Malware Analysis Report

Ransomware.Wannacry Malware

June 2023 | Theodoros Vergos “cde” | v1.0

Table of Contents

Executive Report

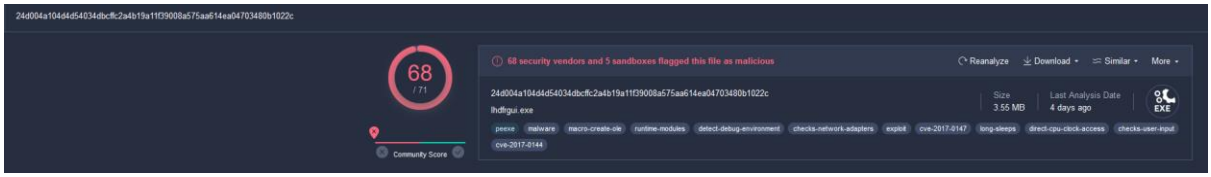
Name	Ransomware.wannacry.exe
MD5:	db349b97c37d22f5ea1d1841e3c89eb4
SHA1:	e889544aff85ffaf8b0d0da705105dee7c97fe26
SHA256:	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
Architecture:	x86
Signature:	Microsoft Visual C++ v6.0

The file in question has been identified as an encryptor with worm capabilities. The malware has two main components, the propagator and the encryptor. Symptoms of malware presence if the network include DNS requests for the URL *hxxp://www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com/*, systems performing ARP requests to the network in order to discover other systems followed by connection attempts on TCP port 445 (SMB). For a successful infection the malware needs to be executed with administrative rights. Then a DNS request and an http request are performed, if the HTTP request returns an HTTP -200 response the malware does not continue with the execution.

In order to mitigate this particular strain, it is recommended to add the following URL *hxxp://www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com/* to systems' hosts file and DNS server records, redirecting any requests to a sinkhole server.

Additionally, a YARA rule has been included in this report to aid in identifying the malware in the wild.

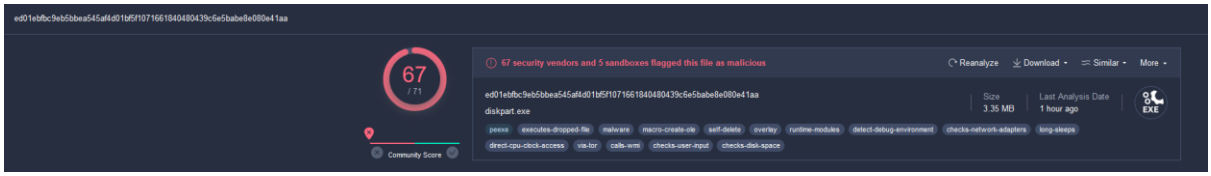
Currently, this malware has 68/71 vendors detections in *virustotal.com*



The main encryption mechanism is considered the following executable that is unpacked from the initial malware and can be used with other delivery methods as well, without relying on the *Ransomware.wannacry.exe* executable:

Name	Tasksche.exe
MD5	84c82835a5d21bbcf75a61706d8ab549
Sha1	5ff465afaabcbf0150d1a3ab2c2e74f3a4426467
SHA256	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
Architecture	x86
Signature	Microsoft Visual C++ v6.0

This malware has 67/71 vendor detection in *virustotal.com*



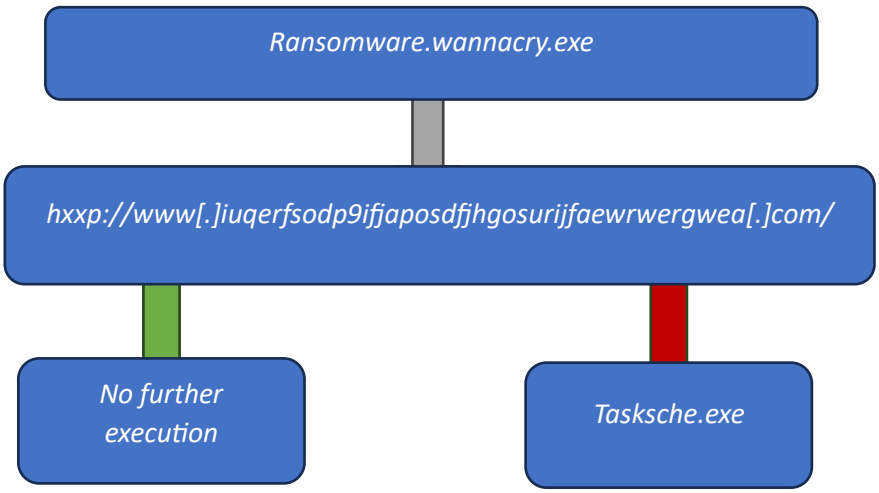
For this executable no workaround was detected in order to stop the execution.

YARA Rule

```
rule wannacry {

    meta:
        last_updated = "2023-06-18"
        author = "cde"
        description = "A Yara rule for detecting wannacry ransomware. This is
a part of the final lab for PMAT"

    strings:
        // Fill out identifying strings and other criteria
        $string1 = "http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com"
ascii
        $string2 = "C:\\%s\\qeriuwjhrf" ascii
        $string3 = "WANACRY!" ascii
        $string4 = "cmd.exe /c \"%s\""
        $string5 = "icacls . /grant Everyone:"
        $string6 = ".wnry"
        $string7 = "13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94"
        $string8 = "12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw"
        $string9 = "115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn"
        $PE_byte = "MZ"

    condition:
        // Fill out the conditions that must be met to identify the binary
        $PE_byte at 0 and
        ($string1 and $string2 and $string3 and $string4 and $string5 and
$string6 and $string7 and $string8 and $string9) or
        $PE_byte at 0 and
        ($string5 and $string6 and $string7 and $string8 and $string9)
}
```

High Level Technical Summary

When *Ransomware.wannacry.exe* is executed with administrative privileges the malware checks if it can make a successful callback to the URL *hxxp://www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com/* and if the callback is successful the malware is not executed. If on the other hand there is no successful response the malware proceeds to unpack its components.



Ransomware.wannacry.exe will try to identify other hosts on the network and infect them as well by connecting to systems that allow connections on the TCP port 445, which is typically used for SMB. If no hosts are identified the rest of the malware is unpacked inside C:\ProgramData\bqtztzryebik717. From there Tasksche.exe is executed which enumerates the system and encrypts user files that are related to business, productivity or entertainment.

In the following sections of Static and Dynamic analysis all results are documented and reported.

