

# Practical Malware Analysis & Triage

## Malware Analysis Report

### WannaCry Dropper Malware

April 2022 | Ganoes | v1.0

# Table of Contents

<b>Table of Contents .....</b>	<b>2</b>
<b>Executive Summary .....</b>	<b>3</b>
<b>High-Level Technical Summary .....</b>	<b>4</b>
<b>Malware Composition.....</b>	<b>6</b>
Ransomware.wannacry.exe .....	6
<b>Basic Static Analysis.....</b>	<b>8</b>
Strings .....	8
PE Inspection .....	11
<b>Basic Dynamic Analysis .....</b>	<b>13</b>
Kill-switch URL.....	13
Without kill-switch URL.....	13
<b>Advanced Analysis.....</b>	<b>17</b>
Failsafe check.....	17
Detection of the first run.....	18
Creation of the new service.....	19
The extraction of the tasksche.exe .....	20
<b>Indicators of Compromise.....</b>	<b>22</b>
Network Indicators .....	22
Host-based Indicators.....	23
<b>Rules &amp; Signatures.....</b>	<b>25</b>

## Executive Summary

SHA256 hash	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
-------------	--

The WannaCry dropper malware was widely spread to at least 74 countries. Infections started on May 12<sup>th</sup>, 2017. The main goal of this analysis was to get familiar with malware analysis processes. Therefore it focuses mainly on the dropper and it does not analyze the encryptor.

The dropper is written in C/C++ and it targets x32 Windows operating system. It checks the existence of hardcoded URL. If the URL exists the dropper does not do any harm to the computer. Otherwise it creates a new service named “mssecsvc2.0” and it also creates a new file “C:\Windows\tasksche.exe” which contains the payload. The “tasksche.exe” creates the randomly named service to make sure it starts with the start of the computer. Then it starts to encrypt local files and tries to spread to another MS Windows computers - it behaves also as a “worm” and abuses EternalBlue vulnerability of Windows SMB.

Symptoms of infection include encryption of all files on the computer, periodic pop-up of the ransom window and creation of files, services described above.

YARA signature rules are located at the end of the report. Malware sample and hashes have been submitted to VirusTotal for further examination.

