

Oops, your files have been encrypted!

English

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

Payment will be raised on
6/22/2023 16:16:08
Time Left
02:23:51:25

Your files will be lost on
6/26/2023 16:16:08
Time Left
06:23:51:25

[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)

Send \$300 worth of bitcoin to this address:

 **bitcoin**
ACCEPTED HERE

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Malware Analysis Report

Ransomware.Wannacry Malware

June 2023 | Theodoros Vergos "cde" | v1.0

Table of Contents

Executive Report	3
YARA Rule	4
High Level Technical Summary	5
Static Analysis.....	6
Advanced Static Analysis.....	8
Main:	8
Fnc00408090 - No available callback:	9
Fcn.00407c40	10
Fcn.00407ce0 - the encryptor:	12
Dynamic Analysis	15

Executive Report

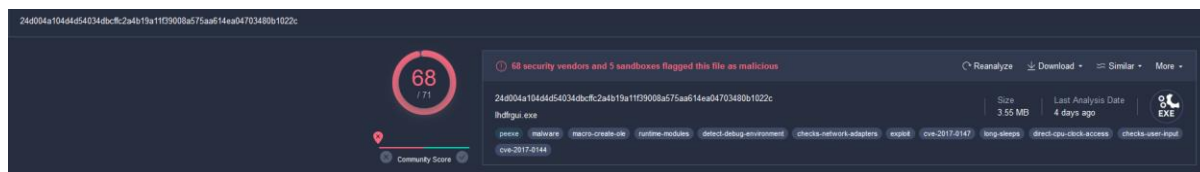
Name	Ransomware.wannacry.exe
MD5:	db349b97c37d22f5ea1d1841e3c89eb4
SHA1:	e889544aff85ffaf8b0d0da705105dee7c97fe26
SHA256:	24d004a104d4d54034dbccfc2a4b19a11f39008a575aa614ea04703480b1022c
Architecture:	x86
Signature:	Microsoft Visual C++ v6.0

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[.jiuqerfsodp9iffjaposdfjhgosurijfaewrwegwea[.]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[.jiuqerfsodp9iffjaposdfjhgosurijfaewrwegwea[.]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.

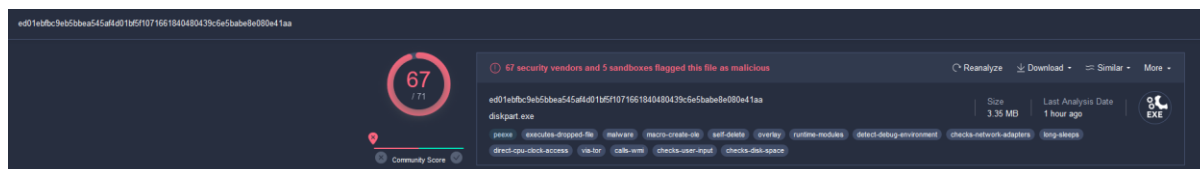
Currently, this malware has **68/71** vendors detections in *virustotal.com*



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.

Ransomware.Wannacry Malware
June 2023
V1.0

<https://t.me/learningnets>

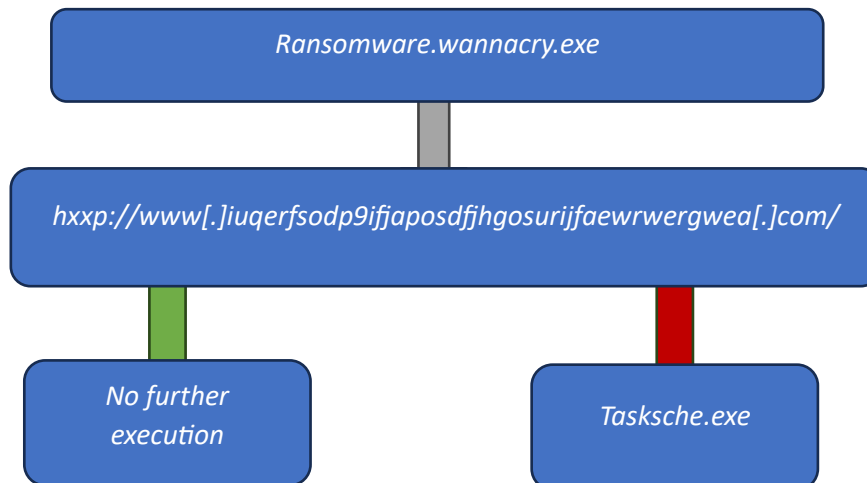
YARA Rule

```
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.iuqerfsodp9ifjaposdfjhgosurijfaewrwegwea.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 = "115p7UMMngo1pMvkhHijcRdfJNXj6LrLn"  
        $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[.]jiuqerfsodp9ifjaposdfjhgosurijfaewrwegwea[.]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\bqztzryebik717*. 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[.]iugerfsodp9ifjaposdfjhgosurijfaewrwegwea[.]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.iugerfsodp9ifjaposdfjhgosurijfaewrwegwea.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.