Static Analysis

The following interesting strings have been identified using floss -n 7:

First batch of suspicious strings include the callback URL and the first executable to be unpacked.

hxxp://www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com

```
427 C:\%s\qeriuwjhrf
428 C:\%s\%s
429 WINDOWS
430 tasksche.exe
431 CloseHandle
432 WriteFile
433 CreateFileA
434 CreateProcessA
435 http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
436 !This program cannot be run in DOS mode.
437 `.rdata
```

Some of the libraries used by the malware, strings that are used in the YARA rule and icacls granting everyone the full access to all files.

```
571 MSVCP60.dll
572 GetStartupInfoA
573 advapi32.dll
574 WANACRY!
575 CloseHandle
576 DeleteFileW
577 MoveFileExW
578 MoveFileW
579 ReadFile
580 WriteFile
581 CreateFileW
582 kernel32.dll
583 O|x8+^_
584 2/O-_.X8w.+
585 |~}%.15
586 Microsoft Enhanced RSA and AES Cryptographic Provider
587 CryptGenKey
588 CryptDecrypt
589 CryptEncrypt
590 CryptDestroyKey
591 CryptImportKey
592 CryptAcquireContextA
593 cmd.exe /c "%s"
594 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
595 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
596 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
597 Global\MsWinZonesCacheCounterMutexA
598 tasksche.exe
599 TaskStart
600 icacls . /grant Everyone:F /T /C /Q
601 attrib +h .
602 WNcry@2ol7
603 GetNativeSystemInfo
604 .?AVexception@@
605 incompatible version
```

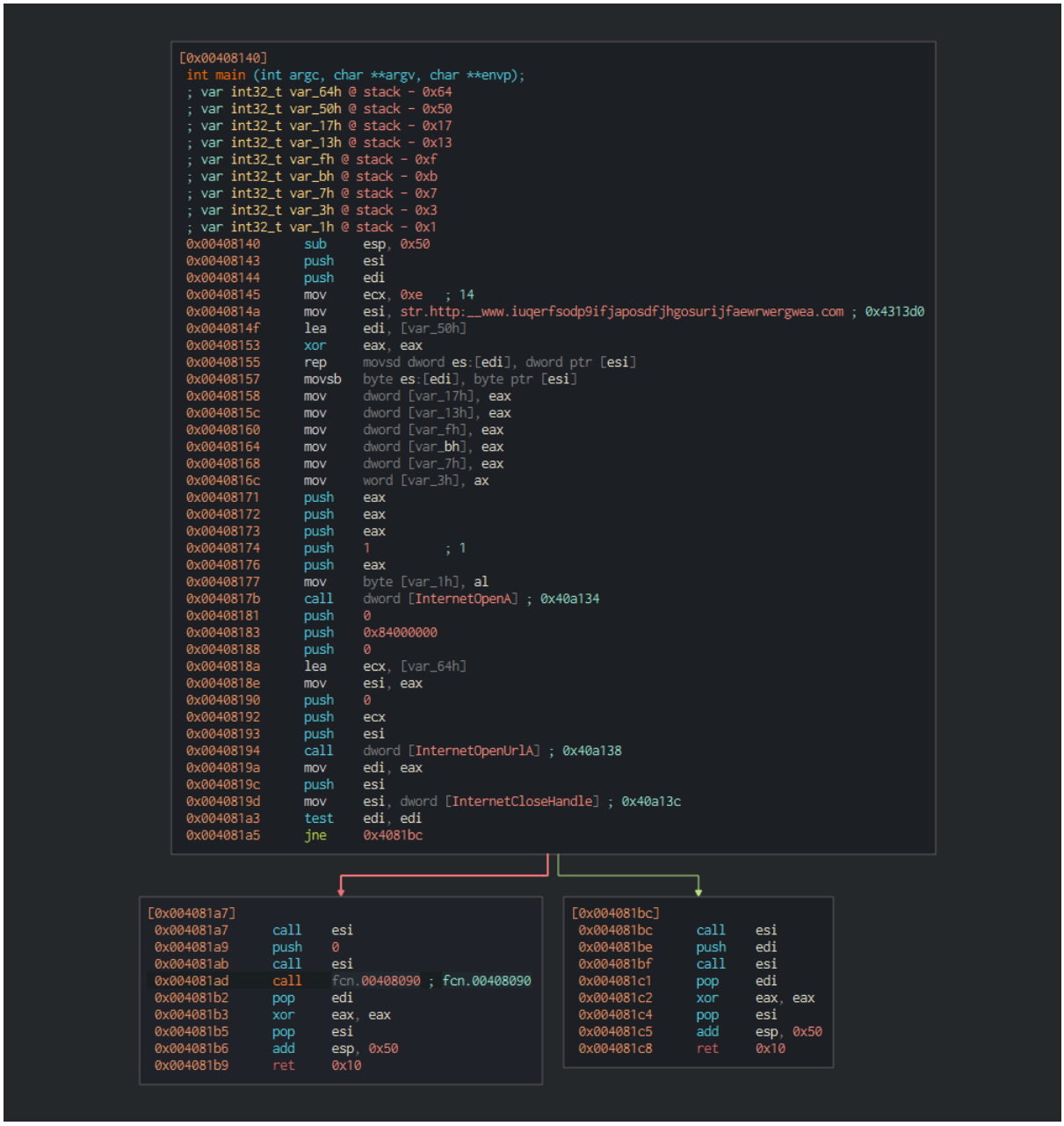
This is the list of files to be unpacked by the encryptor.

```
2885    %l?E)!o
2886    msg/m_bulgarian.wnry
2887    msg/m_chinese (simplified).wnry
2888    "t=.|Vbq-
2889    msg/m_chinese (traditional).wnry
2890    msg/m_croatian.wnry
2891    msg/m_czech.wnry
2892    msg/m_danish.wnry
2893    msg/m_dutch.wnry
2894    msg/m_english.wnry
2895    msg/m_filipino.wnry
2896    msg/m_finnish.wnry
2897    msg/m_french.wnry
2898    msg/m_german.wnry
2899    msg/m_greek.wnry
2900    msg/m_indonesian.wnry
2901    msg/m_italian.wnry
2902    msg/m_japanese.wnry
2903    msg/m_korean.wnry
2904    msg/m_latvian.wnry
2905    msg/m_norwegian.wnry
2906    msg/m_polish.wnry
2907    msg/m_portuguese.wnry
2908    msg/m_romanian.wnry
2909    msg/m_russian.wnry
2910    msg/m_slovak.wnry
2911    msg/m_spanish.wnry
2912    msg/m_swedish.wnry
2913    msg/m_turkish.wnry
2914    msg/m_vietnamese.wnry
2915    taskdl.exe
2916    taskse.exe
```

Advanced Static Analysis

Adding the malware in cutter, we were able to identify the main functions and logic of the initial program.