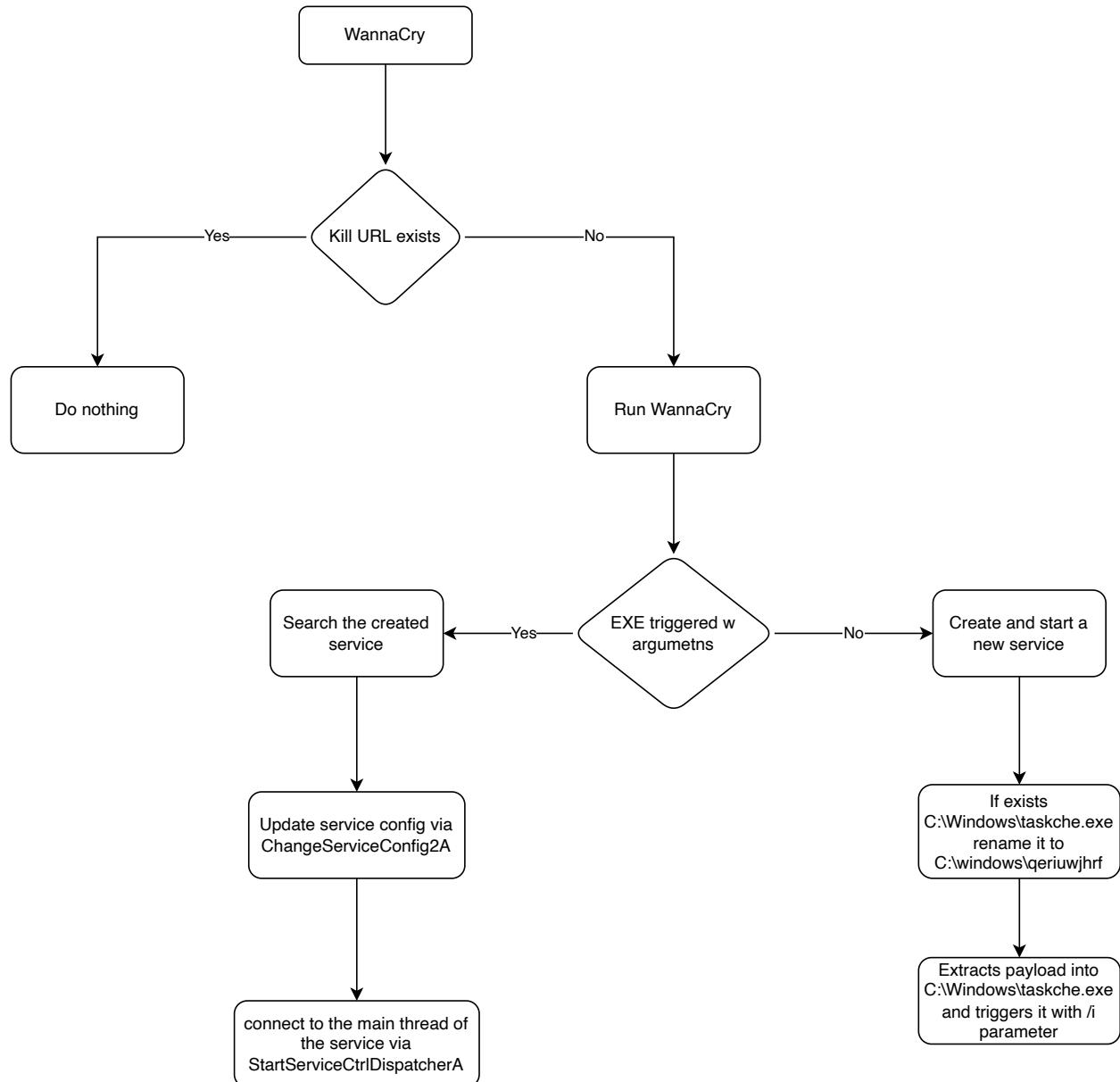
## High-Level Technical Summary

WannaCry consists of two parts: a stage 0 dropper and an unpacked stage 2 encryption and worm program. It first attempts to contact its “kill switch” URL (`hxxps://iuquerfsodp9ifjaposdfjhgosurijfaewrwegwea.com`). If the contact is successful, it ends the execution. This mechanism helped to stop infections in 2017.

If the URL is not accessible, then the dropper creates a new Windows service named “`mssecsvc2.0`”. The display name of this service is “Microsoft Security Center (2.0) Service”. This service starts the original binary with parameter “`-m security`”. The dropper determines if the initial setup was done based on the number of arguments.

Once the service is created and started, the dropper moves file “`C:\Windows\tasksche.exe`” to “`C:\Windows\qeriuwjhrf`”. Then the dropper extracts its resource `0x727` into the “`C:\Windows\tasksche.exe`” and starts this binary with “`/i`” parameter. This binary contains the payload of this malware.

It extracts its helper files into the new folder with the randomly chosen name in `%ProgramData%`. It also creates an own service with the same random name. The stage 2 program encrypts all files on the file system. It also tries to spread by abusing SMB protocol (port 445/TCP) and its EternalBlue vulnerability.



## Malware Composition

WannaCry consists of the following components:

File Name	SHA256 Hash
<b>Ransomware.wannacry.exe</b>	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
<b>tasksche.exe</b>	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa

### [Ransomware.wannacry.exe](#)

The initial executable that runs checks if the kill switch URL is accessible. If it is not, then it creates the new service for the persistence and it extracts and triggers the payload (C:/Windows/tasksche.exe).

### [Tasksche.exe:](#)

The payload of this malware. It also creates own service for its persistence. This time, the name is randomly chosen. It also creates a hidden directory with the same random name inside %PROGRAMDATA%.

This binary abuses the vulnerability of the Windows SMB named EternalBlue to spread among computers. It also encrypts all files on the computer. Once it is completed, the pop-up window with the ransom message is displayed.



Fig 1: The ransom message on the infected computer.



## Basic Static Analysis

### Strings

The command to extract all strings longer than 6 characters from the binary.

```
FLOSS.exe -n 6 Ransomware.wannacry.exe.malz > floss.exe.txt
```

```
OpenServiceA
ADVAPI32.dll
WS2_32.dll
??1_Lockit@std@@QAE@XZ
??0_Lockit@std@@QAE@XZ
MSVCP60.dll
GetPerAdapterInfo
GetAdaptersInfo
iphlpapi.dll
InternetCloseHandle
InternetOpenUrlA
InternetOpenA
WININET.dll
sprintf
_endthreadex
strncpy
_beginthreadex
```

Fig 2: The binary opens the URL.



```
3   malloc
9   _adjust_fdiv
0   launcher.dll
1   PlayGame
2   C:\%s\%s
3   WINDOWS
4   mssecsvc.exe
5   !This program cannot be run in DOS mode.
6   /4%D/4%D/4%D4
7   D|4%D4
8   D&4&D&1
```

Fig 3: The binary dynamically generates path.

```
62  mssecsvc2.0
63  Microsoft Security Center (2.0) Service
64  %s -m security
65  C:\%s\queriuwjhrf
66  C:\%s\%s
67  WINDOWS
68  tasksche.exe
69  CloseHandle
70  WriteFile
71  CreateFileA
72  CreateProcessA
73  http://www.iuquerfsodp9ifjaposdfjhgosurijfaewrwegwea.com
74  !This program cannot be run in DOS mode.
75  ` .rdata
76  @.data
77  SWJcf
78  WWWWWPj
79  S4lGAt
```

