQ .ARC .aes .gpg .vmx .vmdk .vdi .sldm
.sldx .sti .sxi 0.602 .hwp .snt .onetoc2 .dwg .pdf .wk1 .wks
0.123 .rtf .csv .txt .vsdx .vsd .edb .eml .msg .ost .pst .potm
.potx .ppam .ppsx .ppsm .pps .pot .pptm .pptx .ppt .xltm .xltx .xlc
.xlm .xlt .xlw .xlsb .xlsm .xlsx .xls .dotx .dotm .dot .docm .docb
.docx .doc

An executable can be found in ".rsrc" section from the PEview:



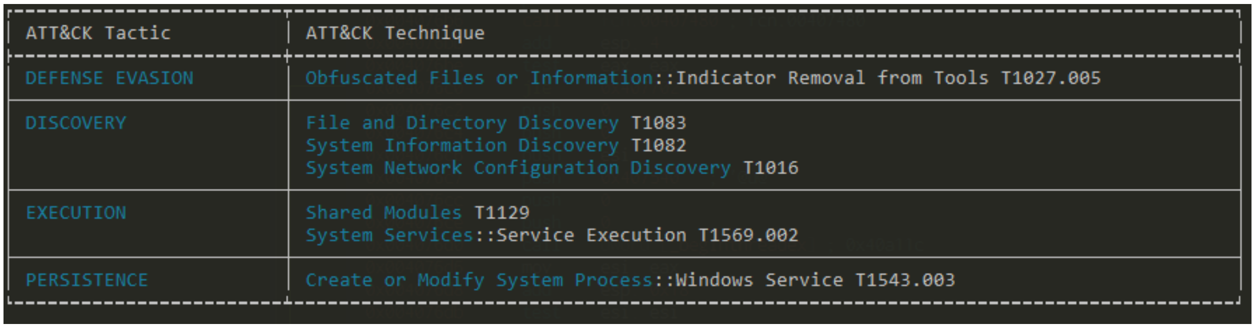
```
Ransomware.wannacry.exe
  IMAGE_DOS_HEADER
  MS-DOS Stub Program
  IMAGE_NT_HEADERS
  IMAGE_SECTION_HEADER .text
  IMAGE_SECTION_HEADER .rdata
  IMAGE_SECTION_HEADER .data
  IMAGE_SECTION_HEADER .rsrc
  SECTION .text
  SECTION .rdata
  SECTION .data
  SECTION .rsrc
    IMAGE_RESOURCE_DIRECTORY Type
    IMAGE_RESOURCE_DIRECTORY NameID
    IMAGE_RESOURCE_DIRECTORY Language
    IMAGE_RESOURCE_DATA_ENTRY
    IMAGE_RESOURCE_DIRECTORY_STRING
    R 0727 0409
    VERSION 0001 0409
```

```
pFile      Raw Data                                          Value
000320A4   4D 5A 90 00 03 00 00 00  04 00 00 00 FF FF 00 00  MZ..............
000320B4   B8 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00  ........@.......
000320C4   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000320D4   00 00 00 00 00 00 00 00  00 00 00 00 F8 00 00 00  ................
000320E4   0E 1F BA 0E 00 B4 09 CD  21 B8 01 4C CD 21 54 68  ........!..L.!Th
000320F4   69 73 20 70 72 6F 67 72  61 6D 20 63 61 6E 6E 6F  is program canno
00032104   74 20 62 65 20 72 75 6E  20 69 6E 20 44 4F 53 20  t be run in DOS 
00032114   6D 6F 64 65 2E 0D 0D 0A  24 00 00 00 00 00 00 00  mode....$.......
00032124   E0 C5 3A D1 A4 A4 54 82  A4 A4 54 82 A4 A4 54 82  ..:....T...T...T
00032134   DF B8 58 82 A6 A4 54 82  CB BB 5F 82 A5 A4 54 82  ..X....T..._...T
00032144   27 B8 5A 82 A0 A4 54 82  CB BB 5E 82 AF A4 54 82  '.Z....T..^....T
00032154   CB BB 50 82 A0 A4 54 82  67 AB 09 82 A9 A4 54 82  ..P....Tg......T
00032164   A4 A4 55 82 07 A4 54 82  92 82 5F 82 A3 A4 54 82  ..U....T.._....T
00032174   63 A2 52 82 A5 A4 54 82  52 69 63 68 A4 A4 54 82  c.R....TRich...T
00032184   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00032194   00 00 00 00 00 00 00 00  50 45 00 00 4C 01 04 00  ........PE..L...
000321A4   41 8F E7 4C 00 00 00 00  00 00 00 00 E0 00 0F 01  A..L............
000321B4   0B 01 06 00 00 70 00 00  00 20 35 00 00 00 00 00  .....p... 5.....
000321C4   BA 77 00 00 00 10 00 00  00 80 00 00 00 00 40 00  .w............@.
000321D4   00 10 00 00 00 10 00 00  04 00 00 00 00 00 00 00  ................
000321E4   04 00 00 00 00 00 00 00  00 A0 35 00 00 10 00 00  ..........5.....
```

*Figure 5 another file inside initial executable*

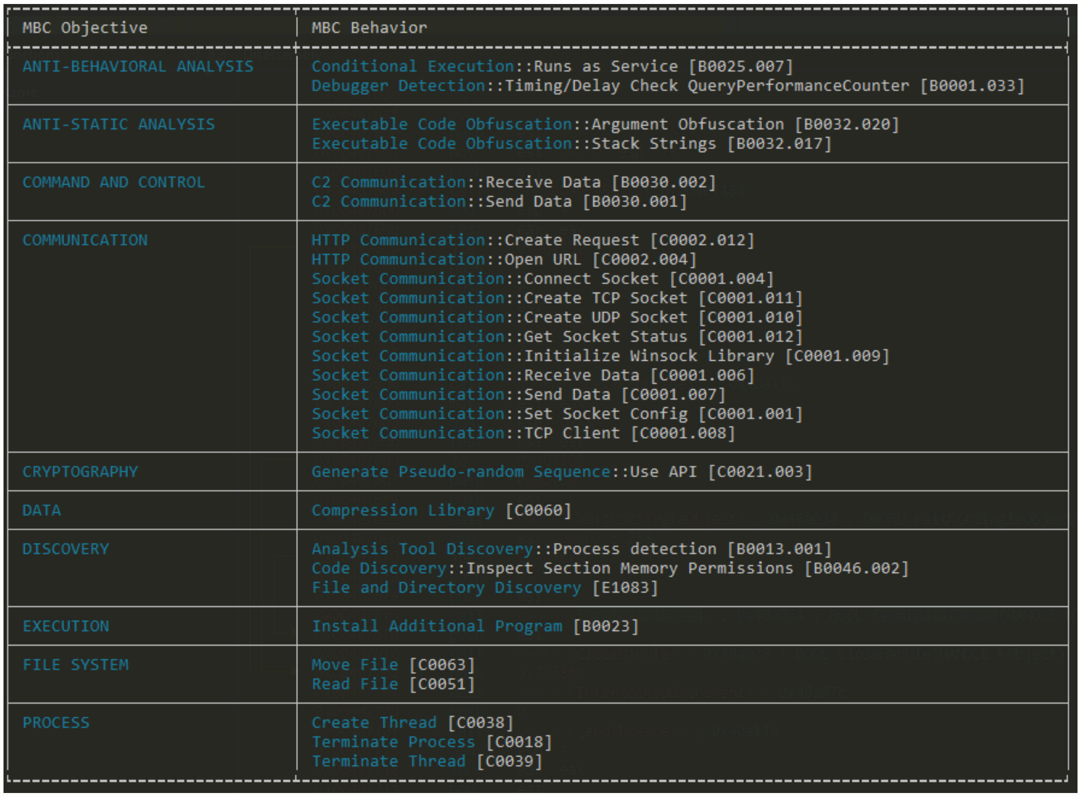
Capa results:

Capa is a program that detects malicious capabilities in suspicious programs by using a set of rules. These rules are meant to be as high-level and human-readable as possible.



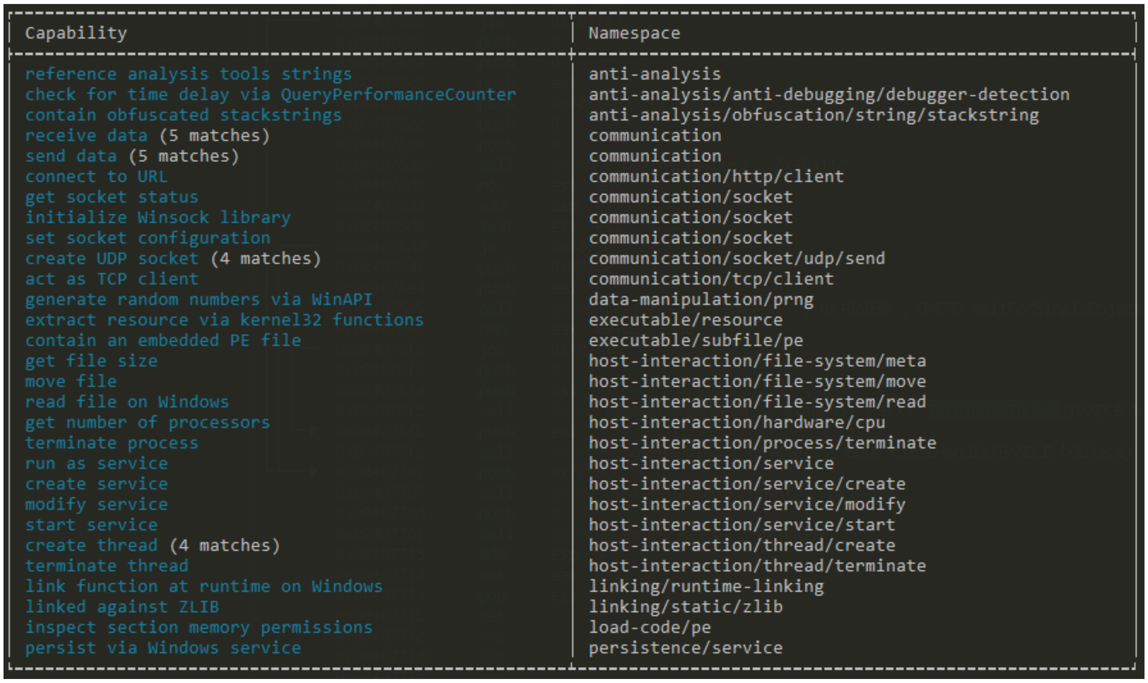
```
+------------------------+------------------------------------------------------------------------------------+
| ATT&CK Tactic          | ATT&CK Technique                                                                   |
|------------------------+------------------------------------------------------------------------------------|
| 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 6 CAPA ATT&CK Tactics*



```
+------------------------------+--------------------------------------------------------------------------+
| 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                    | Analysis Tool Discovery::Process detection [B0013.001]                   |
|                              | 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 7 CAPA MBC Objects*



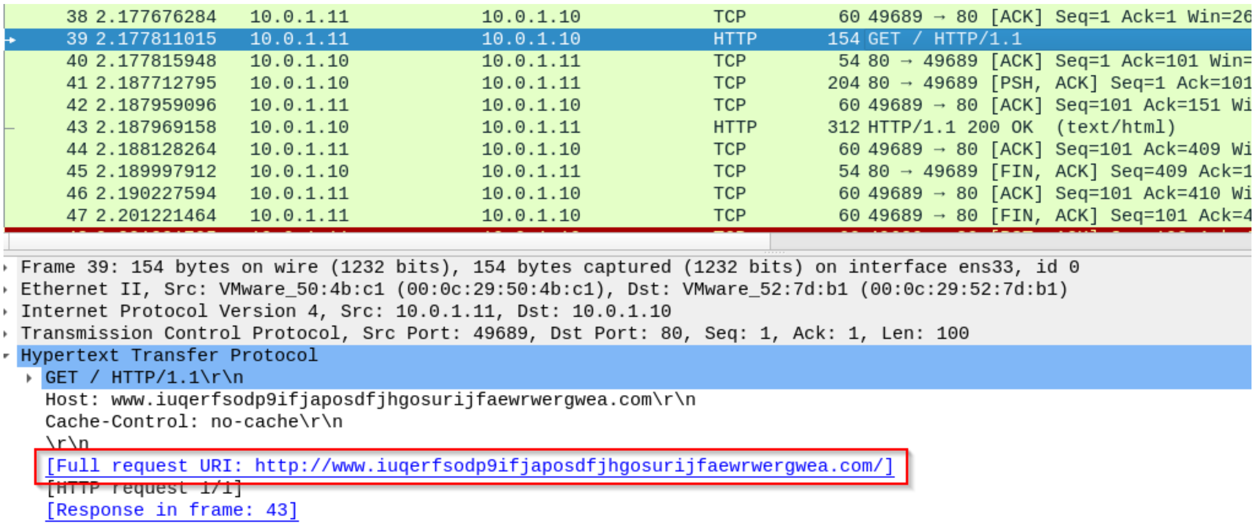
```
+------------------------------------------------------+-------------------------------------------------------+
| Capability                                           | Namespace                                             |
+------------------------------------------------------+-------------------------------------------------------+
| reference analysis tools strings                     | anti-analysis                                         |
| 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 8 CAPA capabilities*

# Basic Dynamic Analysis

In this phase information extracted while executing the malware, monitoring what the malware is doing including network activity, processes, registers, and other activities.

By simulating the internet utilizing inetsim, and capturing the network traffic utilizing Wireshark. while executing WannaCry, it will reach the malicious URL.

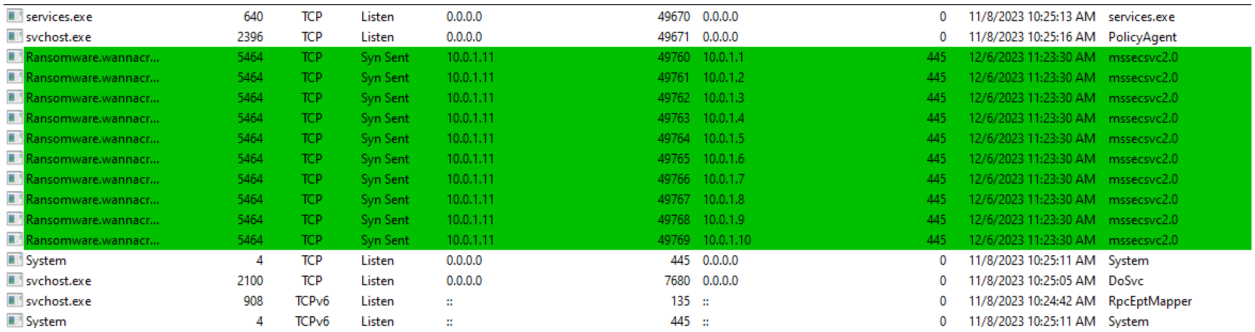