Main:



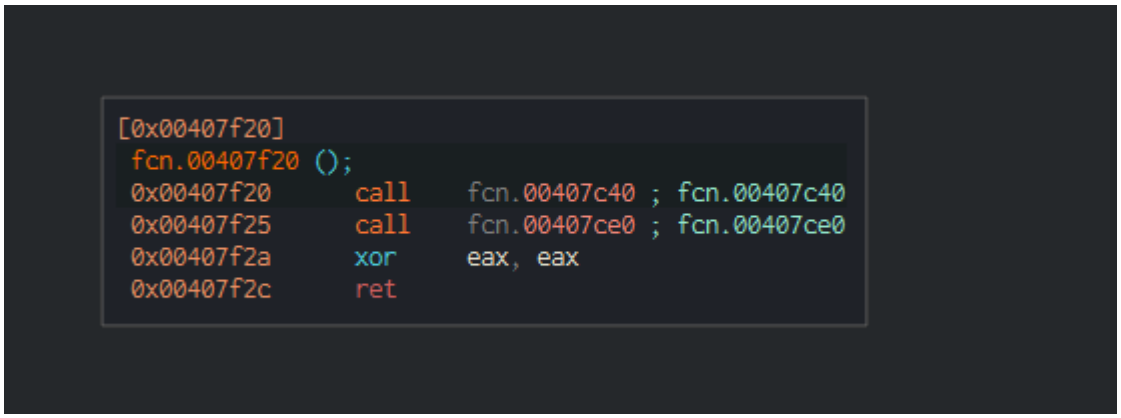
Fnc00408090 - No available callback:

Calls GetModuleFineNameA, then OpenSCManagerA then OpenServiceA and after that fcn.00407fa0

And finally, StarServiceCtrlDispacherA and returns to the main function.

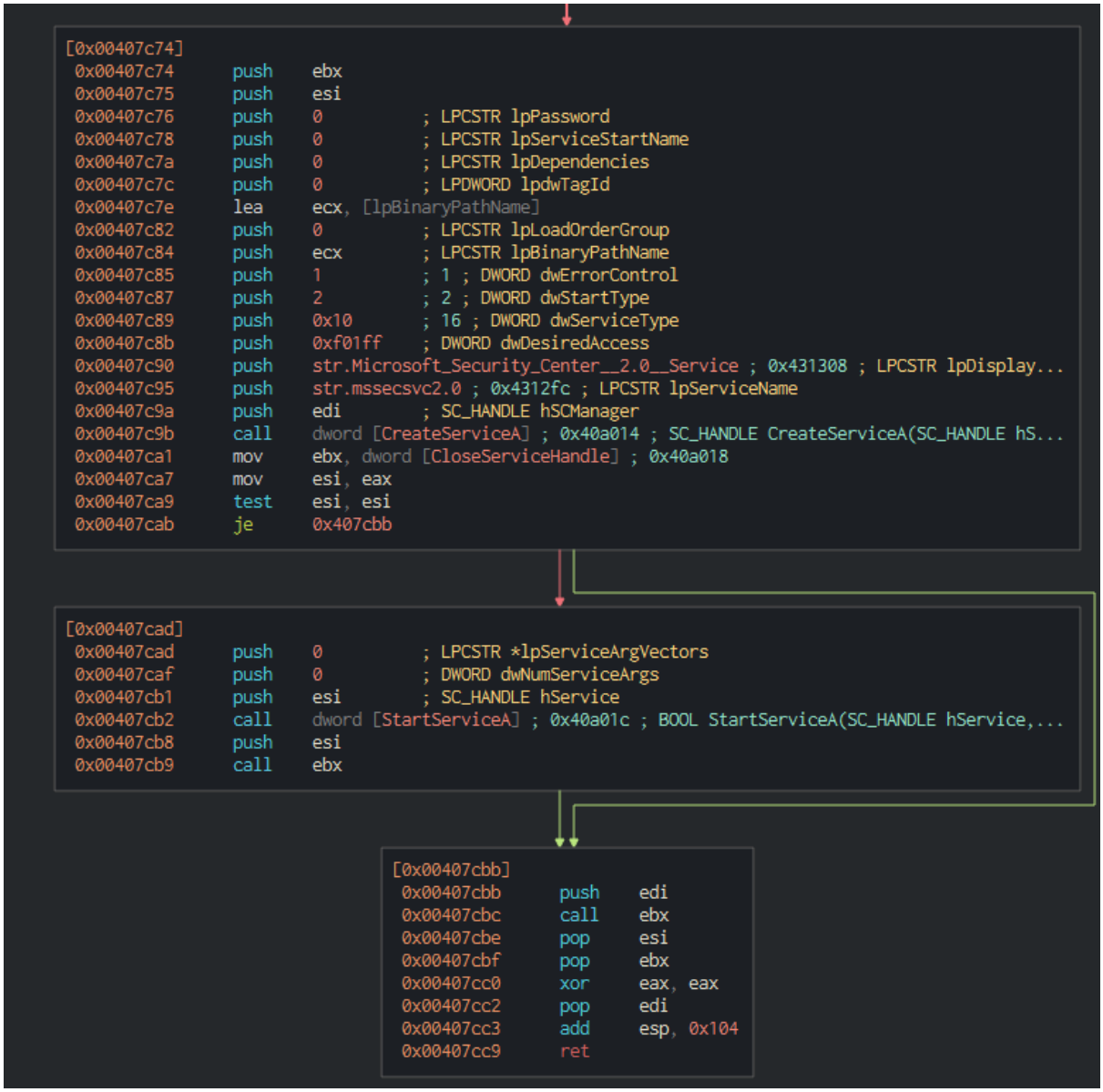
Ransomware.Wannacry Malware
June 2023
V1.0