Fig 4: The kill-switch URL and another names



```
GetStartupInfoA
c.wnry
advapi32.dll
WANACRY!
CloseHandle
DeleteFileW
MoveFileExW
MoveFileW
ReadFile
WriteFile
CreateFileW
kernel32.dll
0|x8+^_
2/0-_X8w.+_
|~}%.15
Microsoft Enhanced RSA and AES Cryptographic Provider
CryptGenKey
CryptDecrypt
CryptEncrypt
CryptDestroyKey
CryptImportKey
CryptAcquireContextA
cmd.exe /c "%s"
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
Global\MsWinZonesCacheCounterMutexA
tasksche.exe
TaskStart
t.wnry
icacls . /grant Everyone:F /T /C /Q
attrib +h .
WNcry@2017
GetNativeSystemInfo
-zAexception@@
```

Fig 5: Suspicious setting of permissions and execution of command



## PE Inspection

The PEStudio tool reveals that the binary is compiled as a 32bit executable built for MS Windows. The description of the binary suggests, that it tries to look as benign software.

The screenshot shows the PEStudio interface with the following details:

property	value
md5-1	DB349B97C37D22F5EA1D1841E3C89EB4
sha1	E889544AFF85FFAF88000DA705105DE7C97FE26
sha256	24D004A104D4D54034DBCFFC2A4B19A11F39008A575AA614EA04703480B1022C
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00
first-bytes-text	M Z .....
file-size	3723264 bytes
entropy	7.964
imphash	n/a
signature	Microsoft Visual C++ v5.0/v6.0 (MFC)
tooling	Visual Studio 2003 - 7.10 SDK
entry-point	55 8B EC 6A FF 68 A0 A1 40 00 68 A2 9B 40 00 64 A1 00 00 00 00 50 64 89 25 00 00 00 00 83 EC 68 53
file-version	6.1.7601.17514 (win7sp1_rtm.101119-1850)
description	Microsoft® Disk Defragmenter
file-type	executable
cpu	32-bit
subsystem	GUI
compiler-stamp	0x4CE78ECC (Sat Nov 20 09:03:08 2010   UTC)
debugger-stamp	n/a
resources-stamp	0x00000000 (Thu Jan 01 00:00:00 1970   UTC)
import-stamp	0x00000000 (Thu Jan 01 00:00:00 1970   UTC)
exports-stamp	n/a

Fig 6: The overall information from PEStudio

In the PEView tool, we can examine the Import Address Table of the binary. It displays multiple suspicious methods.