```

570 _contloapi
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 0|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 115p7UMMngo1pMvkvHijcRdfJNXj6LrLn
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@2017
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:

```

[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.iuqerfsodp9ifjaposdfjhgosurijfaewrgwea.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

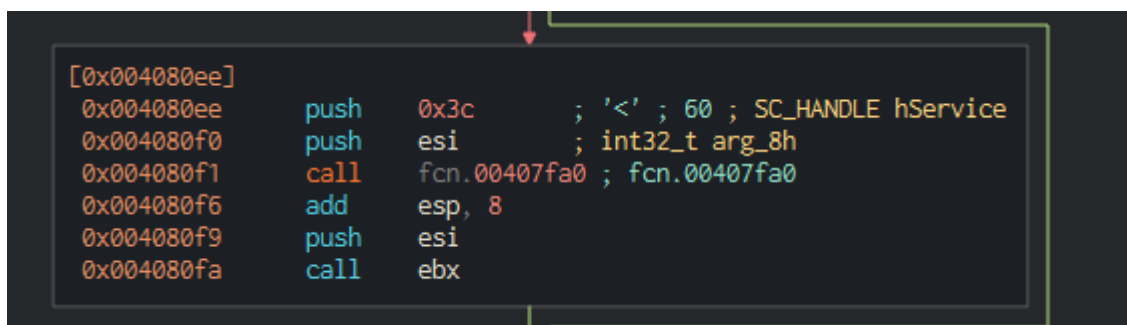
[0x004081bc]
0x004081bc  call   esi
0x004081be  push   edi
0x004081bf  call   esi
0x004081c1  pop    edi
0x004081c2  xor    eax, eax
0x004081c4  pop    esi
0x004081c5  add    esp, 0x50
0x004081c8  ret    0x10

```

Fnc00408090 - No available callback:



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



And finally, StarServiceCtrlDispatcherA and returns to the main function.

Otherwise calls function 00407f20

```
[0x00407f20]
fcn.00407f20 ();
0x00407f20 call fcn.00407c40 ; fcn.00407c40
0x00407f25 call fcn.00407ce0 ; fcn.00407ce0
0x00407f2a xor eax, eax
0x00407f2c ret
```