```
   38 2.177676284  10.0.1.11            10.0.1.10            TCP        60 49689 → 80 [ACK] Seq=1 Ack=1 Win=26
→  39 2.177811015  10.0.1.11            10.0.1.10            HTTP      154 GET / HTTP/1.1
   40 2.177815948  10.0.1.10            10.0.1.11            TCP        54 80 → 49689 [ACK] Seq=1 Ack=101 Win=
   41 2.187712795  10.0.1.10            10.0.1.11            TCP       204 80 → 49689 [PSH, ACK] Seq=1 Ack=101
   42 2.187959096  10.0.1.11            10.0.1.10            TCP        60 49689 → 80 [ACK] Seq=101 Ack=151 Wi
   43 2.187969158  10.0.1.10            10.0.1.11            HTTP      312 HTTP/1.1 200 OK  (text/html)
   44 2.188128264  10.0.1.11            10.0.1.10            TCP        60 49689 → 80 [ACK] Seq=101 Ack=409 Wi
   45 2.189997912  10.0.1.10            10.0.1.11            TCP        54 80 → 49689 [FIN, ACK] Seq=409 Ack=1
   46 2.190227594  10.0.1.11            10.0.1.10            TCP        60 49689 → 80 [ACK] Seq=101 Ack=410 Wi
   47 2.201221464  10.0.1.11            10.0.1.10            TCP        60 49689 → 80 [FIN, ACK] Seq=101 Ack=4

▸ Frame 39: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) on interface ens33, id 0
▸ Ethernet II, Src: VMware_50:4b:c1 (00:0c:29:50:4b:c1), Dst: VMware_52:7d:b1 (00:0c:29:52:7d:b1)
▸ Internet Protocol Version 4, Src: 10.0.1.11, Dst: 10.0.1.10
▸ Transmission Control Protocol, Src Port: 49689, 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: 43]
```

*Figure 9 Malicious URL*

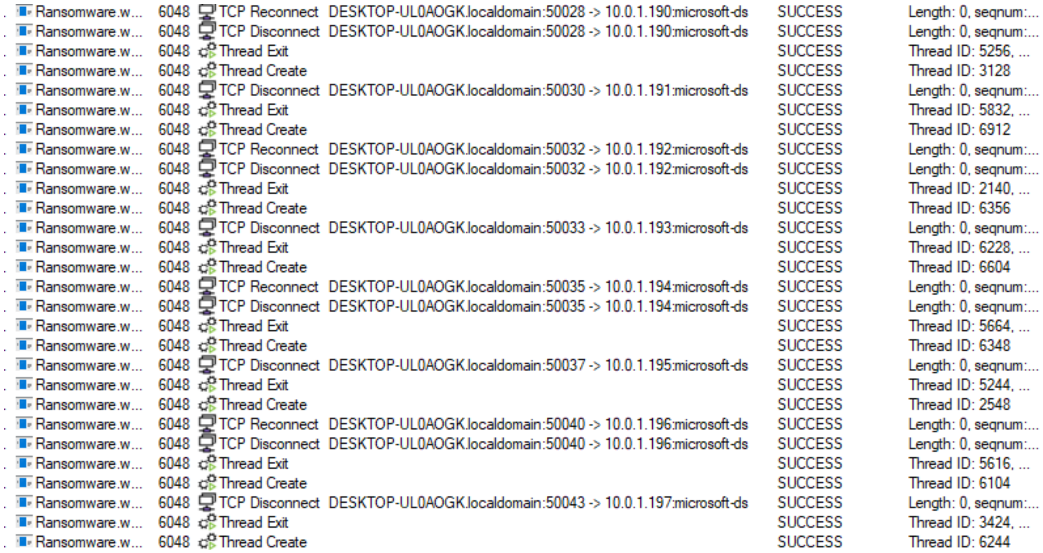
The malware will not detonate its malicious payload if there is 200 OK response for the requested URL.

Conversely, the malicious payload start detonating, and at the beginning of the detonating it will start propagating on local network if there is no internet connection using TCP/445 port number.



| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| services.exe | 640 | TCP | Listen | 0.0.0.0 | 49670 | 0.0.0.0 | 0 | 11/8/2023 10:25:13 AM | services.exe |
| svchost.exe | 2396 | TCP | Listen | 0.0.0.0 | 49671 | 0.0.0.0 | 0 | 11/8/2023 10:25:16 AM | PolicyAgent |
| Ransomware.wannacr... | 5464 | TCP | Syn Sent | 10.0.1.11 | 49760 | 10.0.1.1 | 445 | 12/6/2023 11:23:30 AM | mssecsvc2.0 |
| Ransomware.wannacr... | 5464 | TCP | Syn Sent | 10.0.1.11 | 49761 | 10.0.1.2 | 445 | 12/6/2023 11:23:30 AM | mssecsvc2.0 |
| Ransomware.wannacr... | 5464 | TCP | Syn Sent | 10.0.1.11 | 49762 | 10.0.1.3 | 445 | 12/6/2023 11:23:30 AM | mssecsvc2.0 |
| Ransomware.wannacr... | 5464 | TCP | Syn Sent | 10.0.1.11 | 49763 | 10.0.1.4 | 445 | 12/6/2023 11:23:30 AM | mssecsvc2.0 |
| Ransomware.wannacr... | 5464 | TCP | Syn Sent | 10.0.1.11 | 49764 | 10.0.1.5 | 445 | 12/6/2023 11:23:30 AM | mssecsvc2.0 |
| Ransomware.wannacr... | 5464 | TCP | Syn Sent | 10.0.1.11 | 49765 | 10.0.1.6 | 445 | 12/6/2023 11:23:30 AM | mssecsvc2.0 |
| Ransomware.wannacr... | 5464 | TCP | Syn Sent | 10.0.1.11 | 49766 | 10.0.1.7 | 445 | 12/6/2023 11:23:30 AM | mssecsvc2.0 |
| Ransomware.wannacr... | 5464 | TCP | Syn Sent | 10.0.1.11 | 49767 | 10.0.1.8 | 445 | 12/6/2023 11:23:30 AM | mssecsvc2.0 |
| Ransomware.wannacr... | 5464 | TCP | Syn Sent | 10.0.1.11 | 49768 | 10.0.1.9 | 445 | 12/6/2023 11:23:30 AM | mssecsvc2.0 |
| Ransomware.wannacr... | 5464 | TCP | Syn Sent | 10.0.1.11 | 49769 | 10.0.1.10 | 445 | 12/6/2023 11:23:30 AM | mssecsvc2.0 |
| System | 4 | TCP | Listen | 0.0.0.0 | 445 | 0.0.0.0 | 0 | 11/8/2023 10:25:11 AM | System |
| svchost.exe | 2100 | TCP | Listen | 0.0.0.0 | 7680 | 0.0.0.0 | 0 | 11/8/2023 10:25:05 AM | DoSvc |
| svchost.exe | 908 | TCPv6 | Listen | :: | 135 | :: | 0 | 11/8/2023 10:24:42 AM | RpcEptMapper |
| System | 4 | TCPv6 | Listen | :: | 445 | :: | 0 | 11/8/2023 10:25:11 AM | System |

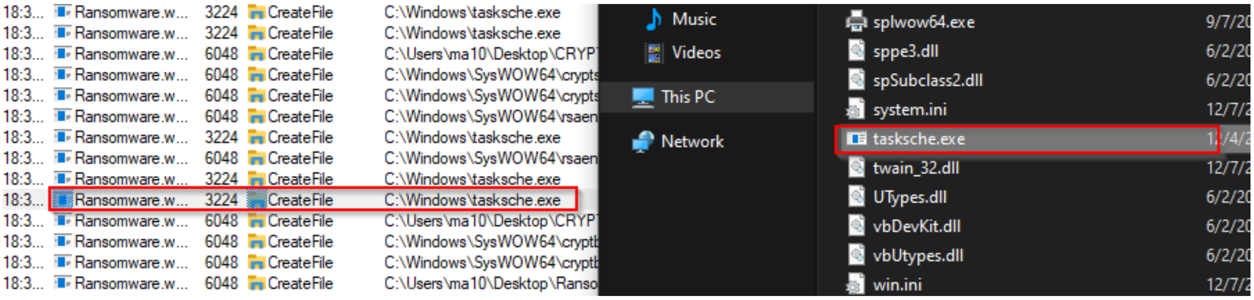
*Figure 10 spreading.*



```
. Ransomware.w...  6048  TCP Reconnect  DESKTOP-UL0AOGK.localdomain:50028 -> 10.0.1.190:microsoft-ds  SUCCESS  Length: 0, seqnum:...
. Ransomware.w...  6048  TCP Disconnect  DESKTOP-UL0AOGK.localdomain:50028 -> 10.0.1.190:microsoft-ds  SUCCESS  Length: 0, seqnum:...
. Ransomware.w...  6048  Thread Exit                                                                    SUCCESS  Thread ID: 5256, ...
. Ransomware.w...  6048  Thread Create                                                                  SUCCESS  Thread ID: 3128
. Ransomware.w...  6048  TCP Disconnect  DESKTOP-UL0AOGK.localdomain:50030 -> 10.0.1.191:microsoft-ds  SUCCESS  Length: 0, seqnum:...
. Ransomware.w...  6048  Thread Exit                                                                    SUCCESS  Thread ID: 5832, ...
. Ransomware.w...  6048  Thread Create                                                                  SUCCESS  Thread ID: 6912
. Ransomware.w...  6048  TCP Reconnect  DESKTOP-UL0AOGK.localdomain:50032 -> 10.0.1.192:microsoft-ds  SUCCESS  Length: 0, seqnum:...
. Ransomware.w...  6048  TCP Disconnect  DESKTOP-UL0AOGK.localdomain:50032 -> 10.0.1.192:microsoft-ds  SUCCESS  Length: 0, seqnum:...
. Ransomware.w...  6048  Thread Exit                                                                    SUCCESS  Thread ID: 2140, ...
. Ransomware.w...  6048  Thread Create                                                                  SUCCESS  Thread ID: 6356
. Ransomware.w...  6048  TCP Disconnect  DESKTOP-UL0AOGK.localdomain:50033 -> 10.0.1.193:microsoft-ds  SUCCESS  Length: 0, seqnum:...
. Ransomware.w...  6048  Thread Exit                                                                    SUCCESS  Thread ID: 6228, ...
. Ransomware.w...  6048  Thread Create                                                                  SUCCESS  Thread ID: 6604
. Ransomware.w...  6048  TCP Reconnect  DESKTOP-UL0AOGK.localdomain:50035 -> 10.0.1.194:microsoft-ds  SUCCESS  Length: 0, seqnum:...
. Ransomware.w...  6048  TCP Disconnect  DESKTOP-UL0AOGK.localdomain:50035 -> 10.0.1.194:microsoft-ds  SUCCESS  Length: 0, seqnum:...
. Ransomware.w...  6048  Thread Exit                                                                    SUCCESS  Thread ID: 5664, ...
. Ransomware.w...  6048  Thread Create                                                                  SUCCESS  Thread ID: 6348
. Ransomware.w...  6048  TCP Disconnect  DESKTOP-UL0AOGK.localdomain:50037 -> 10.0.1.195:microsoft-ds  SUCCESS  Length: 0, seqnum:...
. Ransomware.w...  6048  Thread Exit                                                                    SUCCESS  Thread ID: 5244, ...
. Ransomware.w...  6048  Thread Create                                                                  SUCCESS  Thread ID: 2548
. Ransomware.w...  6048  TCP Reconnect  DESKTOP-UL0AOGK.localdomain:50040 -> 10.0.1.196:microsoft-ds  SUCCESS  Length: 0, seqnum:...
. Ransomware.w...  6048  TCP Disconnect  DESKTOP-UL0AOGK.localdomain:50040 -> 10.0.1.196:microsoft-ds  SUCCESS  Length: 0, seqnum:...
. Ransomware.w...  6048  Thread Exit                                                                    SUCCESS  Thread ID: 5616, ...
. Ransomware.w...  6048  Thread Create                                                                  SUCCESS  Thread ID: 6104
. Ransomware.w...  6048  TCP Disconnect  DESKTOP-UL0AOGK.localdomain:50043 -> 10.0.1.197:microsoft-ds  SUCCESS  Length: 0, seqnum:...
. Ransomware.w...  6048  Thread Exit                                                                    SUCCESS  Thread ID: 3424, ...
. Ransomware.w...  6048  Thread Create                                                                  SUCCESS  Thread ID: 6244
```

*Figure 11 spreading procmon*

The malware installs other executables in multiple location of the host, specifically "tasksche.exe":

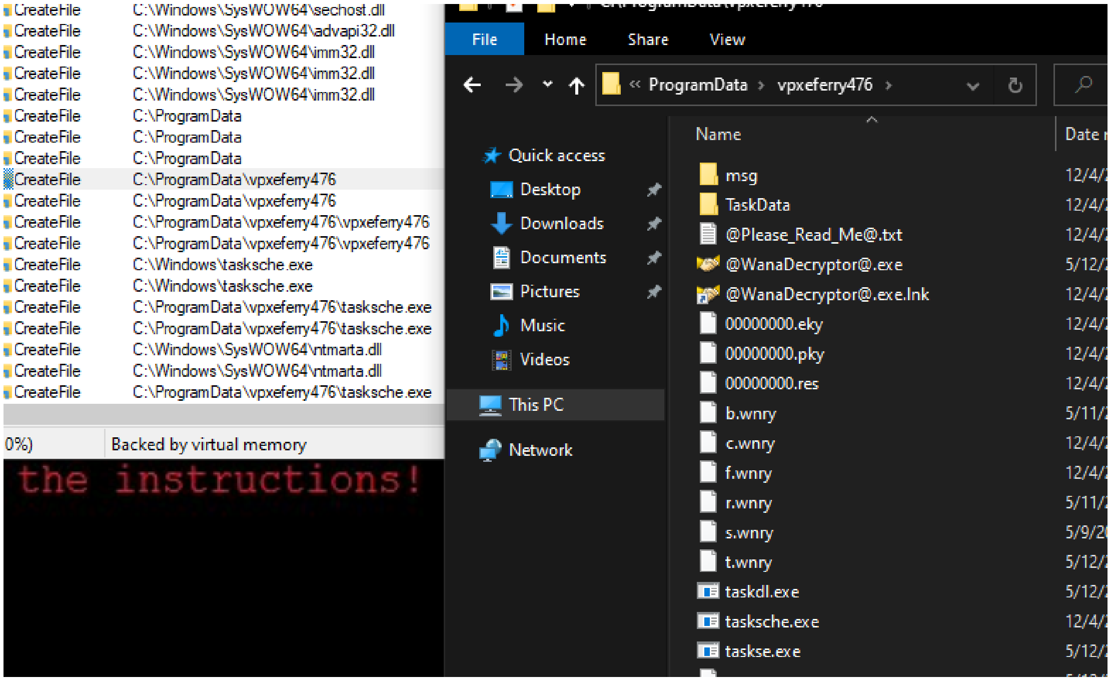