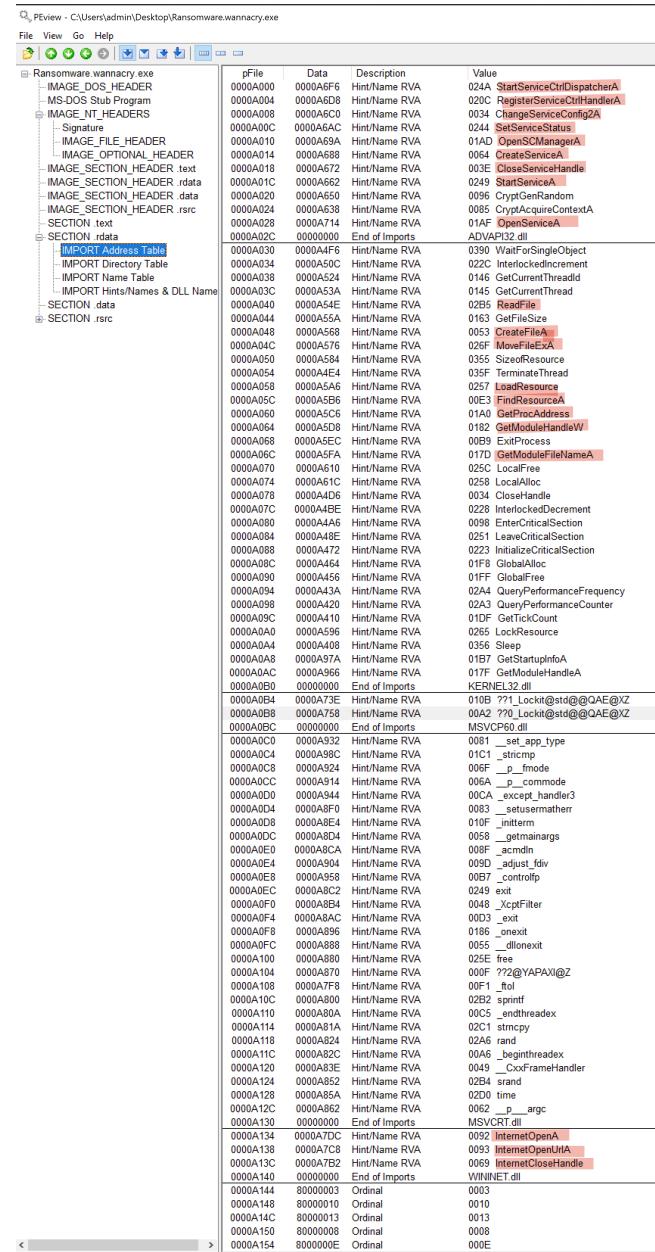


Fig 7: Import address table

# Basic Dynamic Analysis

## Kill-switch URL

When the binary is analyzed in the environment with the fake internet (it pretends success when the tool tries to connect to anything), the binary does not cause any harm at all.

In the network monitoring tool (Wireshark) we can observe, that it tried to connect to the “`hxxp://www.iuquerfsodp9ifjaposdfjhgosurijfaewrwegwea.com`”.

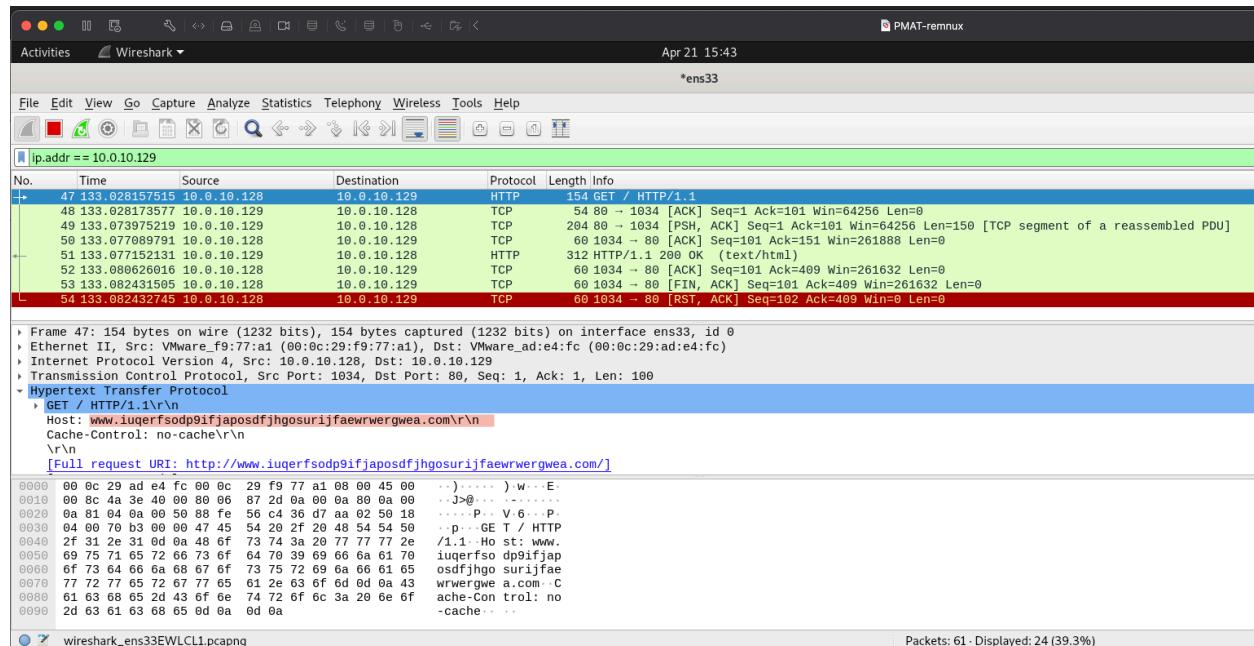


Fig 8: Communication to the kill switch URL

## Without kill-switch URL

The dropper creates a new file “`C:\Windows\tasksche.exe`” which contains the main logic of the malware.