Fcn.00407c40

```
[0x00407c40]
fcn.00407c40 ();
; var LPCSTR lpBinaryPathName @ stack - 0x110
0x00407c40 sub esp, 0x104
0x00407c46 lea eax, [esp]
0x00407c4a push edi
0x00407c4b push data.0070f760 ; 0x70f760
0x00407c50 push str.s__m_security ; 0x431330 ; const char *format
0x00407c55 push eax ; char *s
0x00407c56 call dword [sprintf] ; 0x40a10c ; int sprintf(char *s, const char *format, va...
0x00407c5c add esp, 0xc
0x00407c5f push 0xf003f ; '?' ; DWORD dwDesiredAccess
0x00407c64 push 0 ; LPCSTR lpDatabaseName
0x00407c68 push 0 ; LPCSTR lpMachineName
0x00407c6b call dword [OpenSCManagerA] ; 0x40a010 ; SC_HANDLE OpenSCManagerA(LPCSTR lpMac...
0x00407c6e mov edi, eax
0x00407c70 test edi, edi
0x00407c72 je 0x407cca

[0x00407c74]
0x00407c74 push ebx
0x00407c75 push esi
0x00407c76 push 0 ; LPCSTR lpPassword
0x00407c78 push 0 ; LPCSTR lpServiceStartName
0x00407c7a push 0 ; LPCSTR lpDependencies
0x00407c7c push 0 ; LPWORD lpTragId
0x00407c7e lea ecx, [lpBinaryPathName]
0x00407c82 push 0 ; LPCSTR lpLoadOrderGroup
0x00407c84 push ecx ; LPCSTR lpBinaryPathName
0x00407c85 push 1 ; 1 ; DWORD dwErrorControl
0x00407c87 push 2 ; 2 ; DWORD dwStartType