```
18:3...  Ransomware.w...  3224  CreateFile  C:\Windows\tasksche.exe
18:3...  Ransomware.w...  3224  CreateFile  C:\Windows\tasksche.exe
18:3...  Ransomware.w...  6048  CreateFile  C:\Users\ma10\Desktop\CRYP
18:3...  Ransomware.w...  6048  CreateFile  C:\Windows\SysWOW64\crypts
18:3...  Ransomware.w...  6048  CreateFile  C:\Windows\SysWOW64\crypts
18:3...  Ransomware.w...  6048  CreateFile  C:\Windows\SysWOW64\rsaen
18:3...  Ransomware.w...  3224  CreateFile  C:\Windows\tasksche.exe
18:3...  Ransomware.w...  6048  CreateFile  C:\Windows\SysWOW64\rsaen
18:3...  Ransomware.w...  3224  CreateFile  C:\Windows\tasksche.exe
18:3...  Ransomware.w...  3224  CreateFile  C:\Windows\tasksche.exe
18:3...  Ransomware.w...  6048  CreateFile  C:\Users\ma10\Desktop\CRYP
18:3...  Ransomware.w...  6048  CreateFile  C:\Windows\SysWOW64\cryptb
18:3...  Ransomware.w...  6048  CreateFile  C:\Windows\SysWOW64\cryptb
18:3...  Ransomware.w...  6048  CreateFile  C:\Users\ma10\Desktop\Ranso
```

```
splwow64.exe     9/7/20
sppe3.dll        6/2/20
spSubclass2.dll  6/2/20
system.ini       12/7/2
tasksche.exe     1 /4/2
twain_32.dll     12/7/2
UTypes.dll       6/2/20
vbDevKit.dll     6/2/20
vbUtypes.dll     6/2/20
win.ini          12/7/2
```

*Figure 12 installing other executables.*

Creating a hidden directory perhaps it is malware's staging area:



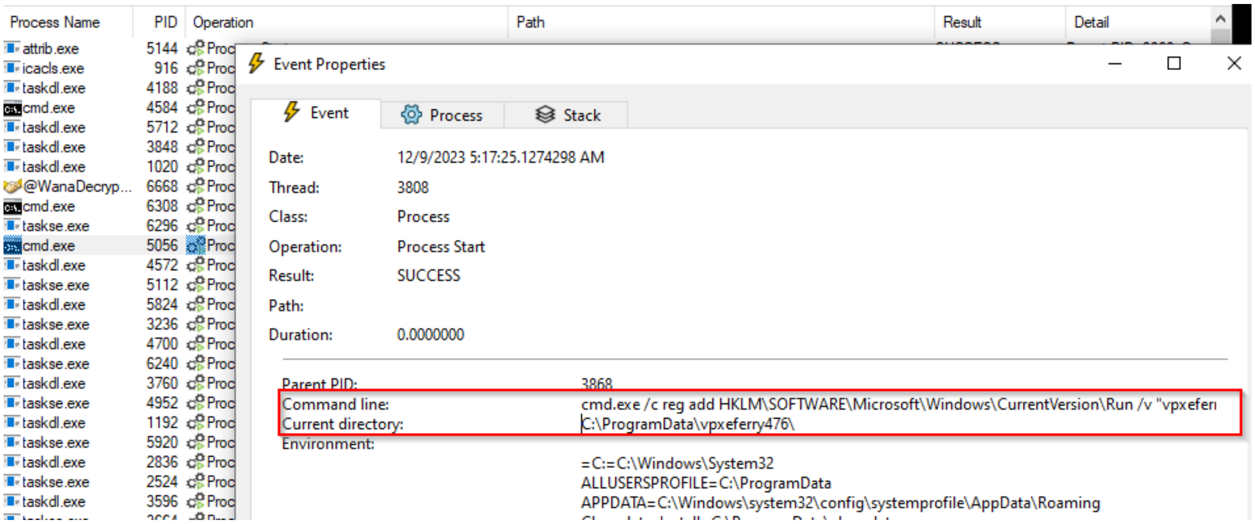
```
CreateFile    C:\Windows\SysWOW64\sechost.dll
CreateFile    C:\Windows\SysWOW64\advapi32.dll
CreateFile    C:\Windows\SysWOW64\imm32.dll
CreateFile    C:\Windows\SysWOW64\imm32.dll
CreateFile    C:\Windows\SysWOW64\imm32.dll
CreateFile    C:\ProgramData
CreateFile    C:\ProgramData
CreateFile    C:\ProgramData
CreateFile    C:\ProgramData\vpxeferry476
CreateFile    C:\ProgramData\vpxeferry476
CreateFile    C:\ProgramData\vpxeferry476\vpxeferry476
CreateFile    C:\ProgramData\vpxeferry476\vpxeferry476
CreateFile    C:\Windows\tasksche.exe
CreateFile    C:\Windows\tasksche.exe
CreateFile    C:\ProgramData\vpxeferry476\tasksche.exe
CreateFile    C:\ProgramData\vpxeferry476\tasksche.exe
CreateFile    C:\Windows\SysWOW64\ntmarta.dll
CreateFile    C:\Windows\SysWOW64\ntmarta.dll
CreateFile    C:\ProgramData\vpxeferry476\tasksche.exe

0%)    Backed by virtual memory

the instructions!
```

| Name | Date |
|---|---|
| msg | 12/4/ |
| TaskData | 12/4/ |
| @Please_Read_Me@.txt | 12/4/ |
| @WanaDecryptor@.exe | 5/12/ |
| @WanaDecryptor@.exe.lnk | 12/4/ |
| 00000000.eky | 12/4/ |
| 00000000.pky | 12/4/ |
| 00000000.res | 12/4/ |
| b.wnry | 5/11/ |
| c.wnry | 12/4/ |
| f.wnry | 12/4/ |
| r.wnry | 5/11/ |
| s.wnry | 5/9/2 |
| t.wnry | 5/12/ |
| taskdl.exe | 5/12/ |
| tasksche.exe | 12/4/ |
| taskse.exe | 5/12/ |

*Figure 13 staging area.*

The malware adds a registry key:

cmd.exe /c reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "vpxeferry476" /t REG_SZ /d "\"C:\ProgramData\vpxeferry476\tasksche.exe\"" /f



| Process Name | PID | Operation |
|---|---|---|
| attrib.exe | 5144 | Proc |
| icacls.exe | 916 | Proc |
| taskdl.exe | 4188 | Proc |
| cmd.exe | 4584 | Proc |
| taskdl.exe | 5712 | Proc |
| taskdl.exe | 3848 | Proc |
| taskdl.exe | 1020 | Proc |
| @WanaDecryp... | 6668 | Proc |
| cmd.exe | 6308 | Proc |
| taskse.exe | 6296 | Proc |
| cmd.exe | 5056 | Proc |
| taskdl.exe | 4572 | Proc |
| taskse.exe | 5112 | Proc |
| taskdl.exe | 5824 | Proc |
| taskse.exe | 3236 | Proc |
| taskdl.exe | 4700 | Proc |
| taskse.exe | 6240 | Proc |
| taskdl.exe | 3760 | Proc |
| taskse.exe | 4952 | Proc |
| taskdl.exe | 1192 | Proc |
| taskse.exe | 5920 | Proc |
| taskdl.exe | 2836 | Proc |
| taskse.exe | 2524 | Proc |
| taskdl.exe | 3596 | Proc |

Date: 12/9/2023 5:17:25.1274298 AM

Thread: 3808

Class: Process

Operation: Process Start

Result: SUCCESS

Path:

Duration: 0.0000000

Parent PID: 3868

Command line: cmd.exe /c reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "vpxeferı

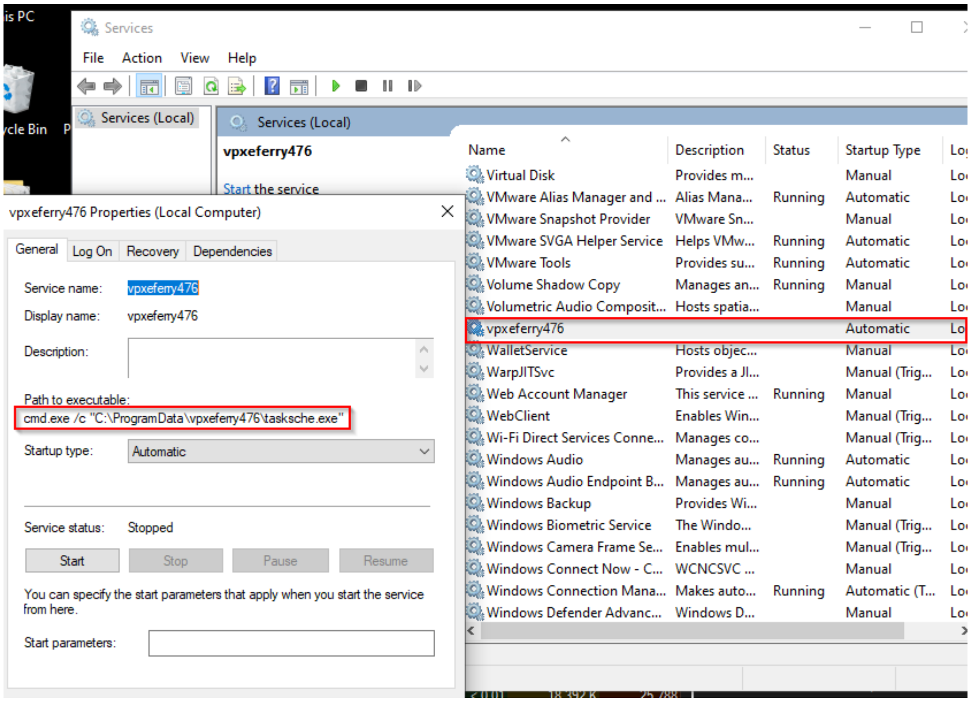
Current directory: C:\ProgramData\vpxeferry476\

Environment:

```
=C:=C:\Windows\System32
ALLUSERSPROFILE=C:\ProgramData
APPDATA=C:\Windows\system32\config\systemprofile\AppData\Roaming
```

*Figure 14 adding registry key.*

The malware creates the service task with the same directory name, it means the file can still run even after rebooting, and encrypt any other files added or any USB that plugged in.


Services
File Action View Help
Services (Local)
vpxeferry476
Start the service
vpxeferry476 Properties (Local Computer)
General Log On Recovery Dependencies

Service name: vpxeferry476

Display name: vpxeferry476

Description:

Path to executable:
cmd.exe /c "C:\ProgramData\vpxeferry476\tasksche.exe"

Startup type: Automatic

Service status: Stopped

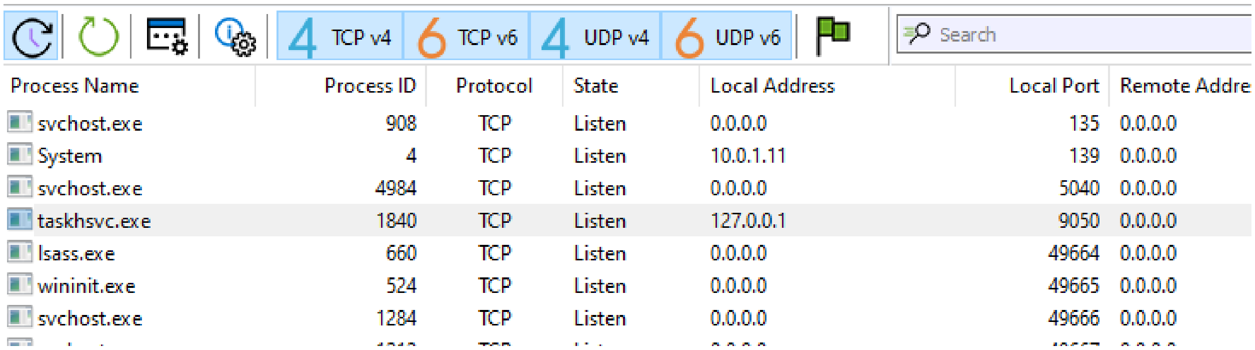
You can specify the start parameters that apply when you start the service from here.

Start parameters:

| Name | Description | Status | Startup Type | Lo |
|---|---|---|---|---|
| Virtual Disk | Provides m... | | Manual | Lo |
| VMware Alias Manager and ... | Alias Mana... | Running | Automatic | Lo |
| VMware Snapshot Provider | VMware Sn... | | Manual | Lo |
| VMware SVGA Helper Service | Helps VMw... | Running | Automatic | Lo |
| VMware Tools | Provides su... | Running | Automatic | Lo |
| Volume Shadow Copy | Manages an... | Running | Manual | Lo |
| Volumetric Audio Composit... | Hosts spatia... | | Manual | Lo |
| vpxeferry476 | | | Automatic | Lo |
| WalletService | Hosts objec... | | Manual | Lo |
| WarpJITSvc | Provides a JI... | | Manual (Trig... | Lo |
| Web Account Manager | This service ... | Running | Manual | Lo |
| WebClient | Enables Win... | | Manual (Trig... | Lo |
| Wi-Fi Direct Services Conne... | Manages co... | | Manual (Trig... | Lo |
| Windows Audio | Manages au... | Running | Automatic | Lo |
| Windows Audio Endpoint B... | Manages au... | Running | Automatic | Lo |
| Windows Backup | Provides Wi... | | Manual | Lo |
| Windows Biometric Service | The Windo... | | Manual (Trig... | Lo |
| Windows Camera Frame Se... | Enables mul... | | Manual (Trig... | Lo |
| Windows Connect Now - C... | WCNCSVC ... | | Manual | Lo |
| Windows Connection Mana... | Makes auto... | Running | Automatic (T... | Lo |
| Windows Defender Advanc... | Windows D... | | Manual | Lo |

*Figure 15 creating malicious service task.*

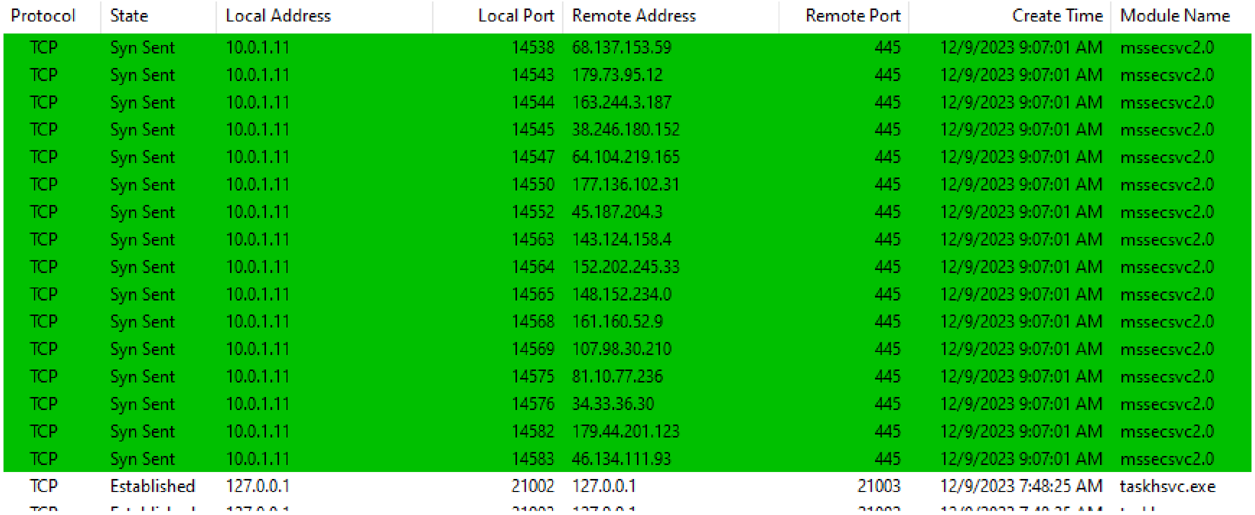
The taskhsvc.exe start listening on localhost TCP/9050 port number and from any remote address



| Process Name | Process ID | Protocol | State | Local Address | Local Port | Remote Addre |
|---|---|---|---|---|---|---|
| svchost.exe | 908 | TCP | Listen | 0.0.0.0 | 135 | 0.0.0.0 |
| System | 4 | TCP | Listen | 10.0.1.11 | 139 | 0.0.0.0 |
| svchost.exe | 4984 | TCP | Listen | 0.0.0.0 | 5040 | 0.0.0.0 |
| taskhsvc.exe | 1840 | TCP | Listen | 127.0.0.1 | 9050 | 0.0.0.0 |
| lsass.exe | 660 | TCP | Listen | 0.0.0.0 | 49664 | 0.0.0.0 |
| wininit.exe | 524 | TCP | Listen | 0.0.0.0 | 49665 | 0.0.0.0 |
| svchost.exe | 1284 | TCP | Listen | 0.0.0.0 | 49666 | 0.0.0.0 |

*Figure 16 listening port*

If there is internet connection while the malware is successfully detonated, it tries to spread with SMB share on public IP Addresses:



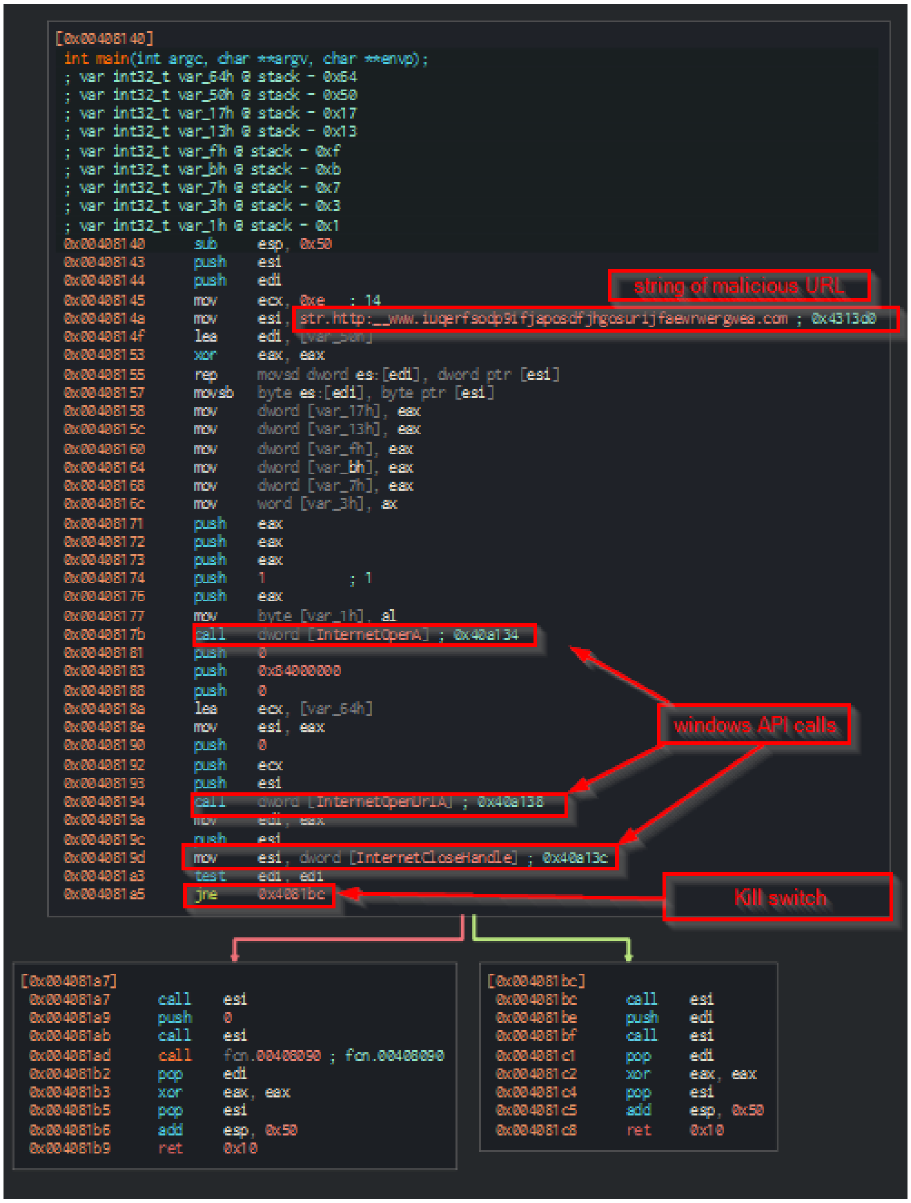
| Protocol | State | Local Address | Local Port | Remote Address | Remote Port | Create Time | Module Name |
|---|---|---|---|---|---|---|---|
| TCP | Syn Sent | 10.0.1.11 | 14538 | 68.137.153.59 | 445 | 12/9/2023 9:07:01 AM | mssecsvc2.0 |
| TCP | Syn Sent | 10.0.1.11 | 14543 | 179.73.95.12 | 445 | 12/9/2023 9:07:01 AM | mssecsvc2.0 |
| TCP | Syn Sent | 10.0.1.11 | 14544 | 163.244.3.187 | 445 | 12/9/2023 9:07:01 AM | mssecsvc2.0 |
| TCP | Syn Sent | 10.0.1.11 | 14545 | 38.246.180.152 | 445 | 12/9/2023 9:07:01 AM | mssecsvc2.0 |
| TCP | Syn Sent | 10.0.1.11 | 14547 | 64.104.219.165 | 445 | 12/9/2023 9:07:01 AM | mssecsvc2.0 |
| TCP | Syn Sent | 10.0.1.11 | 14550 | 177.136.102.31 | 445 | 12/9/2023 9:07:01 AM | mssecsvc2.0 |
| TCP | Syn Sent | 10.0.1.11 | 14552 | 45.187.204.3 | 445 | 12/9/2023 9:07:01 AM | mssecsvc2.0 |
| TCP | Syn Sent | 10.0.1.11 | 14563 | 143.124.158.4 | 445 | 12/9/2023 9:07:01 AM | mssecsvc2.0 |
| TCP | Syn Sent | 10.0.1.11 | 14564 | 152.202.245.33 | 445 | 12/9/2023 9:07:01 AM | mssecsvc2.0 |
| TCP | Syn Sent | 10.0.1.11 | 14565 | 148.152.234.0 | 445 | 12/9/2023 9:07:01 AM | mssecsvc2.0 |
| TCP | Syn Sent | 10.0.1.11 | 14568 | 161.160.52.9 | 445 | 12/9/2023 9:07:01 AM | mssecsvc2.0 |
| TCP | Syn Sent | 10.0.1.11 | 14569 | 107.98.30.210 | 445 | 12/9/2023 9:07:01 AM | mssecsvc2.0 |
| TCP | Syn Sent | 10.0.1.11 | 14575 | 81.10.77.236 | 445 | 12/9/2023 9:07:01 AM | mssecsvc2.0 |
| TCP | Syn Sent | 10.0.1.11 | 14576 | 34.33.36.30 | 445 | 12/9/2023 9:07:01 AM | mssecsvc2.0 |
| TCP | Syn Sent | 10.0.1.11 | 14582 | 179.44.201.123 | 445 | 12/9/2023 9:07:01 AM | mssecsvc2.0 |
| TCP | Syn Sent | 10.0.1.11 | 14583 | 46.134.111.93 | 445 | 12/9/2023 9:07:01 AM | mssecsvc2.0 |
| TCP | Established | 127.0.0.1 | 21002 | 127.0.0.1 | 21003 | 12/9/2023 7:48:25 AM | taskhsvc.exe |

*Figure 17 spreading to public networks.*

# Advanced Static Analysis

This phase malware will not be executed, statically debugging into assembly language level, figuring out the source code and how the malware triggers its malicious payload. In this phase cutter tool is being used.

The main function of the malware sample contains a malicious URL string, windows API calls to initialize internet connection and reaching specified URL, the result of the reaching the malicious URL will be saved and then based of the result the kill switch decides to detonate malicious payload or not.



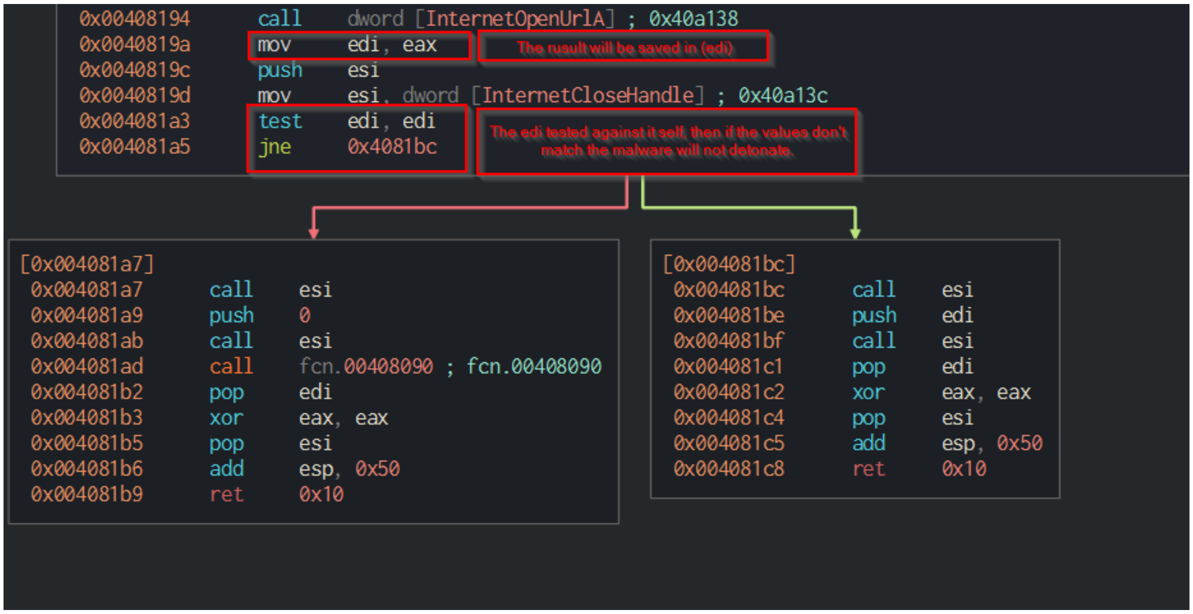
```
[0x00408140]
 int main(int argc, char **argv, char **envp);
 ; var int32_t var_64h @ stack - 0x64
 ; var int32_t var_50h @ stack - 0x50
 ; var int32_t var_17h @ stack - 0x17
 ; var int32_t var_13h @ stack - 0x13
 ; var int32_t var_fh @ stack - 0xf
 ; var int32_t var_bh @ stack - 0xb
 ; var int32_t 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
```

Figure 18 main function (cutter)

The result of the malicious URL response will be saved in the (edi), then the test function will test the result of (edi) against itself, based on that, the JNE (Jump Not Equal) will decide to continue and run the rest of the payload or not.