1:19:22... [R] Ransomware.w...	3308	[!] CreateFile	C:\Windows\SysWOW64\mswsock.dll	SUCCESS	Desired Access: R...
1:19:22... [R] Ransomware.w...	3308	[!] CreateFile	C:\Windows\SysWOW64\winnsi.dll	SUCCESS	Desired Access: R...
1:19:22... [R] Ransomware.w...	3308	[!] CreateFile	C:\Windows\SysWOW64\winnsi.dll	SUCCESS	Desired Access: R...
1:19:22... [R] Ransomware.w...	3308	[!] CreateFile	C:\Users\admin\Desktop\urlmon.dll	NAME NOT FOUND	Desired Access: R...
1:19:22... [R] Ransomware.w...	3308	[!] CreateFile	C:\Windows\SysWOW64\urlmon.dll	SUCCESS	Desired Access: R...
1:19:22... [R] Ransomware.w...	3308	[!] CreateFile	C:\Windows\SysWOW64\urlmon.dll	SUCCESS	Desired Access: R...
1:19:22... [R] Ransomware.w...	3308	[!] CreateFile	C:\Users\admin\Desktop\srvccl.dll	NAME NOT FOUND	Desired Access: R...
1:19:22... [R] Ransomware.w...	3308	[!] CreateFile	C:\Users\admin\Desktop\netutils.dll	NAME NOT FOUND	Desired Access: R...
1:19:22... [R] Ransomware.w...	3308	[!] CreateFile	C:\Windows\SysWOW64\srvccl.dll	SUCCESS	Desired Access: R...
1:19:22... [R] Ransomware.w...	3308	[!] CreateFile	C:\Windows\SysWOW64\inetutils.dll	SUCCESS	Desired Access: R...
1:19:22... [R] Ransomware.w...	3308	[!] CreateFile	C:\Windows\SysWOW64\srvccl.dll	SUCCESS	Desired Access: R...
1:19:22... [R] Ransomware.w...	3308	[!] CreateFile	C:\Windows\SysWOW64\inetutils.dll	SUCCESS	Desired Access: R...
1:19:22... [R] Ransomware.w...	3308	[!] CreateFile	C:\Windows\SysWOW64\ole32.dll	SUCCESS	Desired Access: R...
1:19:22... [R] Ransomware.w...	3308	[!] CreateFile	C:\Windows\SysWOW64\ole32.dll	SUCCESS	Desired Access: R...
1:19:22... [R] Ransomware.w...	3308	[!] CreateFile	C:\Windows\SysWOW64\dnsapi.dll	SUCCESS	Desired Access: R...
1:19:22... [R] Ransomware.w...	3308	[!] CreateFile	C:\Windows\SysWOW64\dnsapi.dll	SUCCESS	Desired Access: R...
1:19:22... [R] Ransomware.w...	3308	[!] CreateFile	C:\Windows\SysWOW64\rasadhlp.dll	SUCCESS	Desired Access: R...
1:19:22... [R] Ransomware.w...	3308	[!] CreateFile	C:\Windows\SysWOW64\rasadhlp.dll	SUCCESS	Desired Access: R...
1:19:22... [R] Ransomware.w...	3308	[!] CreateFile	C:\Users\admin\Desktop\CRYPTSP.dll	NAME NOT FOUND	Desired Access: R...
1:19:22... [R] Ransomware.w...	3308	[!] CreateFile	C:\Windows\SysWOW64\cryptsp.dll	SUCCESS	Desired Access: R...
1:19:22... [R] Ransomware.w...	3308	[!] CreateFile	C:\Windows\SysWOW64\cryptsp.dll	SUCCESS	Desired Access: R...
1:19:22... [R] Ransomware.w...	3440	[!] CreateFile	C:\Windows\tasksche.exe	NAME NOT FOUND	Desired Access: R...
1:19:22... [R] Ransomware.w...	3440	[!] CreateFile	C:\Windows\tasksche.exe	SUCCESS	Desired Access: G...
1:19:22... [R] Ransomware.w...	3308	[!] CreateFile	C:\Windows\SysWOW64\rsaenh.dll	SUCCESS	Desired Access: R...
1:19:22... [R] Ransomware.w...	3440	[!] CreateFile	C:\Windows\tasksche.exe	SUCCESS	Desired Access: R...
1:19:22... [R] Ransomware.w...	3308	[!] CreateFile	C:\Windows\SysWOW64\rsaenh.dll	SUCCESS	Desired Access: R...
1:19:22... [R] Ransomware.w...	3308	[!] CreateFile	C:\Users\admin\Desktop\CRYPTBASE.dll	NAME NOT FOUND	Desired Access: R...
1:19:22... [R] Ransomware.w...	3308	[!] CreateFile	C:\Windows\SysWOW64\cryptbase.dll	SUCCESS	Desired Access: R...
1:19:22... [R] Ransomware.w...	3308	[!] CreateFile	C:\Windows\SysWOW64\cryptbase.dll	SUCCESS	Desired Access: R...
1:19:22... [R] Ransomware.w...	3308	[!] CreateFile	C:\Users\admin\Desktop\Ransomware....	SUCCESS	Desired Access: G...
1:19:22... [R] Ransomware.w...	3440	[!] CreateFile	C:\Windows\tasksche.exe	SUCCESS	Desired Access: R...
1:19:22... [R] Ransomware.w...	3440	[!] CreateFile	C:\Windows\tasksche.exe	SUCCESS	Desired Access: R...
1:19:22... [R] Ransomware.w...	3440	[!] CreateFile	C:\Windows\tasksche.exe	SUCCESS	Desired Access: R...

Fig 9: The extracted tasksche.exe binary



The “taskche.exe” creates a new hidden directory with the random name and a new service with the same name. It extracts its helper files inside the created directory.