0x00407c89 push 0x10 ; 16 ; DWORD dwServiceType
0x00407c8b push 0xf01ff ; DWORD dwDesiredAccess
0x00407c90 push str.Microsoft_Security_Center_2.0__Service ; 0x431308 ; LPCSTR lpDisplay...
0x00407c95 push str.mssecsv2.0 ; 0x4312fc ; LPCSTR lpServiceName
0x00407c9a push edi ; SC_HANDLE hSCManager
0x00407c9b call dword [CreateServiceA] ; 0x40a014 ; SC_HANDLE CreateServiceA(SC_HANDLE hS...
0x00407ca1 mov ebx, dword [CloseServiceHandle] ; 0x40a018
0x00407ca7 mov esi, eax
0x00407ca9 test esi, esi
0x00407cab je 0x407cbb

[0x00407cad]
0x00407cad push 0 ; LPCSTR *lpServiceArgVectors
0x00407caf push 0 ; DWORD dwNumServiceArgs
0x00407cb1 push esi ; SC_HANDLE hService
0x00407cb2 call dword [StartServiceA] ; 0x40a01c ; BOOL StartServiceA(SC_HANDLE hService,...
0x00407cb8 push esi
0x00407cb9 call ebx

[0x00407cbb]
0x00407cbb push edi
0x00407cbb call ebx
0x00407cbe pop esi
0x00407cbf pop ebx
0x00407cc0 xor eax, eax
0x00407cc2 pop edi
0x00407cc3 add esp, 0x104
0x00407cc9 ret

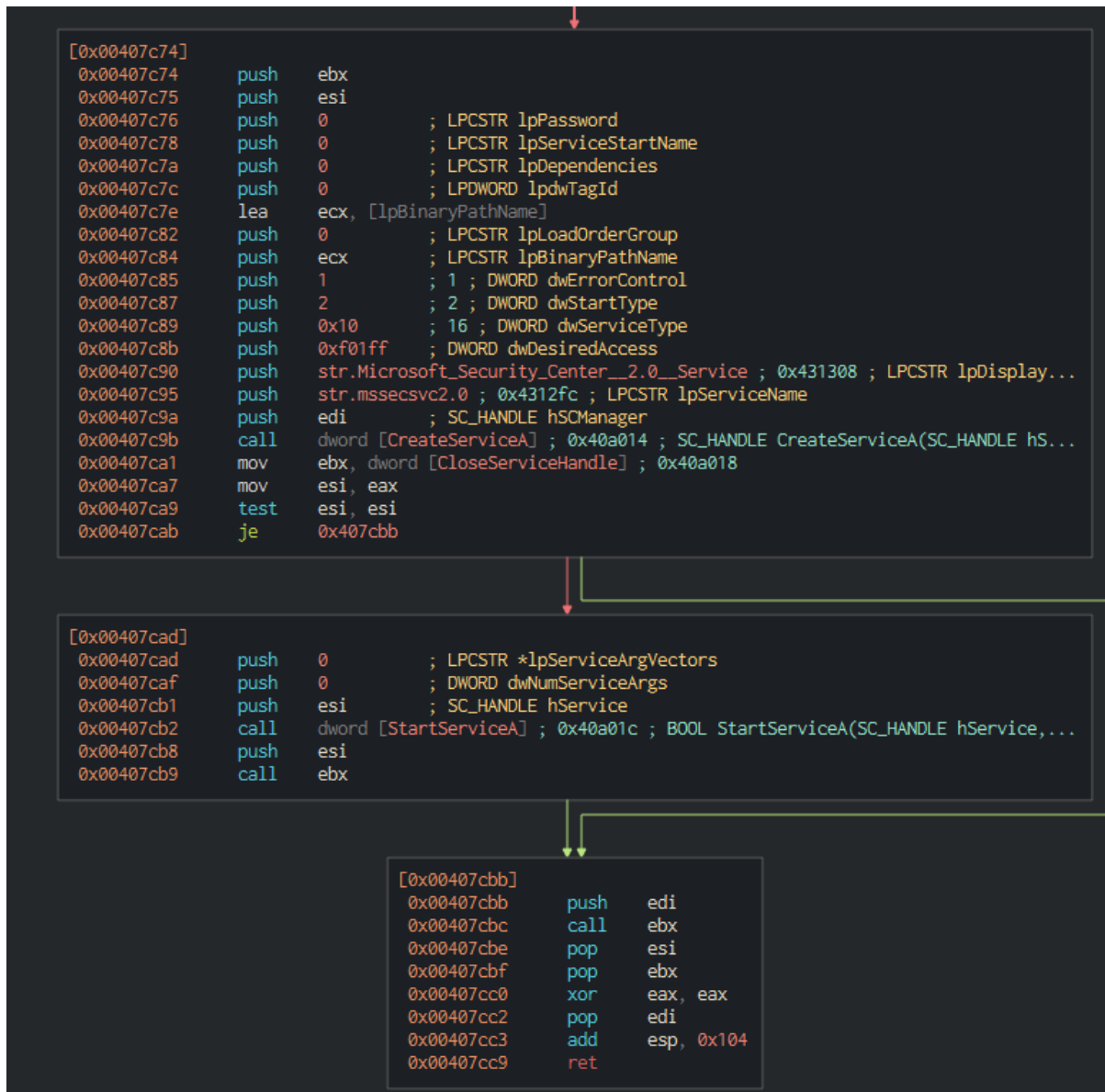
[0x00407cca]
0x00407cca xor eax, eax
0x00407ccc pop edi
0x00407ccd add esp, 0x104
0x00407cd3 ret
```