```
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
```

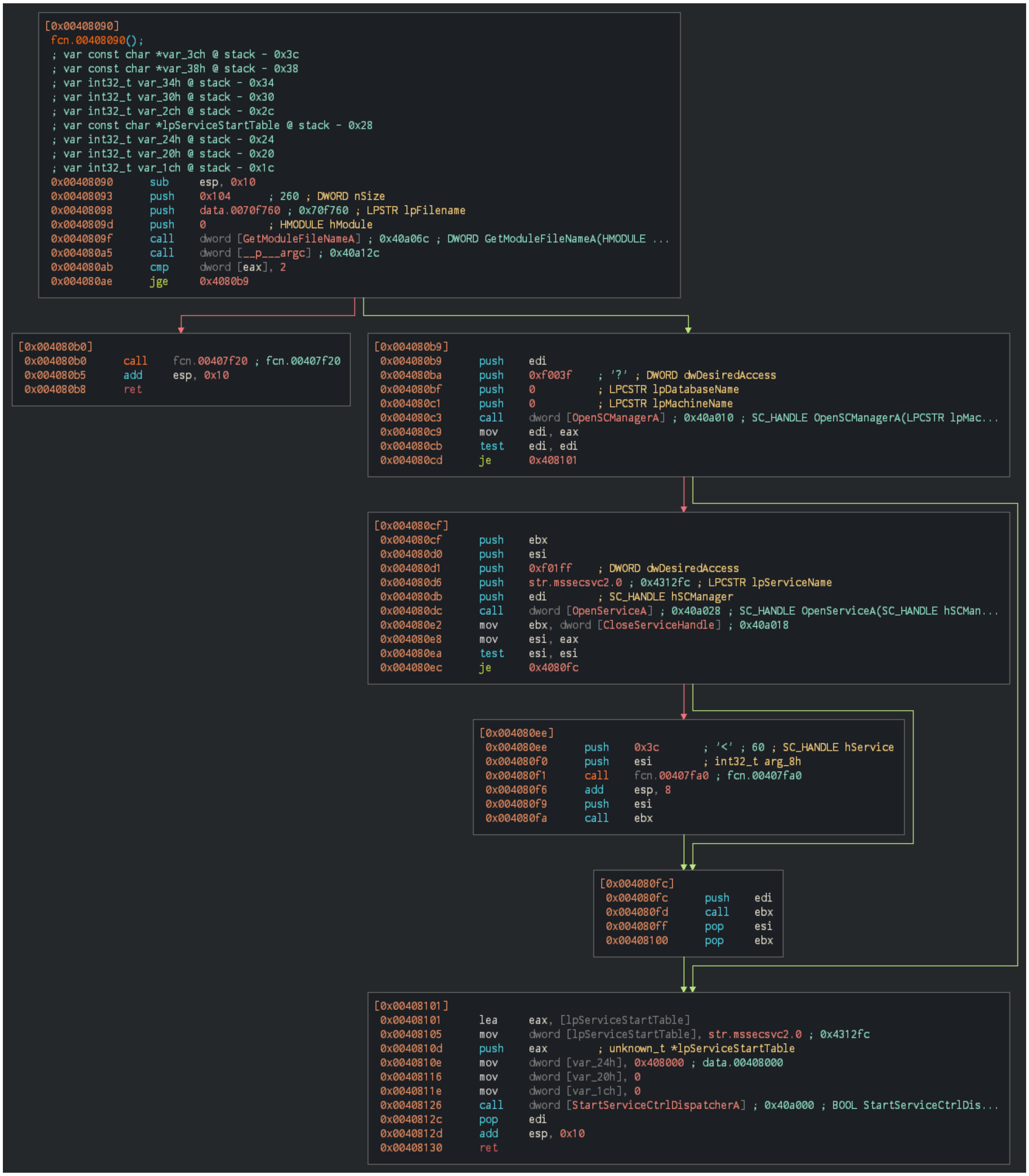
The rusult will be saved in (edi)

The edi tested against it self, then if the values don't match the malware will not detonate.

*Figure 19 kill switch.*

If the values matched, the payload would continue and executes the rest of malicious payload which they reside in the third call function of the memory address [00408090] from left, otherwise the JNE function will jump to memory address [0x4081bc] and exit the program.

The rest of the payload in the address has been called after successful execution.



```
[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
```

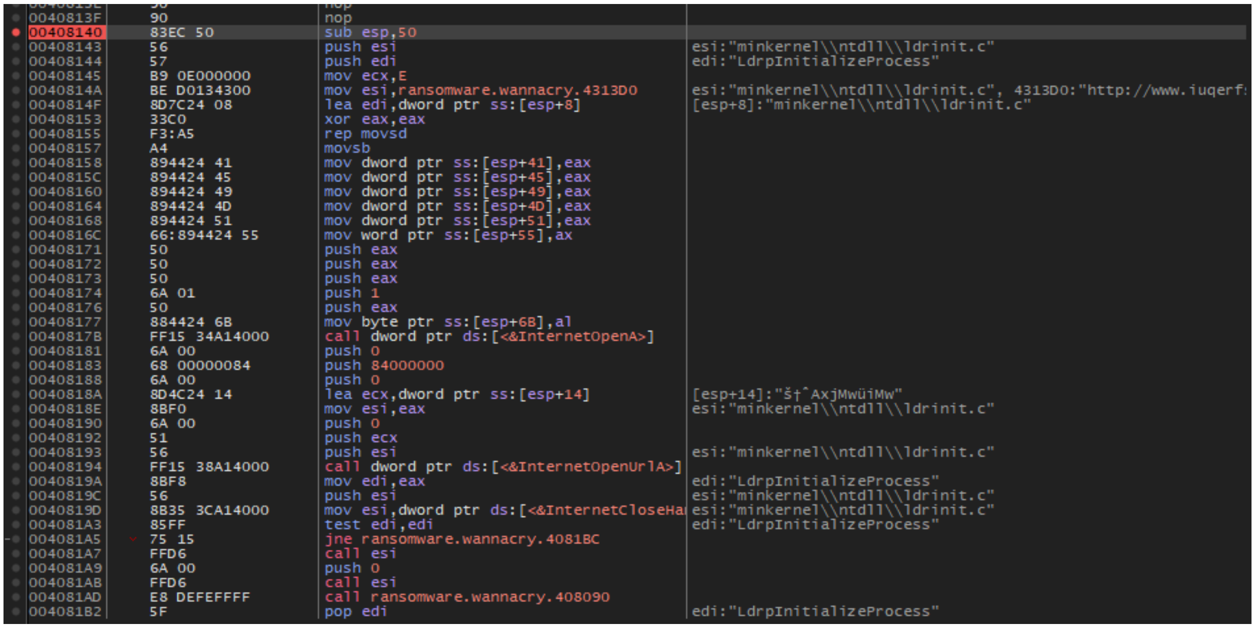
```
[0x004080fc]
 0x004080fc      push    edi
 0x004080fd      call    ebx
 0x004080ff      pop     esi
 0x00408100      pop     ebx
```

```
[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 20 malicious payload*

# Advanced Dynamic Analysis

In Advanced Dynamic Analysis phase, the malware is executing inside debugger, this provides the ability to change the malware routine and process while executing.
Using a tool like x32dbg, a breakpoint is set to the main function address [0x0408140] that could be found in the advanced static analysis phase where the kill switch URL is checked before executing entire payload.



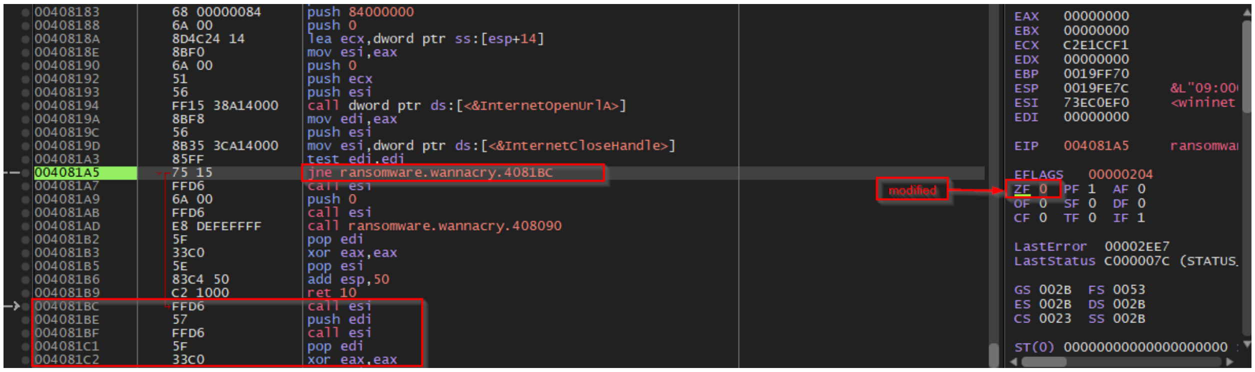
```
0040813F   90                nop
00408140   83EC 50           sub esp,50
00408143   56                push esi                                  esi:"minkernel\\ntdll\\ldrinit.c"
00408144   57                push edi                                  edi:"LdrpInitializeProcess"
00408145   B9 0E000000       mov ecx,E
0040814A   BE D0134300       mov esi,ransomware.wannacry.4313D0        esi:"minkernel\\ntdll\\ldrinit.c", 4313D0:"http://www.iuqerf
0040814F   8D7C24 08         lea edi,dword ptr ss:[esp+8]              [esp+8]:"minkernel\\ntdll\\ldrinit.c"
00408153   33C0              xor eax,eax
00408155   F3:A5             rep movsd
00408157   A4                movsb
00408158   894424 41         mov dword ptr ss:[esp+41],eax
0040815C   894424 45         mov dword ptr ss:[esp+45],eax
00408160   894424 49         mov dword ptr ss:[esp+49],eax
00408164   894424 4D         mov dword ptr ss:[esp+4D],eax
00408168   894424 51         mov dword ptr ss:[esp+51],eax
0040816C   66:894424 55      mov word ptr ss:[esp+55],ax
00408171   50                push eax
00408172   50                push eax
00408173   50                push eax
00408174   6A 01             push 1
00408176   50                push eax
00408177   884424 6B         mov byte ptr ss:[esp+6B],al
0040817B   FF15 34A14000     call dword ptr ds:[<&InternetOpenA>]
00408181   6A 00             push 0
00408183   68 00000084       push 84000000
00408188   6A 00             push 0
0040818A   8D4C24 14         lea ecx,dword ptr ss:[esp+14]             [esp+14]:"š†ˆAxjMwüiMw"
0040818E   8BF0              mov esi,eax                               esi:"minkernel\\ntdll\\ldrinit.c"
00408190   6A 00             push 0
00408192   51                push ecx
00408193   56                push esi                                  esi:"minkernel\\ntdll\\ldrinit.c"
00408194   FF15 38A14000     call dword ptr ds:[<&InternetOpenUrlA>]
0040819A   8BF8              mov edi,eax                               edi:"LdrpInitializeProcess"
0040819C   56                push esi                                  esi:"minkernel\\ntdll\\ldrinit.c"
0040819D   8B35 3CA14000     mov esi,dword ptr ds:[<&InternetCloseHa   esi:"minkernel\\ntdll\\ldrinit.c"
004081A3   85FF              test edi,edi                              edi:"LdrpInitializeProcess"
004081A5   75 15             jne ransomware.wannacry.4081BC
004081A7   FFD6              call esi
004081A9   6A 00             push 0
004081AB   FFD6              call esi
004081AD   E8 DEFEFFFF       call ransomware.wannacry.408090
004081B2   5F                pop edi                                   edi:"LdrpInitializeProcess"
```

*Figure 21 x32 Debugger*

Hence, we can validate the payload behavior and summarize in points:

1- The ZF (Zero Flag) is already set to 1.
2- When the malicious URL is not responds, due to internet availability or domain is not hosted (not-exist) the result will be zero and saved in EAX (EAX=0)
3- Then the value of EAX moved to EDI this will set EDI to zero (EDI=0)
4- The EDI tested against itself, in this case the EDI remains zero and ZF remains 1 meaning the test function result is set to zero.
5- The JNE will not execute its function and the payload will continue the rest of its activity.

However, if ZF value modified to 0, the JNE function will jump to [0x04081BC] address and exit the program even if the malicious URL is unreachable, meaning the rest of malicious payload will not execute.