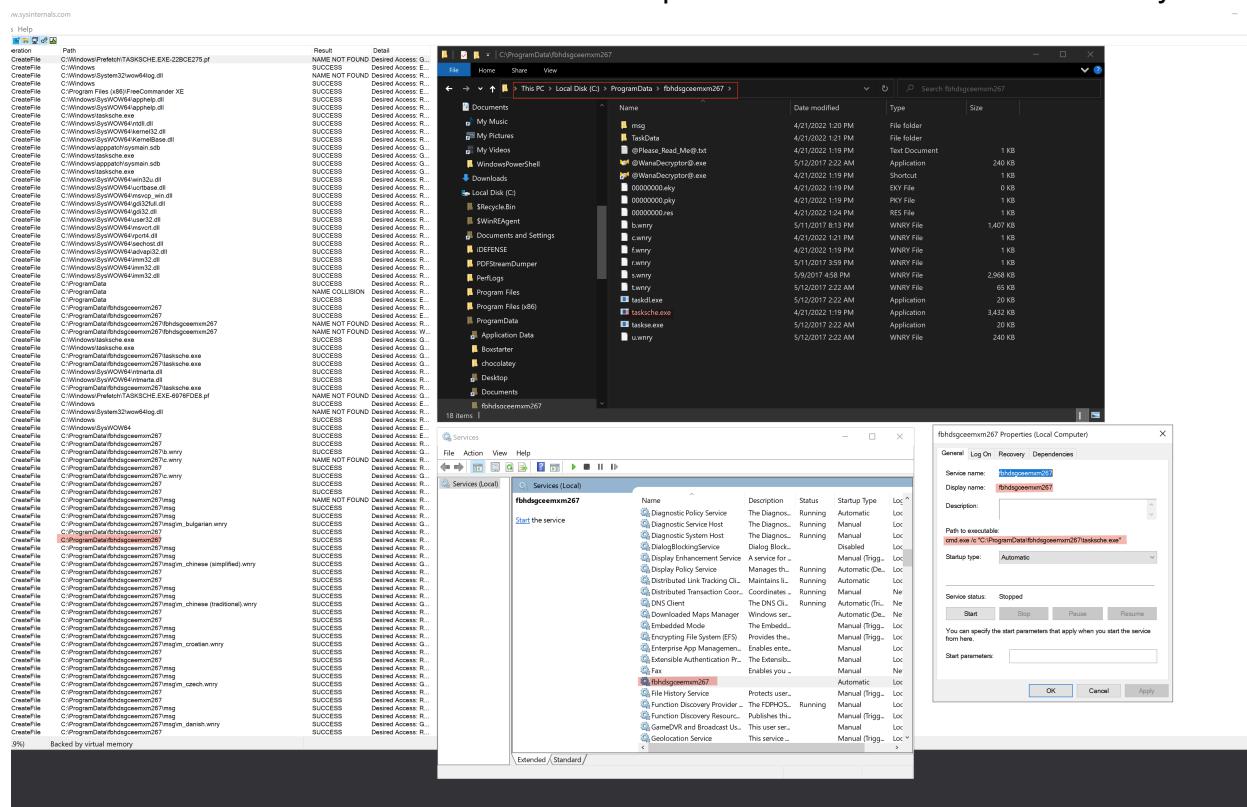


Fig 10: The created hidden folder and new service

Later it tries to communicate with other computers on the network via port 445/TCP (SMB protocol). If it finds any of such computers, it tries to infect it by abusing the EternalBlue vulnerability.