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

Ransomware.Wannacry Malware

June 2023

V1.0



Fcn.00407ce0 - the encryptor:

```
[0x00407ce0]
fcn.00407ce0 ();
; var int32_t var_30ch @ stack - 0x30c
; var int32_t var_304h @ stack - 0x304
; var int32_t var_2e0h @ stack - 0x2e0
; var int32_t var_2dch @ stack - 0x2dc
; var int32_t var_2d8h @ stack - 0x2d8
; var int32_t var_2d4h @ stack - 0x2d4
; var int32_t var_2d0h @ stack - 0x2d0
; var int32_t var_2cch @ stack - 0x2cc
; var int32_t var_2a4h @ stack - 0x2a4
; var int32_t var_2a0h @ stack - 0x2a0
; var LPVOID var_29ch @ stack - 0x29c
; var int32_t var_28ch @ stack - 0x28c
; var int32_t var_258h @ stack - 0x258
; var LPCWSTR lpExistingFileName @ stack - 0x24c
; var LPCWSTR lpNewFileName @ stack - 0x148
0x00407ce0 sub esp, 0x260
0x00407ce6 push ebx
0x00407ce7 push ebp
0x00407ce8 push esi
0x00407ce9 push edi
0x00407cea push str.kernel32.dll ; 0x4313b4 ; LPCWSTR lpModuleName
0x00407cef call dword [GetModuleHandleW] ; 0x40a064 ; HMODULE GetModuleHandleW(LPCWSTR lp...
0x00407cf5 mov esi, eax
0x00407cf7 xor ebx, ebx
0x00407cf9 cmp esi, ebx
0x00407cfb je 0x407f08
```

```
[0x00407d01]
0x00407d01 mov edi, dword [GetProcAddress] ; 0x40a060
0x00407d07 push str.CreateProcessA ; 0x4313a4 ; LPOVERLAPPED lpOverlapped
0x00407d0c push esi ; LPDWORD lpNumberOfBytesWritten
0x00407d0d call edi
0x00407d0f push str.CreateFileA ; 0x431398 ; DWORD nNumberOfBytesToWrite
0x00407d14 push esi ; LPCVOID lpBuffer
0x00407d15 mov dword data.00431478, eax ; 0x431478
0x00407d1a call edi
0x00407d1c push str.WriteFile ; 0x43138c ; HANDLE hFile
0x00407d21 push esi
0x00407d22 mov dword data.00431458, eax ; 0x431458
0x00407d27 call edi
0x00407d29 push str.CloseHandle ; 0x431380 ; HANDLE hObject
0x00407d2e push esi
0x00407d2f mov dword data.00431460, eax ; 0x431460
0x00407d34 call edi
0x00407d36 mov ecx, dword data.00431478 ; 0x431478
0x00407d3c mov dword data.0043144c, eax ; 0x43144c
0x00407d41 cmp ecx, ebx
0x00407d43 je 0x407f08
```

```
[0x00407d49]
0x00407d49 cmp dword data.00431458, ebx ; 0x431458
0x00407d4f je 0x407f08
```

```
[0x00407d55]
0x00407d55 cmp dword data.00431460, ebx ; 0x431460
0x00407d5b je 0x407f08
```



```

[0x00407e54]
0x00407e54  mov     eax, dword [var_2cch]
0x00407e58  lea    edx, [var_2cch]
0x00407e5c  push   ebx
0x00407e5d  push   edx
0x00407e5e  push   ebp
0x00407e5f  push   eax
0x00407e60  push   esi
0x00407e61  call   dword [data.00431460] ; 0x431460
0x00407e67  push   esi
0x00407e68  call   dword [data.0043144c] ; 0x43144c
0x00407e6e  xor    ecx, ecx
0x00407e70  xor    eax, eax
0x00407e72  mov    dword [var_2dch], ecx
0x00407e76  lea    edi, [var_2cch]
0x00407e7a  mov    dword [var_2d8h], ecx
0x00407e7e  lea    edx, [var_28ch]
0x00407e82  mov    dword [var_2d4h], ecx
0x00407e86  mov    ecx, 0x10 ; 16
0x00407e8b  rep    stosd dword es:[edi], eax
0x00407e8d  mov    edi, data.00431340 ; 0x431340
0x00407e92  or     ecx, 0xffffffff ; -1
0x00407e95  repne scasb al, byte es:[edi]
0x00407e97  not    ecx
0x00407e99  sub    edi, ecx
0x00407e9b  mov    dword [var_2e0h], ebx
0x00407e9f  mov    esi, edi
0x00407ea1  mov    ebp, ecx
0x00407ea3  mov    edi, edx
0x00407ea5  or     ecx, 0xffffffff ; -1
0x00407ea8  repne scasb al, byte es:[edi]
0x00407eaa  mov    ecx, ebp
0x00407eac  dec    edi
0x00407ead  shr    ecx, 2
0x00407eb0  rep    movsd dword es:[edi], dword ptr [esi]
0x00407eb2  mov    ecx, ebp
0x00407eb4  lea    eax, [var_2e0h]
0x00407eb8  and    ecx, 3
0x00407ebb  push   eax
0x00407ebc  rep    movsb byte es:[edi], byte ptr [esi]
0x00407ebe  lea    ecx, [var_2d0h]
0x00407ec2  lea    edx, [var_28ch]
0x00407ec6  push   ecx
0x00407ec7  push   ebx
0x00407ec8  push   ebx
0x00407ec9  push   0x80000000
0x00407ece  push   ebx
0x00407ecf  push   ebx
0x00407ed0  push   ebx
0x00407ed1  push   edx
0x00407ed2  push   ebx
0x00407ed3  mov    dword [var_2d0h], 0x44 ; 'D' ; 68
0x00407edb  mov    word [var_2a0h], bx
0x00407ee0  mov    dword [var_2a4h], 0x81 ; 129
0x00407ee8  call   dword [data.00431478] ; 0x431478
0x00407eee  test   eax, eax
0x00407ef0  je     0x407f08

```

```

[0x00407ef2]
0x00407ef2  mov    eax, dword [var_304h]
0x00407ef6  push   eax
0x00407ef7  call   dword [data.0043144c] ; 0x43144c
0x00407efd  mov    ecx, dword [var_30ch]
0x00407f01  push   ecx
0x00407f02  call   dword [data.0043144c] ; 0x43144c

[0x00407f08]
0x00407f08  pop    edi
0x00407f09  pop    esi
0x00407f0a  pop    ebp
0x00407f0b  xor    eax, eax
0x00407f0d  pop    ebx
0x00407f0e  add    esp, 0x260
0x00407f14  ret