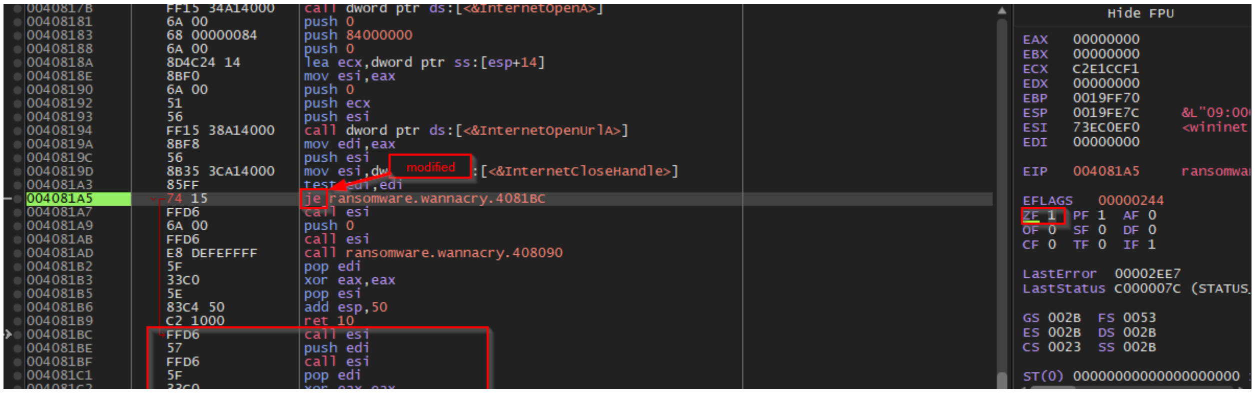


```
00408183   68 00000084     push 84000000
00408188   6A 00           push 0
0040818A   8D4C24 14       lea ecx,dword ptr ss:[esp+14]
0040818E   8BF0            mov esi,eax
00408190   6A 00           push 0
00408192   51              push ecx
00408193   56              push esi
00408194   FF15 38A14000   call dword ptr ds:[<&InternetOpenUrlA>]
0040819A   8BF8            mov edi,eax
0040819C   56              push esi
0040819D   8B35 3CA14000   mov esi,dword ptr ds:[<&InternetCloseHandle>]
004081A3   85FF            test edi,edi
004081A5   75 15           jne ransomware.wannacry.4081BC
004081A7   FFD6            call esi
004081A9   6A 00           push 0
004081AB   FFD6            call esi
004081AD   E8 DEFEFFFF     call ransomware.wannacry.408090
004081B2   5F              pop edi
004081B3   33C0            xor eax,eax
004081B5   5E              pop esi
004081B6   83C4 50         add esp,50
004081B9   C2 1000         ret 10
004081BC   FFD6            call esi
004081BE   57              push edi
004081BF   FFD6            call esi
004081C1   5F              pop edi
004081C2   33C0            xor eax,eax
```

```
EAX   00000000
EBX   00000000
ECX   C2E1CCF1
EDX   00000000
EBP   0019FF70
ESP   0019FE7C      &L"09:00
ESI   73EC0EF0      <wininet
EDI   00000000

EIP   004081A5      ransomwa

EFLAGS    00000204
ZF 0  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1

LastError   00002EE7
LastStatus  C000007C (STATUS_

GS 002B  FS 0053
ES 002B  DS 002B
CS 0023  SS 002B

ST(0) 00000000000000000000
```

Figure 22 modifying ZF

Another way to force malicious payload to not execute is by modifying the JNE to JE when the ZF is already set to 1, in another word by this modification we can say “If the malicious URL is unreachable, and the result of comparing EDI are equal, jump to [0x04081BC] address, do not execute the malicious payload and exit the program.”



```
0040817B   FF15 34A14000   call dword ptr ds:[<&InternetOpenA>]
00408181   6A 00           push 0
00408183   68 00000084     push 84000000
00408188   6A 00           push 0
0040818A   8D4C24 14       lea ecx,dword ptr ss:[esp+14]
0040818E   8BF0            mov esi,eax
00408190   6A 00           push 0
00408192   51              push ecx
00408193   56              push esi
00408194   FF15 38A14000   call dword ptr ds:[<&InternetOpenUrlA>]
0040819A   8BF8            mov edi,eax
0040819C   56              push esi
0040819D   8B35 3CA14000   mov esi,dw          :[<&InternetCloseHandle>]
004081A3   85FF            test edi,edi
004081A5   74 15           je ransomware.wannacry.4081BC
004081A7   FFD6            call esi
004081A9   6A 00           push 0
004081AB   FFD6            call esi
004081AD   E8 DEFEFFFF     call ransomware.wannacry.408090
004081B2   5F              pop edi
004081B3   33C0            xor eax,eax
004081B5   5E              pop esi
004081B6   83C4 50         add esp,50
004081B9   C2 1000         ret 10
004081BC   FFD6            call esi
004081BE   57              push edi
004081BF   FFD6            call esi
004081C1   5F              pop edi
004081C2   33C0            xor eax,eax
```

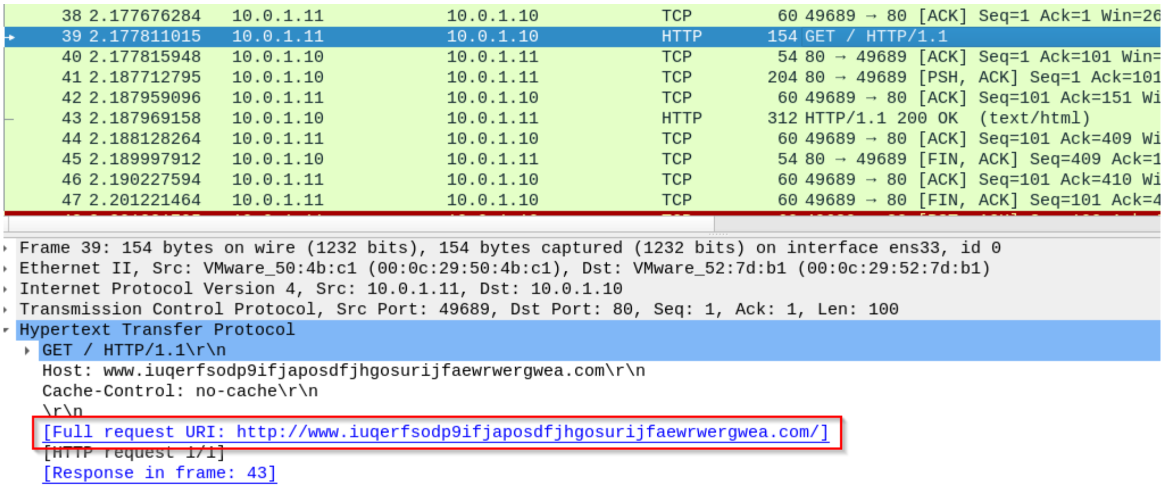
```
Hide FPU

EAX   00000000
EBX   00000000
ECX   C2E1CCF1
EDX   00000000
EBP   0019FF70
ESP   0019FE7C      &L"09:00
ESI   73EC0EF0      <wininet
EDI   00000000

EIP   004081A5      ransomwa

EFLAGS    00000244
ZF 1  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1

LastError   00002EE7
LastStatus  C000007C (STATUS_

GS 002B  FS 0053
ES 002B  DS 002B
CS 0023  SS 002B

ST(0) 00000000000000000000
```

Figure 23 modifying JNE

# Indicators of Compromise

## Network Indicators

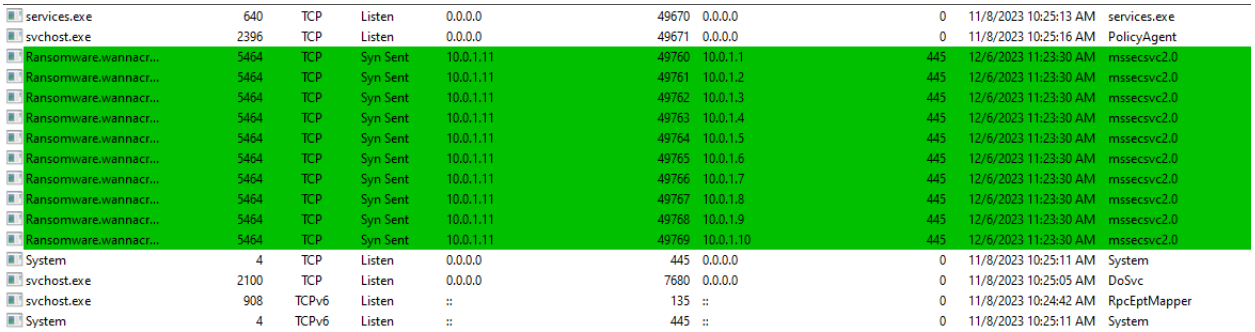
Reaching out to the malicious URL: hxxp://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com



```
 38 2.177676284   10.0.1.11          10.0.1.10          TCP          60 49689 → 80 [ACK] Seq=1 Ack=1 Win=26
 39 2.177811015   10.0.1.11          10.0.1.10          HTTP        154 GET / HTTP/1.1
 40 2.177815948   10.0.1.10          10.0.1.11          TCP          54 80 → 49689 [ACK] Seq=1 Ack=101 Win=
 41 2.187712795   10.0.1.10          10.0.1.11          TCP         204 80 → 49689 [PSH, ACK] Seq=1 Ack=101
 42 2.187959096   10.0.1.11          10.0.1.10          TCP          60 49689 → 80 [ACK] Seq=101 Ack=151 Wi
 43 2.187969158   10.0.1.10          10.0.1.11          HTTP        312 HTTP/1.1 200 OK  (text/html)
 44 2.188128264   10.0.1.11          10.0.1.10          TCP          60 49689 → 80 [ACK] Seq=101 Ack=409 Wi
 45 2.189997912   10.0.1.10          10.0.1.11          TCP          54 80 → 49689 [FIN, ACK] Seq=409 Ack=1
 46 2.190227594   10.0.1.11          10.0.1.10          TCP          60 49689 → 80 [ACK] Seq=101 Ack=410 Wi
 47 2.201221464   10.0.1.11          10.0.1.10          TCP          60 49689 → 80 [FIN, ACK] Seq=101 Ack=4

Frame 39: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) on interface ens33, id 0
Ethernet II, Src: VMware_50:4b:c1 (00:0c:29:50:4b:c1), Dst: VMware_52:7d:b1 (00:0c:29:52:7d:b1)
Internet Protocol Version 4, Src: 10.0.1.11, Dst: 10.0.1.10
Transmission Control Protocol, Src Port: 49689, 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: 43]
```

*Figure 24 Wireshark capture initial URL check*

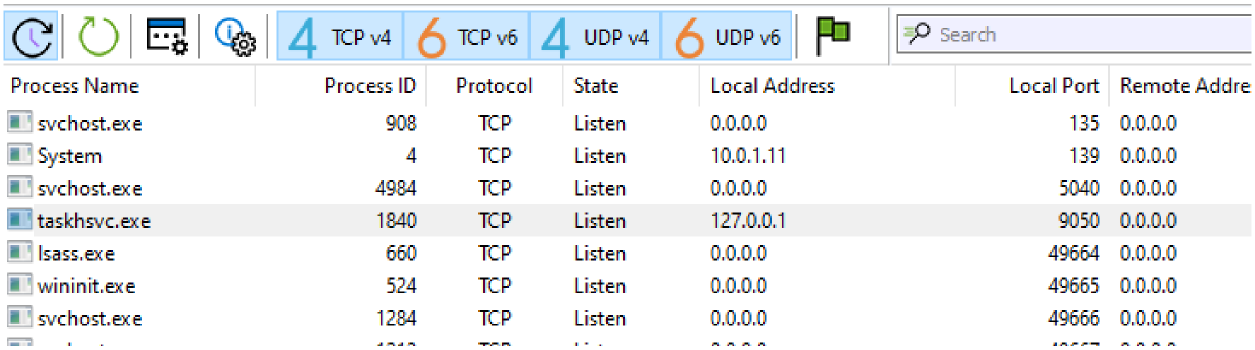
Propagating in the local network of the victim through SMB port TCP/445.



| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| services.exe | 640 | TCP | Listen | 0.0.0.0 | 49670 | 0.0.0.0 | 0 | 11/8/2023 10:25:13 AM | services.exe |
| svchost.exe | 2396 | TCP | Listen | 0.0.0.0 | 49671 | 0.0.0.0 | 0 | 11/8/2023 10:25:16 AM | PolicyAgent |
| Ransomware.wannacr... | 5464 | TCP | Syn Sent | 10.0.1.11 | 49760 | 10.0.1.1 | 445 | 12/6/2023 11:23:30 AM | mssecsvc2.0 |
| Ransomware.wannacr... | 5464 | TCP | Syn Sent | 10.0.1.11 | 49761 | 10.0.1.2 | 445 | 12/6/2023 11:23:30 AM | mssecsvc2.0 |
| Ransomware.wannacr... | 5464 | TCP | Syn Sent | 10.0.1.11 | 49762 | 10.0.1.3 | 445 | 12/6/2023 11:23:30 AM | mssecsvc2.0 |
| Ransomware.wannacr... | 5464 | TCP | Syn Sent | 10.0.1.11 | 49763 | 10.0.1.4 | 445 | 12/6/2023 11:23:30 AM | mssecsvc2.0 |
| Ransomware.wannacr... | 5464 | TCP | Syn Sent | 10.0.1.11 | 49764 | 10.0.1.5 | 445 | 12/6/2023 11:23:30 AM | mssecsvc2.0 |
| Ransomware.wannacr... | 5464 | TCP | Syn Sent | 10.0.1.11 | 49765 | 10.0.1.6 | 445 | 12/6/2023 11:23:30 AM | mssecsvc2.0 |
| Ransomware.wannacr... | 5464 | TCP | Syn Sent | 10.0.1.11 | 49766 | 10.0.1.7 | 445 | 12/6/2023 11:23:30 AM | mssecsvc2.0 |
| Ransomware.wannacr... | 5464 | TCP | Syn Sent | 10.0.1.11 | 49767 | 10.0.1.8 | 445 | 12/6/2023 11:23:30 AM | mssecsvc2.0 |
| Ransomware.wannacr... | 5464 | TCP | Syn Sent | 10.0.1.11 | 49768 | 10.0.1.9 | 445 | 12/6/2023 11:23:30 AM | mssecsvc2.0 |
| Ransomware.wannacr... | 5464 | TCP | Syn Sent | 10.0.1.11 | 49769 | 10.0.1.10 | 445 | 12/6/2023 11:23:30 AM | mssecsvc2.0 |
| System | 4 | TCP | Listen | 0.0.0.0 | 445 | 0.0.0.0 | 0 | 11/8/2023 10:25:11 AM | System |
| svchost.exe | 2100 | TCP | Listen | 0.0.0.0 | 7680 | 0.0.0.0 | 0 | 11/8/2023 10:25:05 AM | DoSvc |
| svchost.exe | 908 | TCPv6 | Listen | :: | 135 | :: | 0 | 11/8/2023 10:24:42 AM | RpcEptMapper |
| System | 4 | TCPv6 | Listen | :: | 445 | :: | 0 | 11/8/2023 10:25:11 AM | System |

*Figure 25 indicating propagating in network*

The taskhsvc.exe will be listening on TCP/9050.