System	4	TCP	Listen	169.254.44.118	139	0.0.0	0	4/21/2022 7:12:34 AM System
[Time Wait]		TCP	Time Wait	10.0.10.128	1048	10.0.10.1	445	
Ransomware.wannacry-	5940	TCP	Syn Sent	169.254.44.118	1198	169.254.118.1	445	4/21/2022 1:12:47 PM mssecsv2.0
Ransomware.wannacry-	5940	TCP	Syn Sent	169.254.44.118	1199	169.254.119.1	445	4/21/2022 1:12:47 PM mssecsv2.0
Ransomware.wannacry-	5940	TCP	Syn Sent	10.0.10.128	1200	17.12.234.232	445	4/21/2022 1:12:47 PM mssecsv2.0
Ransomware.wannacry-	5940	TCP	Syn Sent	10.0.10.128	1201	33.197.20.132	445	4/21/2022 1:12:47 PM mssecsv2.0
Ransomware.wannacry-	5940	TCP	Syn Sent	169.254.44.118	1202	169.254.120.1	445	4/21/2022 1:12:47 PM mssecsv2.0
Ransomware.wannacry-	5940	TCP	Syn Sent	169.254.44.118	1203	169.254.121.1	445	4/21/2022 1:12:47 PM mssecsv2.0
Ransomware.wannacry-	5940	TCP	Syn Sent	169.254.44.118	1204	169.254.122.1	445	4/21/2022 1:12:47 PM mssecsv2.0
Ransomware.wannacry-	5940	TCP	Syn Sent	10.0.10.128	1205	40.124.196.211	445	4/21/2022 1:12:47 PM mssecsv2.0
Ransomware.wannacry-	5940	TCP	Syn Sent	10.0.10.128	1206	175.91.35.3	445	4/21/2022 1:12:47 PM mssecsv2.0
Ransomware.wannacry-	5940	TCP	Syn Sent	169.254.44.118	1207	169.254.123.1	445	4/21/2022 1:12:47 PM mssecsv2.0
Ransomware.wannacry-	5940	TCP	Syn Sent	169.254.44.118	1208	169.254.124.1	445	4/21/2022 1:12:47 PM mssecsv2.0
Ransomware.wannacry-	5940	TCP	Syn Sent	10.0.10.128	1209	133.182.72.100	445	4/21/2022 1:12:47 PM mssecsv2.0
Ransomware.wannacry-	5940	TCP	Syn Sent	169.254.44.118	1210	169.254.125.1	445	4/21/2022 1:12:47 PM mssecsv2.0
Ransomware.wannacry-	5940	TCP	Syn Sent	169.254.44.118	1211	169.254.126.1	445	4/21/2022 1:12:48 PM mssecsv2.0
Ransomware.wannacry-	5940	TCP	Syn Sent	10.0.10.128	1212	25.128.196.194	445	4/21/2022 1:12:48 PM mssecsv2.0
Ransomware.wannacry-	5940	TCP	Syn Sent	169.254.44.118	1213	169.254.127.1	445	4/21/2022 1:12:48 PM mssecsv2.0
Ransomware.wannacry-	5940	TCP	Syn Sent	169.254.44.118	1214	169.254.128.1	445	4/21/2022 1:12:48 PM mssecsv2.0
svchost.exe	6068	TCP	Listen	0.0.0	5040	0.0.0	0	4/21/2022 7:14:42 AM CDPsvc
lsass.exe	696	TCP	Listen	0.0.0	49664	0.0.0	0	4/21/2022 7:12:30 AM lsass.exe
wininit.exe	556	TCP	Listen	0.0.0	49665	0.0.0	0	4/21/2022 7:12:30 AM wininit.exe

Fig 11: Tasksche.exe tries to discover computers on the network with 445/TCP

In the end, it also encrypts all files and displays the ransom message.



Fig 12: The ransom message



# Advanced Analysis

## Failsafe check

The program at first checks if the URL “`hxxp://www.iuquerfsodp9ifjaposdfjhgosurijfaewrwerwergwea.com`” can be reached. If it is accessible, then it does almost nothing (just closes handles) and ends its run. Otherwise, the method with the malware’s logic `fnc_00408090` is called.

```
[0x00408140]
139: int main (int argc, char **argv, char **envp);
; var int32_t var_14h @ esp+0x28
; var int32_t var_8h @ esp+0x3c
; var int32_t var_41h @ esp+0x75
; var int32_t var_45h @ esp+0x79
; var int32_t var_49h @ esp+0x7d
; var int32_t var_4dh @ esp+0x81
; var int32_t var_51h @ esp+0x85
; var int32_t var_55h @ esp+0x89
; var int32_t var_6bh @ esp+0x8b
sub    esp, 0x50
push   esi
push   edi
mov    eax, 0xe
; 14
mov    esi, str.http:_www.iuquerfsodp9ifjaposdfjhgosurijfaewrwerwergwea.com ; 0x4313d0
lea    edi, [var_8h]
xor    eax, eax
rep    movsd dword es:[edi], dword ptr [esi]
movsb byte es:[edi], byte ptr [esi]
mov    dword [var_41h], eax
mov    dword [var_45h], eax
mov    dword [var_49h], eax
mov    dword [var_4dh], eax
mov    dword [var_51h], eax
mov    word [var_55h], ax
push   eax
push   eax
push   eax
push   1
push   eax
; 1
mov    byte [var_6bh], al
call   dword [InternetOpenA] ; 0x40a134
push   0
push   0x84000000
push   0
lea    ecx, [var_14h]
mov    esi, eax
push   0
push   ecx
push   esi
call   dword [InternetOpenUrlA] ; 0x40a138
mov    edi, eax
push   esi
mov    esi, dword [InternetCloseHandle] ; 0x40a13c
test   edi, edi
jne   0x4081bc

[0x004081a7]
call   esi
push   0
call   esi
call   fcn.00408090
pop    edi
xor    eax, eax
pop    esi
add    esp, 0x50
ret    0x10

[0x004081bc]
call   esi
push   edi
call   esi
pop    edi
xor    eax, eax
pop    esi
add    esp, 0x50
ret    0x10
```

Fig 13: Check of the URL existence



## Detection of the first run

The application detects if it is triggered for the first time by the missing command line arguments. In such case it calls method fnc\_00407f20, which creates a new service and extracts payload.