```

Dynamic Analysis

When executed with user privileges and inetsim the program makes a call to the URL `hxxp://www[.]iugerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com/` we found earlier in static analysis and closes:

```

1104 2023-06-18 10:16:48.037298 172.16.0.4 172.16.0.3 HTTP 154 GET / HTTP/1.1
1108 2023-06-18 10:16:48.042920 172.16.0.3 172.16.0.4 HTTP 312 HTTP/1.1 200 OK (text/html)

> Frame 1104: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) on interface
> Ethernet II, Src: PcsCompu_7a:2d:78 (08:00:27:7a:2d:78), Dst: PcsCompu_9b:ed:2d (08:00:27:9b:ed:2d)
> Internet Protocol Version 4, Src: 172.16.0.4, Dst: 172.16.0.3
> Transmission Control Protocol, Src Port: 49818, Dst Port: 80, Seq: 1, Ack: 1, Len: 154
  > Hypertext Transfer Protocol
    > GET / HTTP/1.1\r\n
      Host: www.iugerfsodp9ifjaposdfjhgosurijfaewrwergwea.com\r\n
      Cache-Control: no-cache\r\n
      \r\n
      [Full request URI: http://www.iugerfsodp9ifjaposdfjhgosurijfaewrwergwea.com/]
      [HTTP request 1/1]
      [Response in frame: 1108]
  
```

User privileges without Inetsim:

DNS request to the same url:

```

91 2023-06-18 10:27:09.354016 172.16.0.4 172.16.0.3 DNS 109 Standard query 0x6dbc A www.iugerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
92 2023-06-18 10:27:09.354067 172.16.0.3 172.16.0.4 ICMP 137 Destination unreachable (Port unreachable)
93 2023-06-18 10:27:09.354081 172.16.0.4 172.16.0.3 DNS 109 Standard query 0x6dbc A www.iugerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
94 2023-06-18 10:27:09.354134 172.16.0.3 172.16.0.4 ICMP 137 Destination unreachable (Port unreachable)

> Frame 93: 109 bytes on wire (872 bits), 109 bytes captured (872 bits) on interface
> Ethernet II, Src: PcsCompu_7a:2d:78 (08:00:27:7a:2d:78), Dst: PcsCompu_9b:ed:2d (08:00:27:9b:ed:2d)
> Internet Protocol Version 4, Src: 172.16.0.4, Dst: 172.16.0.3
> User Datagram Protocol, Src Port: 55151, Dst Port: 53
  > Domain Name System (query)
    > Transaction ID: 0x6dbc
    > Flags: 0x0100 Standard query
      Questions: 1
      Answer RRs: 0
      Authority RRs: 0
      Additional RRs: 0
    > Queries
      > www.iugerfsodp9ifjaposdfjhgosurijfaewrwergwea.com: type A, class IN
        [Retransmitted request. Original request in: 85]
        [Retransmission: True]
  
```

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

```

3:27:09.344660 AM Ransomware.w... 2292 CreateFile C:\Windows\taskche.exe NAME NOT FOUND Desired Access: Read Attributes, Delete, Synchronize, Disposition: Open, Options: Synchronou...
3:27:09.344705 AM Ransomware.w... 2292 CreateFile C:\Windows\taskche.exe ACCESS DENIED Desired Access: Generic Write, Read Attributes, Disposition: Overwriteif, Options: Synchronou...
3:27:09.344707 AM Ransomware.w... 2292 CreateFile C:\Windows\taskche.exe SUCCESS Desired Access: Generic Write, Read Attributes, Disposition: Overwriteif, Options: Synchronou...

```

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

The image shows a Wireshark capture of a network packet. The packet list pane shows a single entry for frame 154, which is a SYN packet from source IP 172.16.0.4 to destination IP 172.16.0.3 on port 445. The packet details pane shows the following information:

- Frame 154: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface Ethernet II, Src: PcsCompu_7a:2d:78 (08:00:27:7a:2d:78), Dst: PcsCompu_9b:ed:2d (08:00:27:9b:ed:2d)
- Internet Protocol Version 4, Src: 172.16.0.4, Dst: 172.16.0.3
- Transmission Control Protocol, Src Port: 49827, Dst Port: 445, Seq: 0, Len: 0
 - Source Port: 49827
 - Destination Port: 445
 - [Stream index: 7]
 - [Conversation completeness: Incomplete (37)]
 - [TCP Segment Len: 0]
 - Sequence Number: 0 (relative sequence number)
 - Sequence Number (raw): 3846823081
 - [Next Sequence Number: 1 (relative sequence number)]
 - Acknowledgment Number: 0
 - Acknowledgment number (raw): 0
 - 1000 = Header Length: 32 bytes (8)
 - Flags: 0x002 (SYN)
 - Window: 64240
 - [Calculated window size: 64240]
 - Checksum: 0x584e [unverified]
 - [Checksum Status: Unverified]
 - Urgent Pointer: 0
 - Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), Window scale: 8 (multiply by 256), No-Operation (NOP), SACK permitted
 - [Timestamps]

The packet bytes pane shows the raw data of the SYN packet: 0000 08 00 27 9b ed 2d 08 00 27 7a 2d 78 08 00 45 00 40 00 34 74 28 40 00 80 06 00 00 ac 10 00 04 ac 10 00 03 c2 a3 01 bd e5 49 dc a9 00 00 00 80 02 00 30 fa f0 58 4e 00 00 02 04 05 b4 01 03 03 08 01 01 0400 04 02

Creates an executable named taskche.exe in C:\ProgramData\bqztzryebik717 along with the rest of the files and executes the encryptor with the command C:\Windows\Taskche.exe /i.

The image shows a Windows command prompt window with the following command and output:

```

C:\Windows\system32> move /y C:\ProgramData\bqztzryebik717\Taskche.exe C:\Windows\Taskche.exe /i

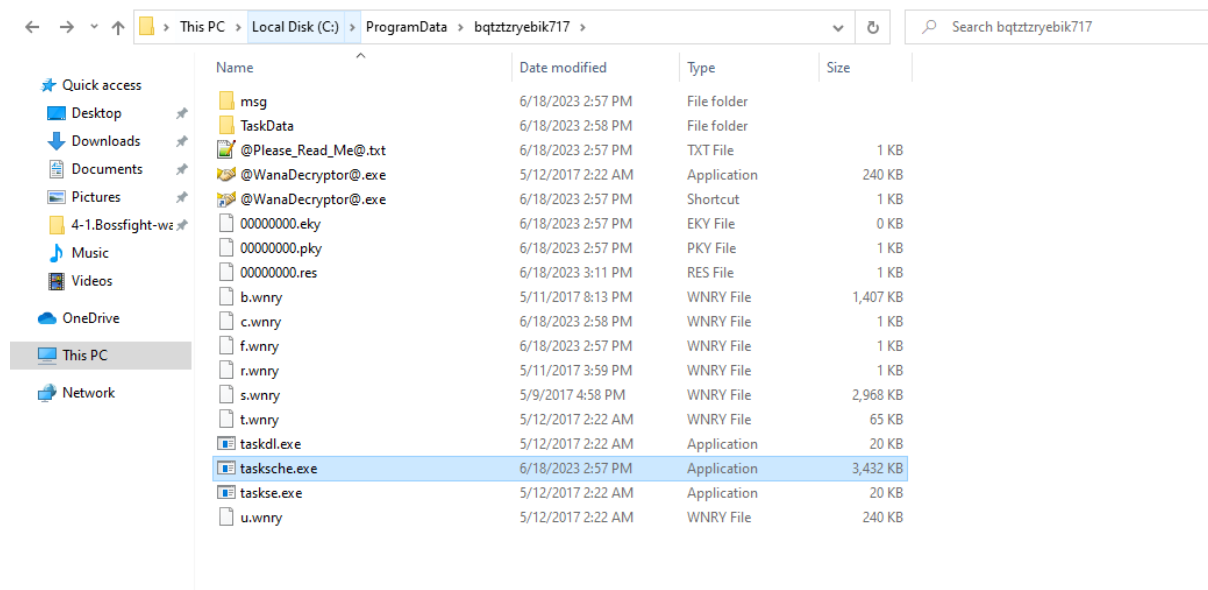
```

The command prompt also shows the execution of a command to create a taskche.exe file in the C:\ProgramData\bqztzryebik717 directory. The output shows the file was successfully created.