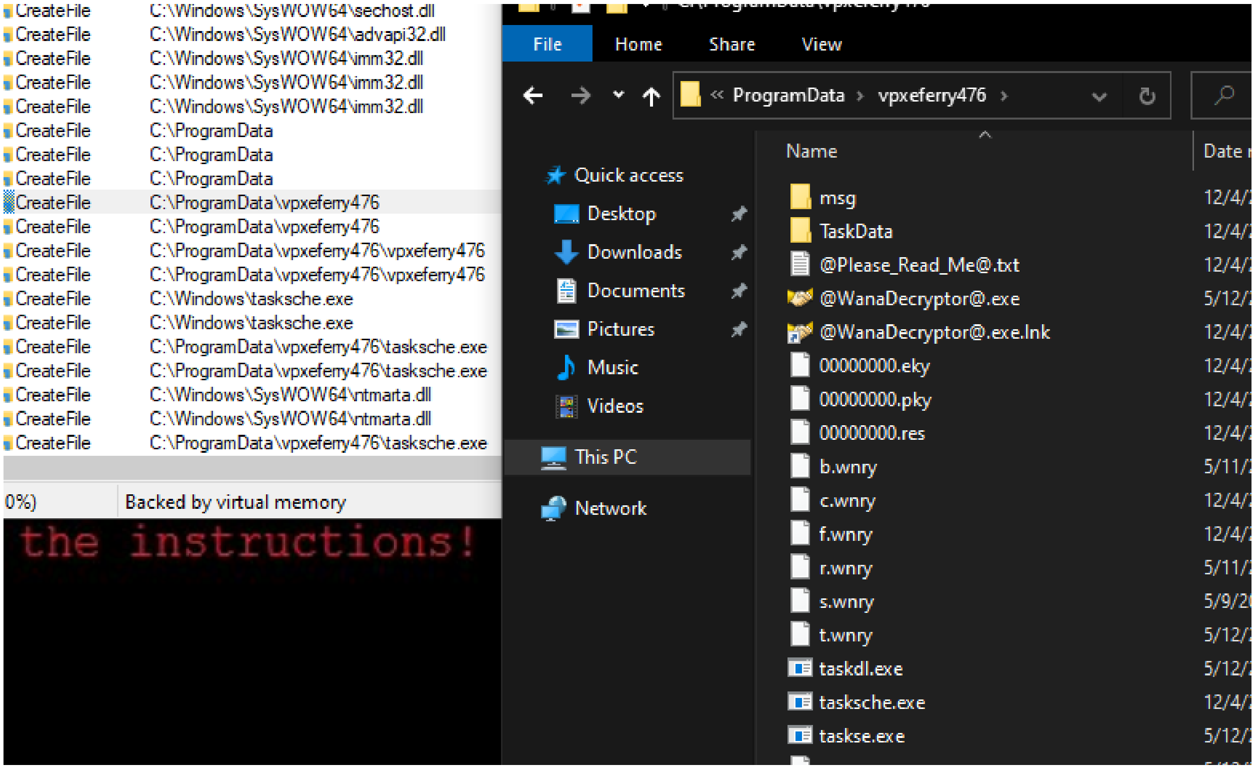


| Process Name | Process ID | Protocol | State | Local Address | Local Port | Remote Addre |
|---|---|---|---|---|---|---|
| svchost.exe | 908 | TCP | Listen | 0.0.0.0 | 135 | 0.0.0.0 |
| System | 4 | TCP | Listen | 10.0.1.11 | 139 | 0.0.0.0 |
| svchost.exe | 4984 | TCP | Listen | 0.0.0.0 | 5040 | 0.0.0.0 |
| taskhsvc.exe | 1840 | TCP | Listen | 127.0.0.1 | 9050 | 0.0.0.0 |
| lsass.exe | 660 | TCP | Listen | 0.0.0.0 | 49664 | 0.0.0.0 |
| wininit.exe | 524 | TCP | Listen | 0.0.0.0 | 49665 | 0.0.0.0 |
| svchost.exe | 1284 | TCP | Listen | 0.0.0.0 | 49666 | 0.0.0.0 |

*Figure 26 indicating listening port*

## Host-based Indicators

When the malware is successfully executed, it will create a hidden directory and make it as it's staging area.



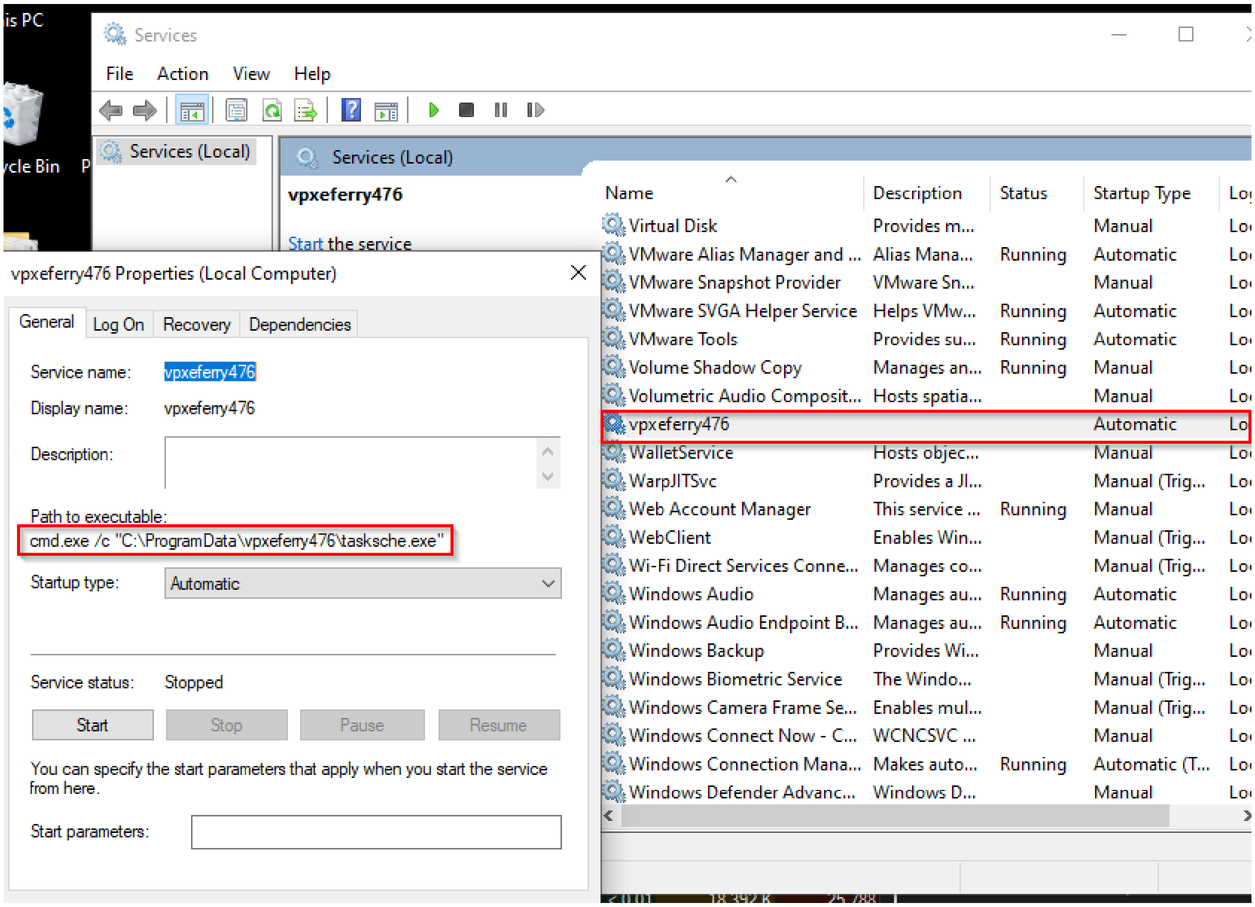
```
CreateFile    C:\Windows\SysWOW64\sechost.dll
CreateFile    C:\Windows\SysWOW64\advapi32.dll
CreateFile    C:\Windows\SysWOW64\imm32.dll
CreateFile    C:\Windows\SysWOW64\imm32.dll
CreateFile    C:\Windows\SysWOW64\imm32.dll
CreateFile    C:\ProgramData
CreateFile    C:\ProgramData
CreateFile    C:\ProgramData
CreateFile    C:\ProgramData\vpxeferry476
CreateFile    C:\ProgramData\vpxeferry476
CreateFile    C:\ProgramData\vpxeferry476\vpxeferry476
CreateFile    C:\ProgramData\vpxeferry476\vpxeferry476
CreateFile    C:\Windows\tasksche.exe
CreateFile    C:\Windows\tasksche.exe
CreateFile    C:\ProgramData\vpxeferry476\tasksche.exe
CreateFile    C:\ProgramData\vpxeferry476\tasksche.exe
CreateFile    C:\Windows\SysWOW64\ntmarta.dll
CreateFile    C:\Windows\SysWOW64\ntmarta.dll
CreateFile    C:\ProgramData\vpxeferry476\tasksche.exe
```

```
0%)    Backed by virtual memory
the instructions!
```

| Name | Date |
|---|---|
| msg | 12/4/ |
| TaskData | 12/4/ |
| @Please_Read_Me@.txt | 12/4/ |
| @WanaDecryptor@.exe | 5/12/ |
| @WanaDecryptor@.exe.lnk | 12/4/ |
| 00000000.eky | 12/4/ |
| 00000000.pky | 12/4/ |
| 00000000.res | 12/4/ |
| b.wnry | 5/11/ |
| c.wnry | 12/4/ |
| f.wnry | 12/4/ |
| r.wnry | 5/11/ |
| s.wnry | 5/9/2 |
| t.wnry | 5/12/ |
| taskdl.exe | 5/12/ |
| tasksche.exe | 12/4/ |
| taskse.exe | 5/12/ |

*Figure 27 indicating hidden directory*

The malware creates a service to remain persistent.



Service name: vpxeferry476

Display name: vpxeferry476

Description:

Path to executable:
cmd.exe /c "C:\ProgramData\vpxeferry476\tasksche.exe"

Startup type: Automatic

Service status: Stopped

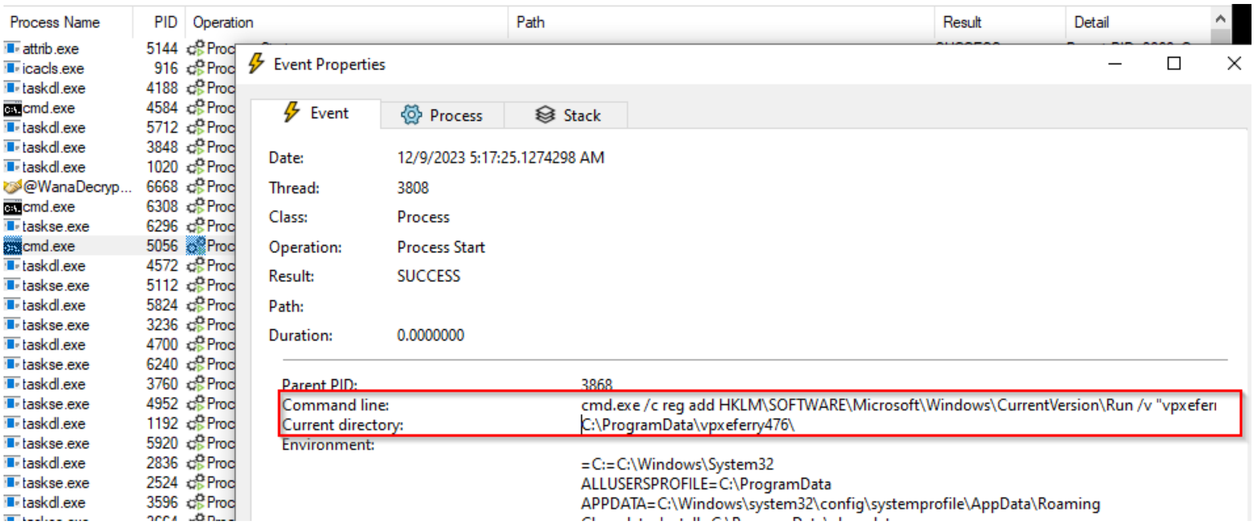
You can specify the start parameters that apply when you start the service from here.