Otherwise calls function 00407f20

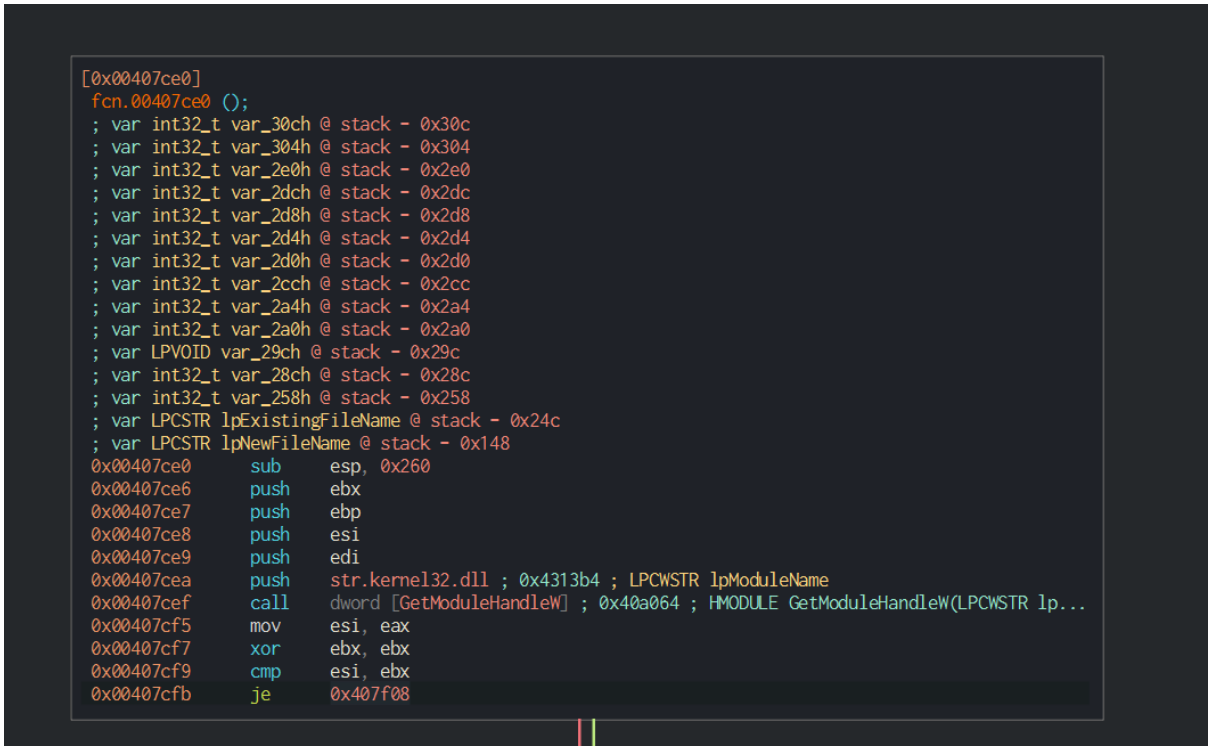


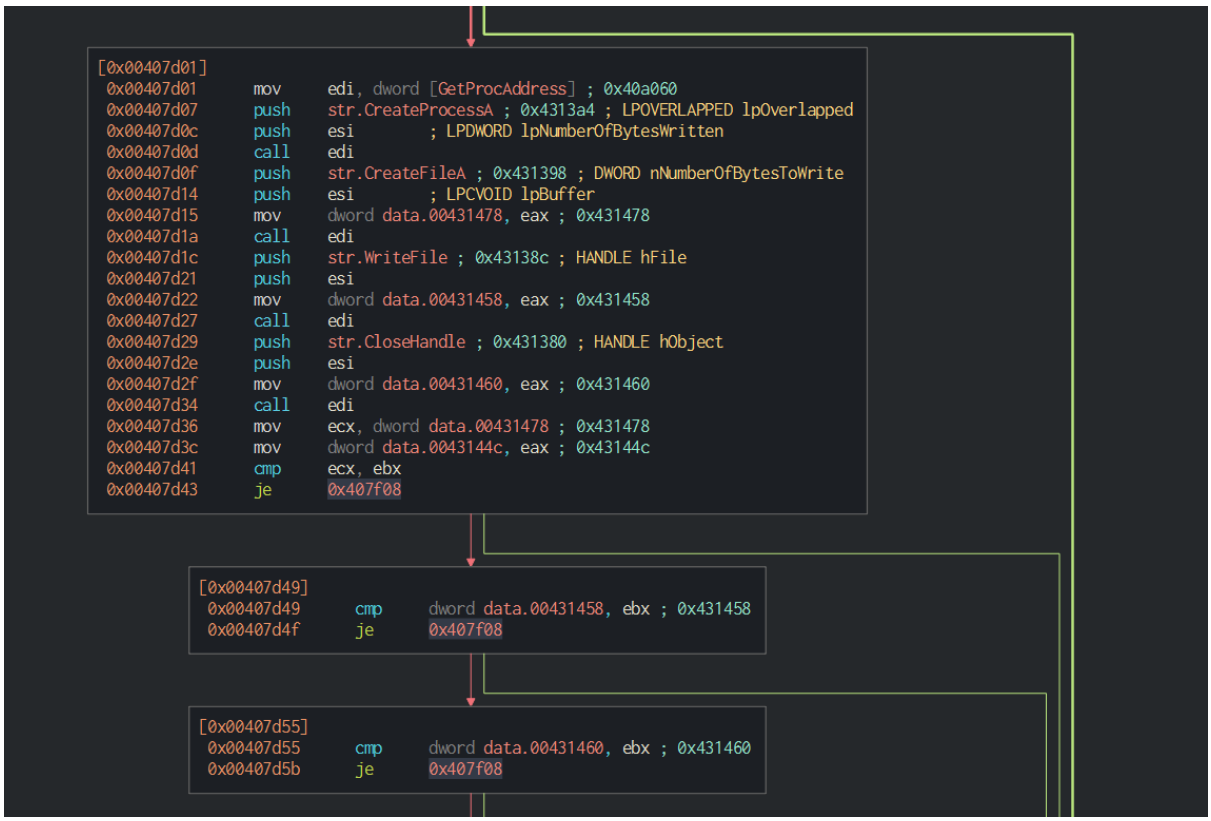
Fcn.00407c40

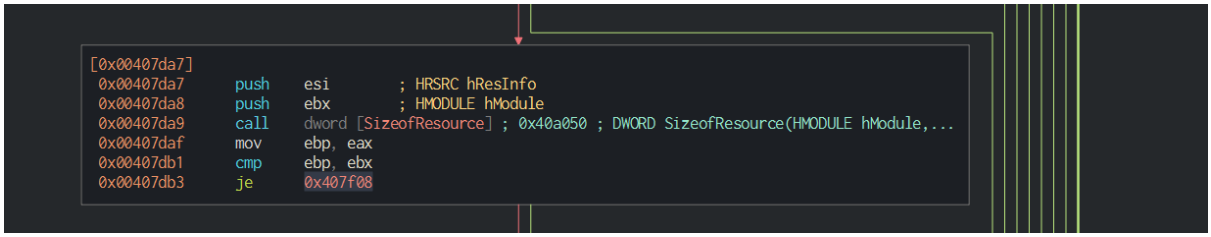
Calls OpenSCManagerA and on successful call jumps to create a service with the following characteristics on the system