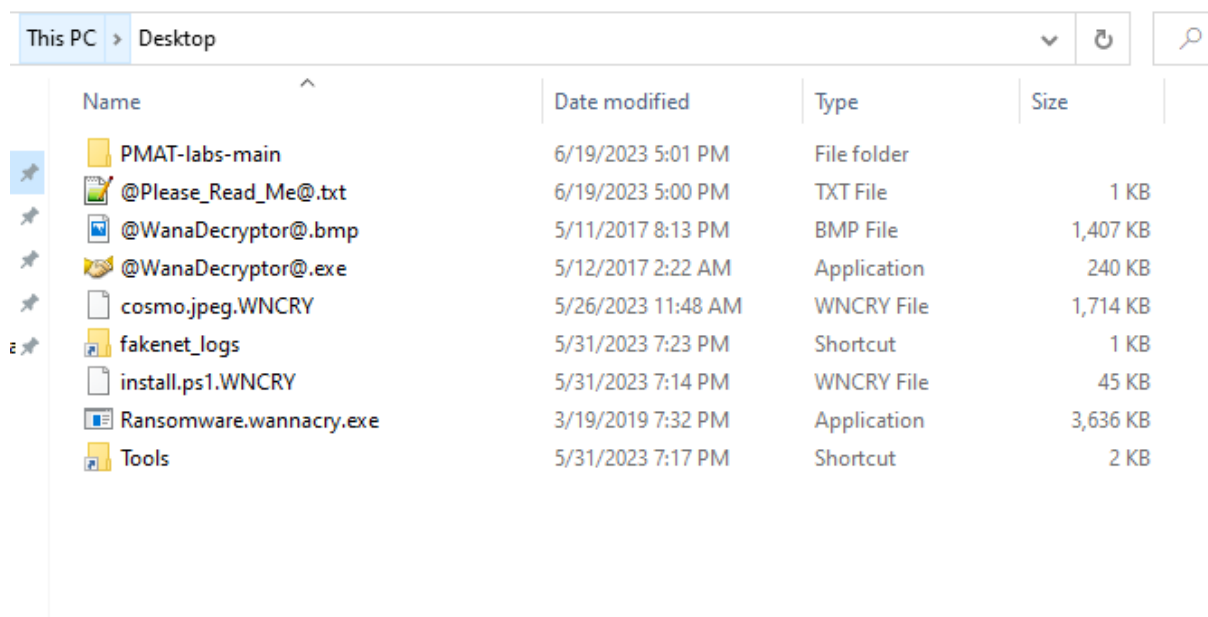
Ransomware.Wannacy Malware
June 2023
V1.0

<https://t.me/learningnets>

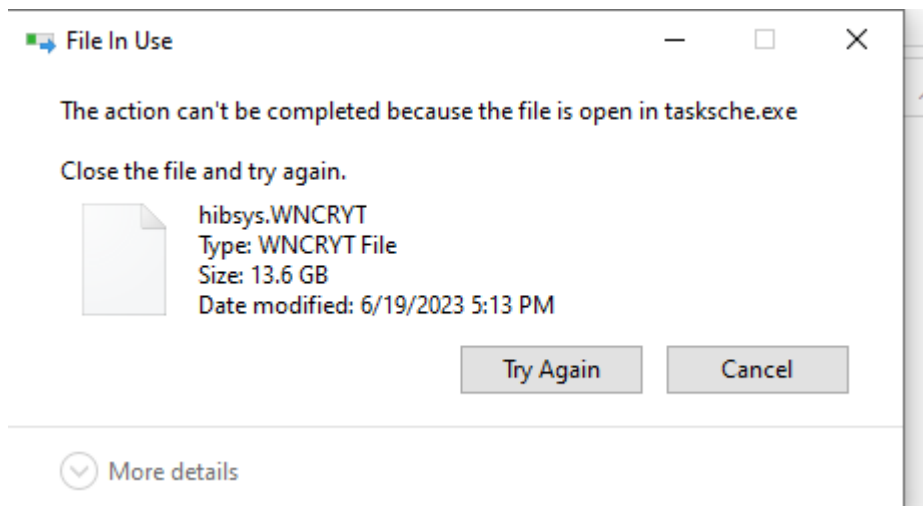
In this part we confirm that the strings we discovered earlier during the part of static analysis were actually file names.



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 hbsys.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)