Start parameters:

| Name | Description | Status | Startup Type | Lo |
|---|---|---|---|---|
| Virtual Disk | Provides m... | | Manual | Lo |
| VMware Alias Manager and ... | Alias Mana... | Running | Automatic | Lo |
| VMware Snapshot Provider | VMware Sn... | | Manual | Lo |
| VMware SVGA Helper Service | Helps VMw... | Running | Automatic | Lo |
| VMware Tools | Provides su... | Running | Automatic | Lo |
| Volume Shadow Copy | Manages an... | Running | Manual | Lo |
| Volumetric Audio Composit... | Hosts spatia... | | Manual | Lo |
| vpxeferry476 | | | Automatic | Lo |
| WalletService | Hosts objec... | | Manual | Lo |
| WarpJITSvc | Provides a JI... | | Manual (Trig... | Lo |
| Web Account Manager | This service ... | Running | Manual | Lo |
| WebClient | Enables Win... | | Manual (Trig... | Lo |
| Wi-Fi Direct Services Conne... | Manages co... | | Manual (Trig... | Lo |
| Windows Audio | Manages au... | Running | Automatic | Lo |
| Windows Audio Endpoint B... | Manages au... | Running | Automatic | Lo |
| Windows Backup | Provides Wi... | | Manual | Lo |
| Windows Biometric Service | The Windo... | | Manual (Trig... | Lo |
| Windows Camera Frame Se... | Enables mul... | | Manual (Trig... | Lo |
| Windows Connect Now - C... | WCNCSVC ... | | Manual | Lo |
| Windows Connection Mana... | Makes auto... | Running | Automatic (T... | Lo |
| Windows Defender Advanc... | Windows D... | | Manual | Lo |

*Figure 28 indicating malicious service*

The malware adds registry key.



| Process Name | PID | Operation | Path | Result | Detail |
|---|---|---|---|---|---|
| attrib.exe | 5144 | Proc | | | |
| icacls.exe | 916 | Proc | | | |
| taskdl.exe | 4188 | Proc | | | |
| cmd.exe | 4584 | Proc | | | |
| taskdl.exe | 5712 | Proc | | | |
| taskdl.exe | 3848 | Proc | | | |
| taskdl.exe | 1020 | Proc | | | |
| @WanaDecryp... | 6668 | Proc | | | |
| cmd.exe | 6308 | Proc | | | |
| taskse.exe | 6296 | Proc | | | |
| cmd.exe | 5056 | Proc | | | |
| taskdl.exe | 4572 | Proc | | | |
| taskse.exe | 5112 | Proc | | | |
| taskdl.exe | 5824 | Proc | | | |
| taskse.exe | 3236 | Proc | | | |
| taskdl.exe | 4700 | Proc | | | |
| taskse.exe | 6240 | Proc | | | |
| taskdl.exe | 3760 | Proc | | | |
| taskse.exe | 4952 | Proc | | | |
| taskdl.exe | 1192 | Proc | | | |
| taskse.exe | 5920 | Proc | | | |
| taskdl.exe | 2836 | Proc | | | |
| taskse.exe | 2524 | Proc | | | |
| taskdl.exe | 3596 | Proc | | | |

Date: 12/9/2023 5:17:25.1274298 AM

Thread: 3808

Class: Process

Operation: Process Start

Result: SUCCESS

Path:

Duration: 0.0000000

Parent PID: 3868

Command line: cmd.exe /c reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "vpxeferı

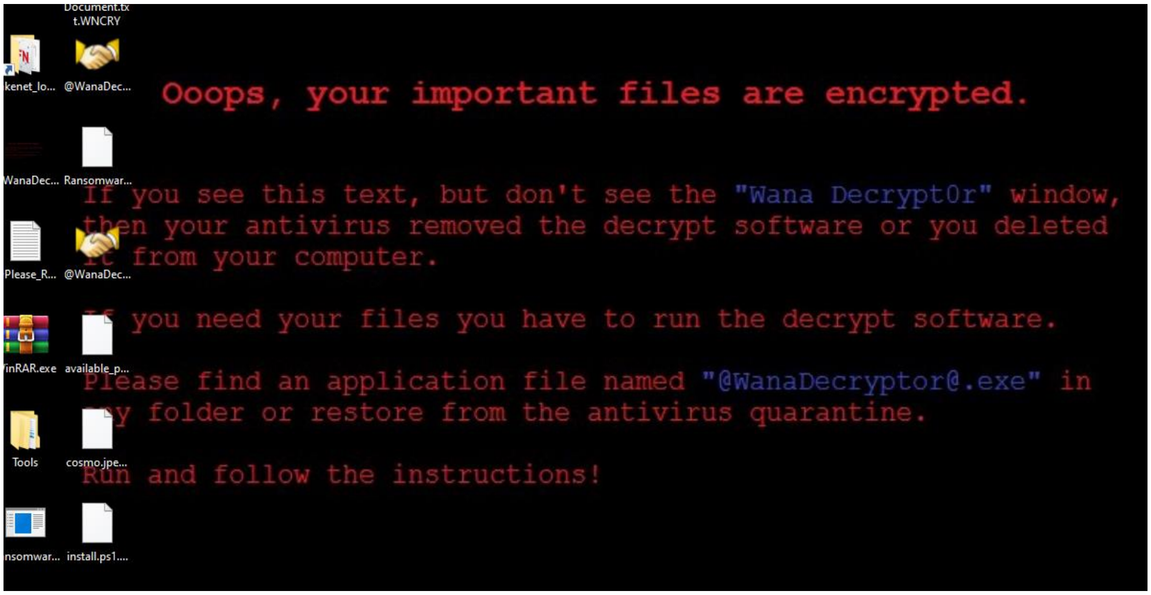
Current directory: C:\ProgramData\vpxeferry476\

Environment:

```
=C:=C:\Windows\System32
ALLUSERSPROFILE=C:\ProgramData
APPDATA=C:\Windows\system32\config\systemprofile\AppData\Roaming
```

*Figure 29 indicating registry key*

Changing desktop wallpaper to a “.bmp” image, meanwhile encrypting files.



Ooops, your important files are encrypted.

If you see this text, but don't see the "Wana Decrypt0r" window, then your antivirus removed the decrypt software or you deleted it from your computer.

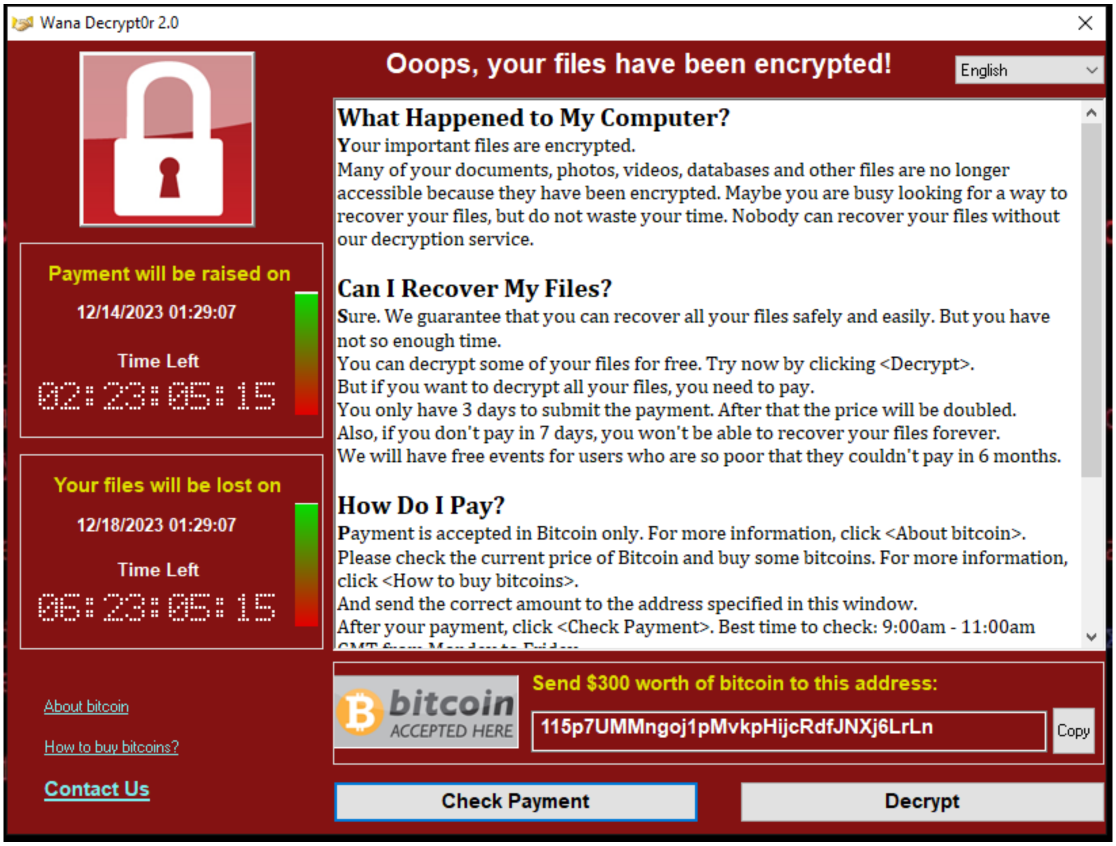
If you need your files you have to run the decrypt software.

Please find an application file named "@WanaDecryptor@.exe" in any folder or restore from the antivirus quarantine.

Run and follow the instructions!

*Figure 30 indicating wallpaper change*

A GUI window pops up in the middle of the screen, to instruct the victim for payment process.



Ooops, your files have been encrypted!

Payment will be raised on

12/14/2023 01:29:07

Time Left

02:23:05:15

Your files will be lost on

12/18/2023 01:29:07

Time Left

06:23:05:15

**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 GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

*Figure 31  decryptor program*

# Rules & Signatures

A full set of YARA rules is included in Appendix A.

URL: hxxp://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

Strings:

www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com"

icacls . /grant Everyone:F /T /C /Q"

\\172.16.99.5\\IPC$"

\\192.168.56.20\\IPC$"

WanaCrypt0r"

C:\\%s\\qeriuwjhrf"

attrib +h ."

tasksche.exe"

diskpart.exe"

taskdl.exe"

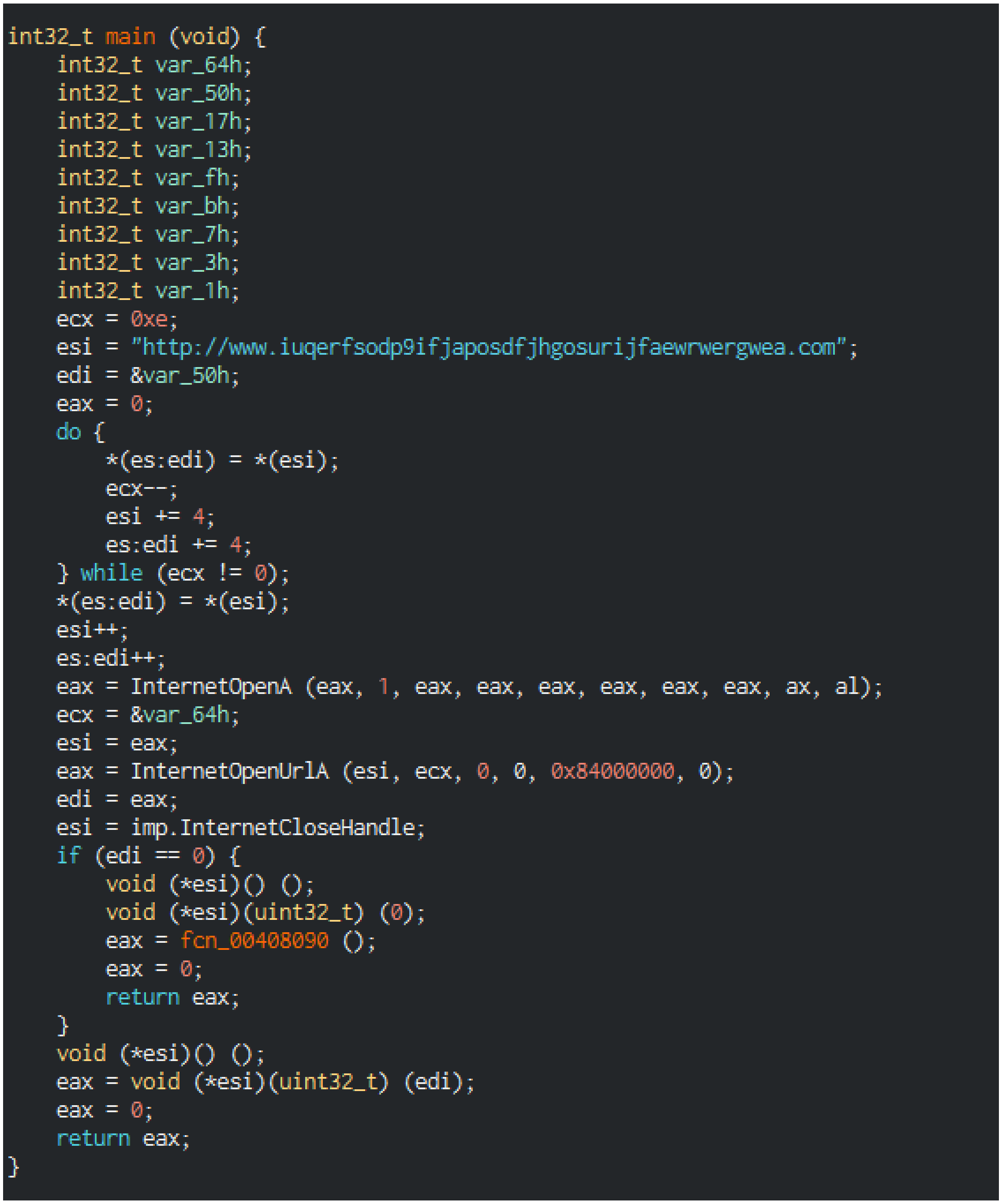
taskse.exe

# Appendices

## A. Yara Rules

```
rule wannaCryDetection {

    meta:
        last_updated = "2023-12-12"
        author = "unShad0wer"
        description = "WannaCry YARA detection rule"
        sha256 =
"24D004A104D4D54034DBCFFC2A4B19A11F39008A575AA614EA04703480B1022C"

    strings:

        $string1 = "www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com" ascii
        $string2 = "icacls . /grant Everyone:F /T /C /Q" ascii
        $string3 = "\\172.16.99.5\\IPC$" ascii
        $string4 = "\\192.168.56.20\\IPC$" ascii
        $string5 = "WanaCrypt0r" ascii
        $string6 = "C:\\%s\\qeriuwjhrf" ascii
        $string7 = "attrib +h ." ascii
        $string8 = "tasksche.exe" ascii
        $string9 = "diskpart.exe" ascii
        $string10 = "taskdl.exe" ascii
        $string11 = "taskse.exe" ascii


    condition:

        $string1 and any of ($string*)
}
```

## B. Decompiled Code Snippets



```
int32_t main (void) {
    int32_t var_64h;
    int32_t var_50h;
    int32_t var_17h;
    int32_t var_13h;
    int32_t var_fh;
    int32_t var_bh;
    int32_t var_7h;
    int32_t var_3h;
    int32_t var_1h;
    ecx = 0xe;
    esi = "http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com";
    edi = &var_50h;
    eax = 0;
    do {
        *(es:edi) = *(esi);
        ecx--;
        esi += 4;
        es:edi += 4;
    } while (ecx != 0);
    *(es:edi) = *(esi);
    esi++;
    es:edi++;
    eax = InternetOpenA (eax, 1, eax, eax, eax, eax, eax, eax, ax, al);
    ecx = &var_64h;
    esi = eax;
    eax = InternetOpenUrlA (esi, ecx, 0, 0, 0x84000000, 0);
    edi = eax;
    esi = imp.InternetCloseHandle;
    if (edi == 0) {
        void (*esi)() ();
        void (*esi)(uint32_t) (0);
        eax = fcn_00408090 ();
        eax = 0;
        return eax;
    }
    void (*esi)() ();
    eax = void (*esi)(uint32_t) (edi);
    eax = 0;
    return eax;
}
```

*Figure 32 decompiled main function*