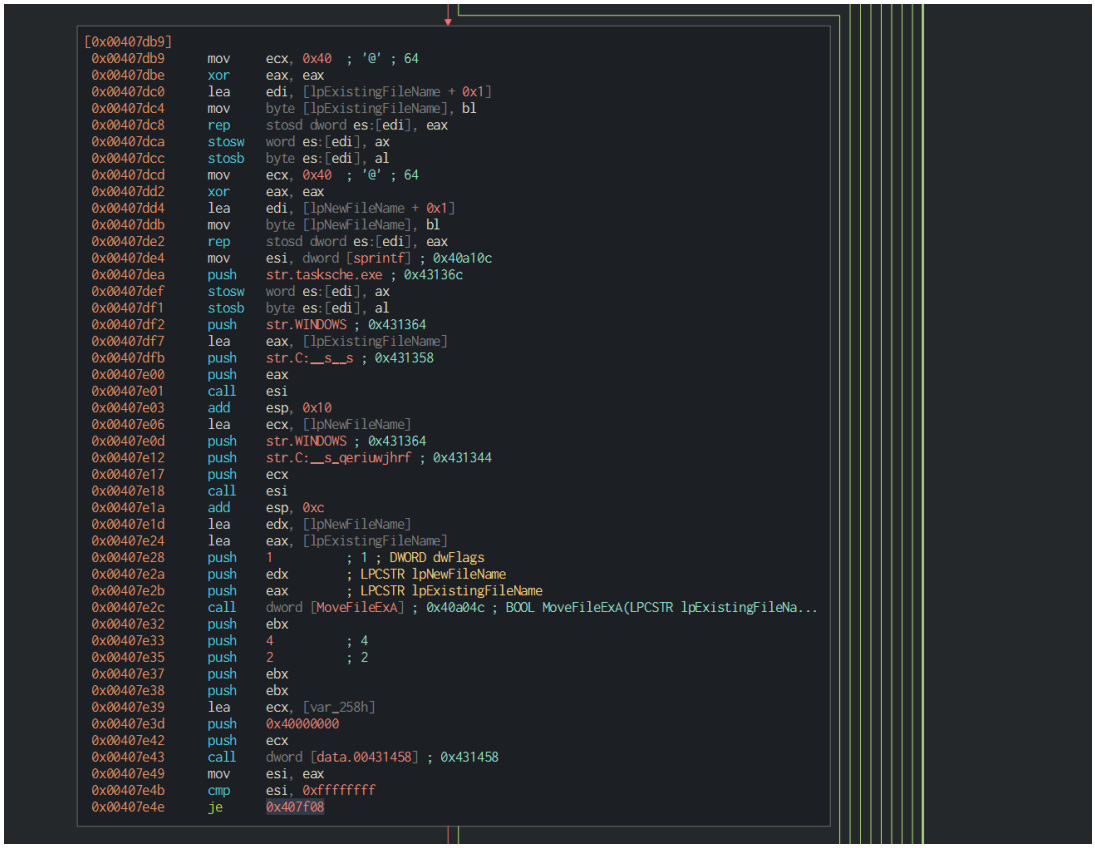


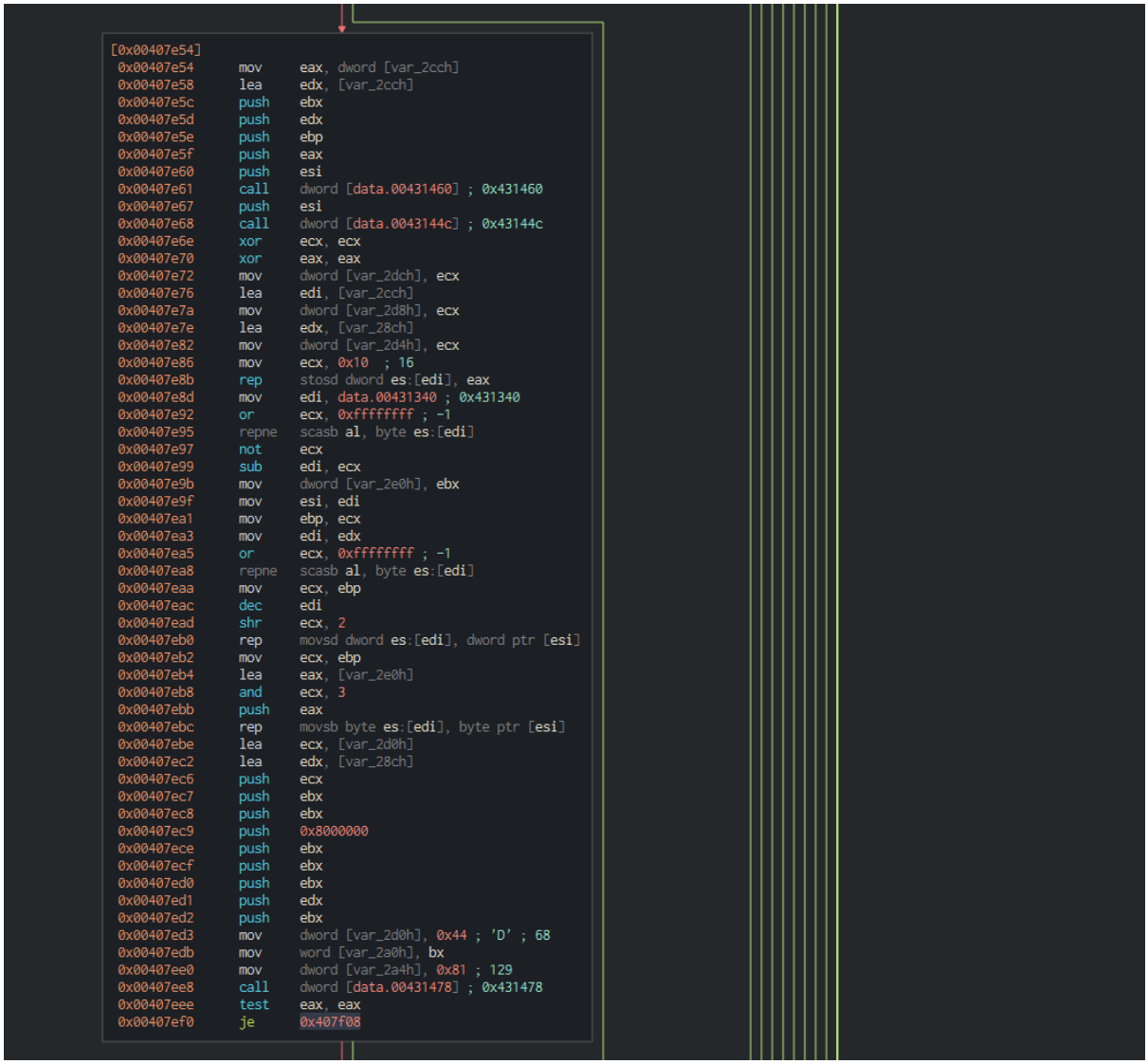
Fcn.00407ce0 - the encryptor:

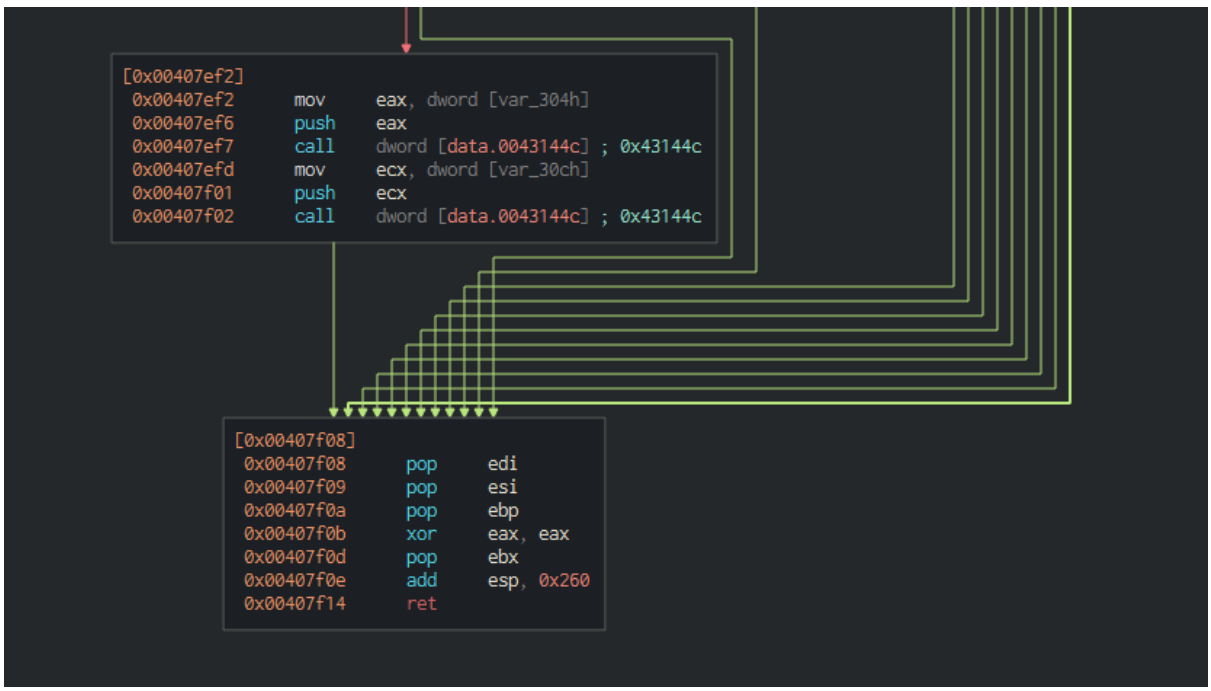






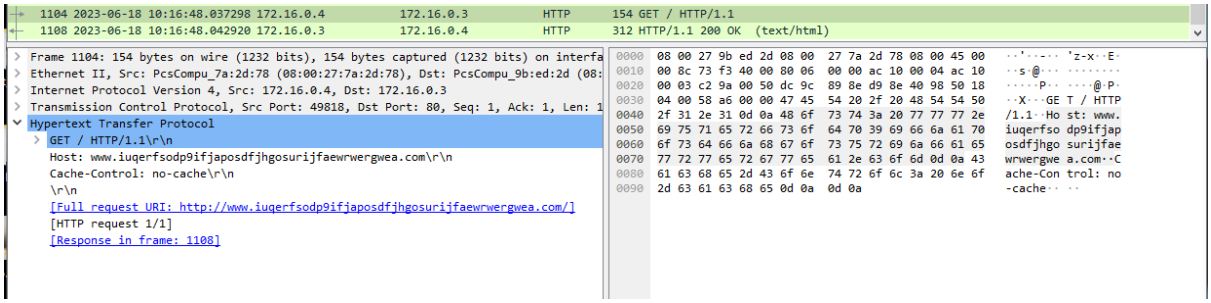






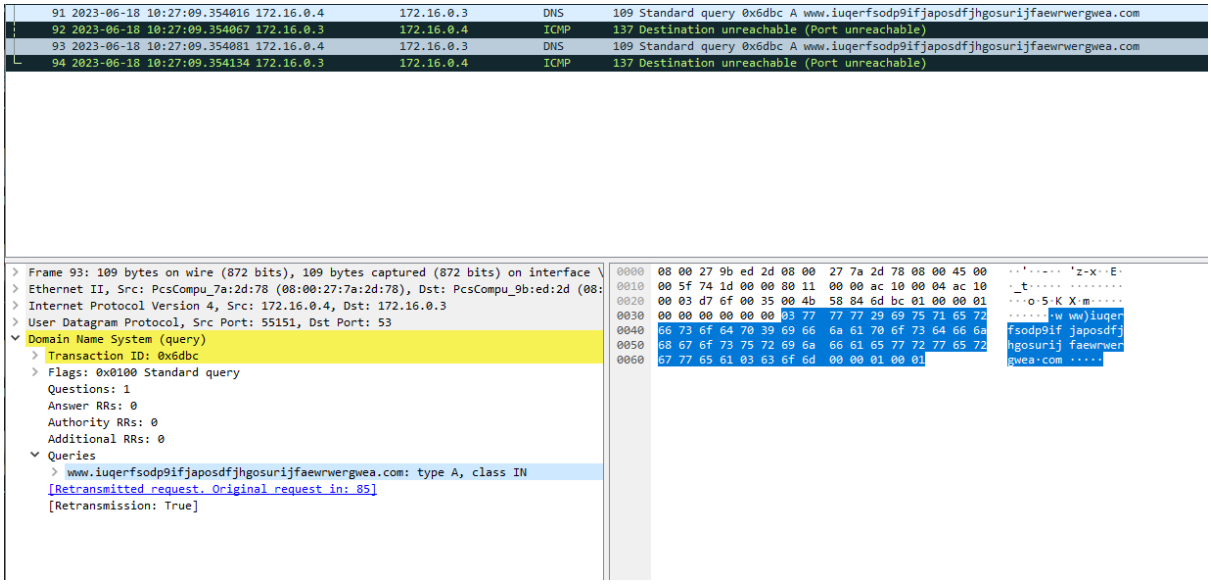
Dynamic Analysis

When executed with user privileges and inetsim the program makes a call to the URL hxxp://www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com/ we found earlier in static analysis and closes:

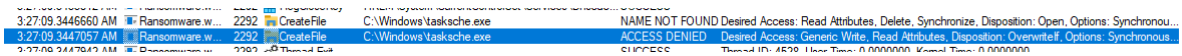


User privileges without Inetsim:

DNS request to the same url:

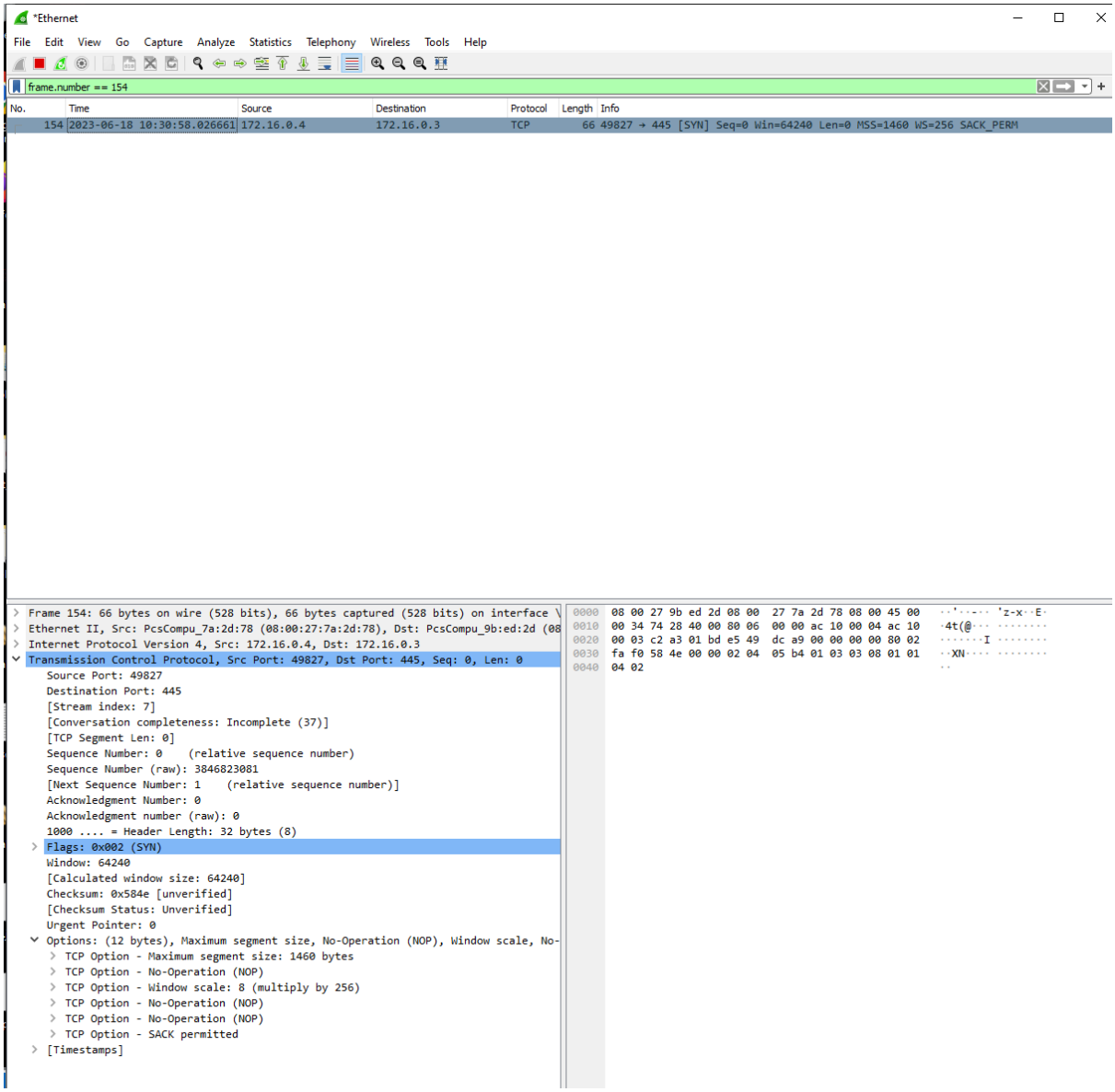


Attempts to create a file in C:\Windows named taskche.exe, fails and exits.

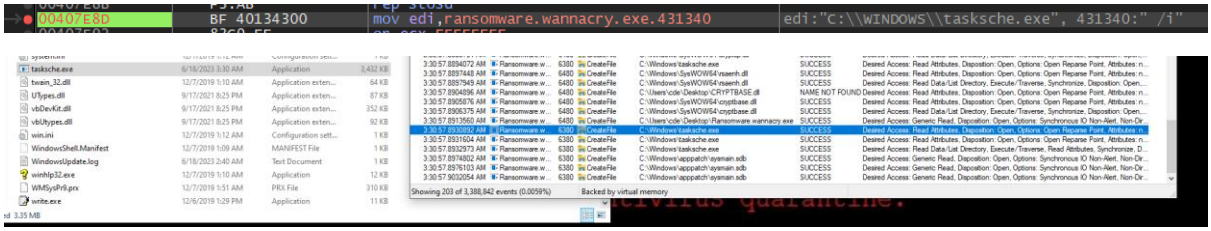


With admin Privileges:

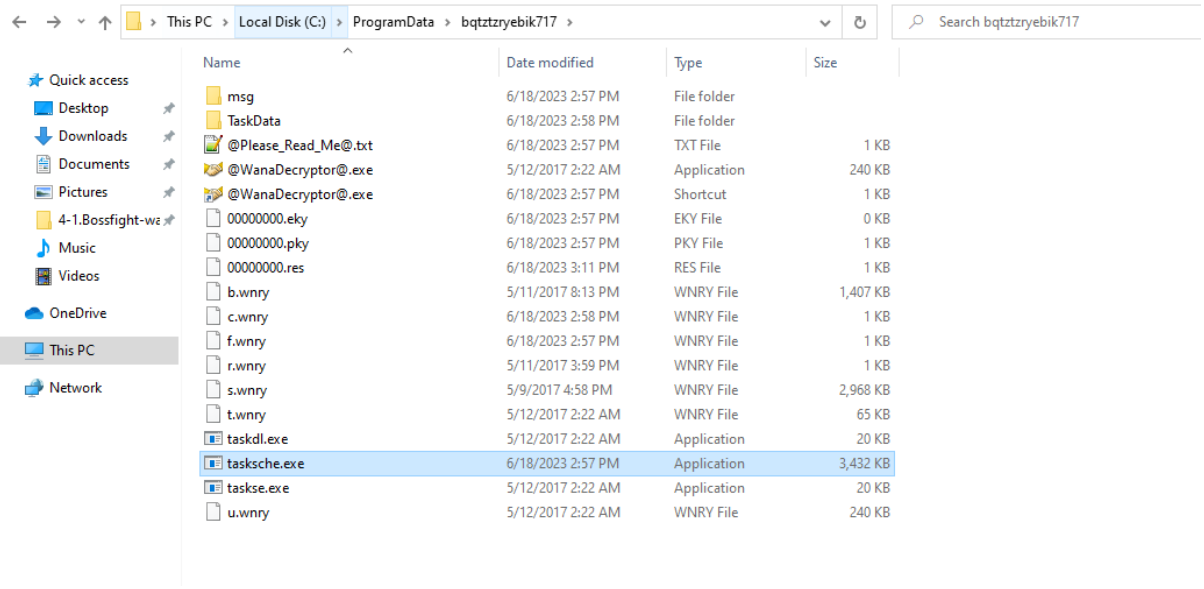
The program executes and encrypts user files. Performs ARP request to the network to find live hosts. Against the only other live host on the network, it attempts to connect to TCP port 445



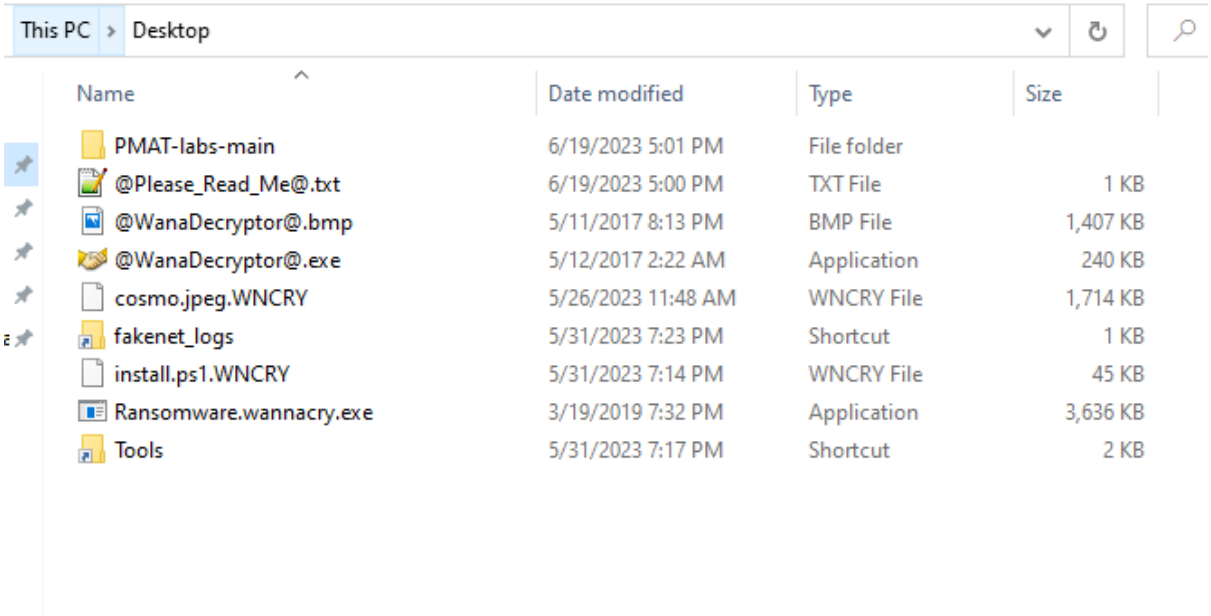
Creates an executable named taskche.exe in C:\ProgramData\bqtztzryebik717 along with the rest of the files and executes the encryptor with the command C:\Windows\Taskche.exe /i.



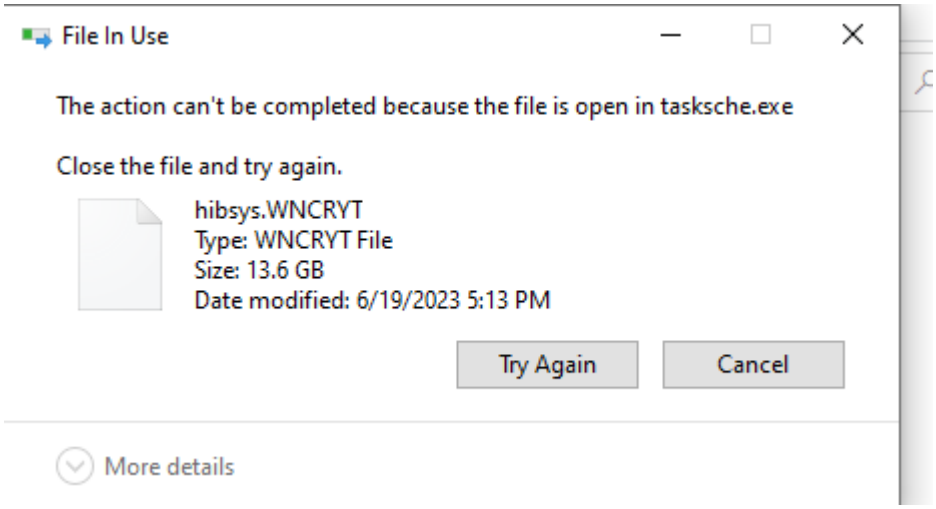
In this part we confirm that the strings we discovered earlier during the part of static analysis were actually file names.



Shortly after the execution, user files are encrypted and the suffix ".WNCRY" is appended to them, the background changes to the ransomware note and the files seen in the picture below are created on the Desktop.



Another finding that after the system encryption the file hibsys.WNCRYT is generated under the C:\Windows\Temp folder that is constantly used by tasksche.exe and grows in size. No further analysis was performed on that file.



During the analysis process it was confirmed that the malware encrypts the following type of files:

1. 7zip
2. Txt
3. Jpeg
4. Ps1

It is confirmed that the malware does not encrypt files with the following suffixes:

1. Exe
2. Md
3. Dat
4. Dll
5. Tmp
6. config
7. No suffix
8. Files under C:\Windows
9. Files under C:\Program Files
10. Files under C:\Program Files (x86)