Otherwise it uses the already created service.

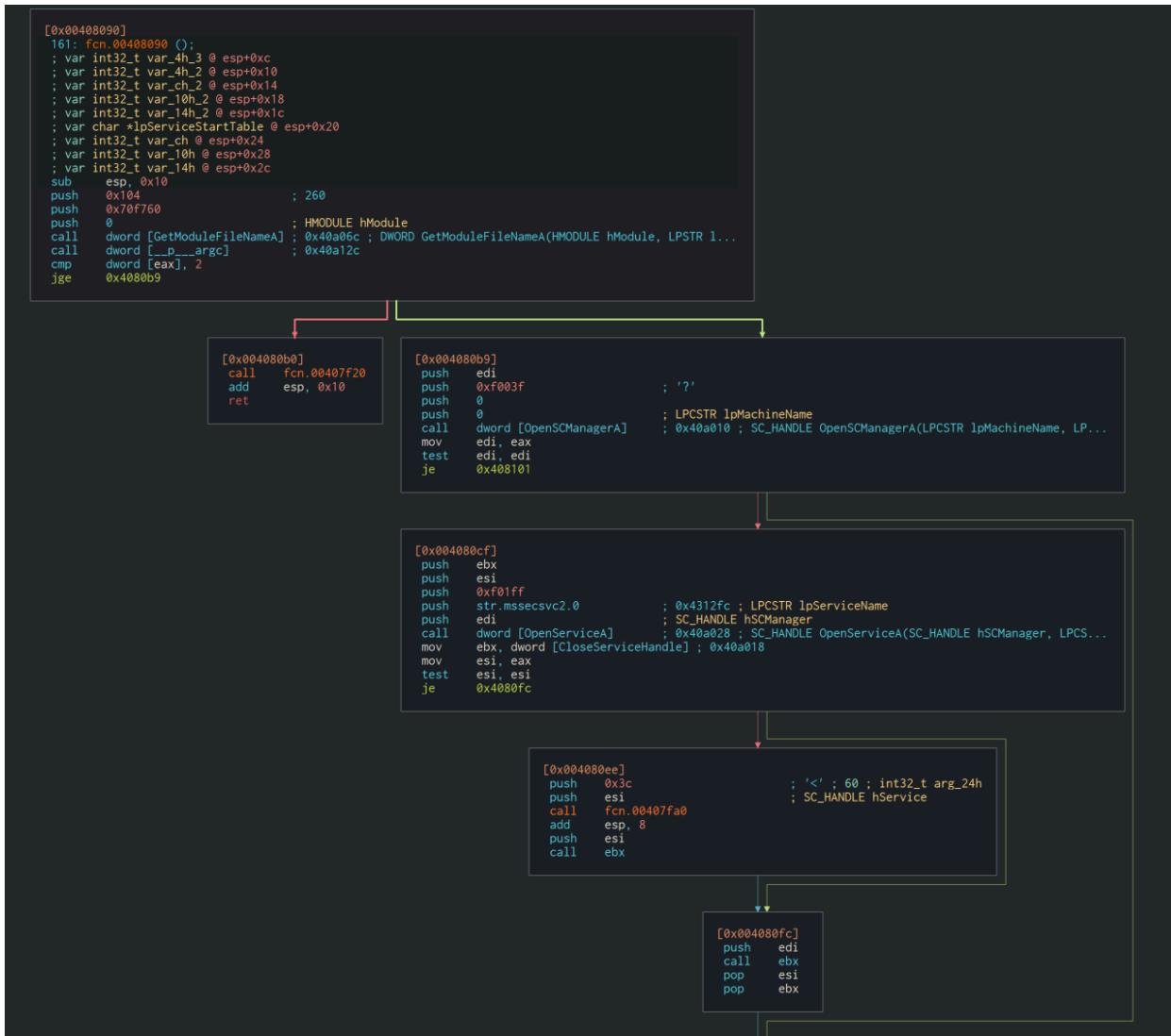


Fig 14: The detection of the first run



## Creation of the new service

The figure below shows decompiled output of the creation of the new service. This decompilation was done by the Ghidra software. I've updated few names inside the example for easier reading.

```
1 undefined4 wannacryCreateAndStartService(void)
2
3 {
4     SC_HANDLE hSCManager;
5     SC_HANDLE hService;
6     char local_104 [260];
7
8     sprintf(local_104,s_%s_m|security_00431330,wannacryFileName);
9     hSCManager = OpenSCManagerA((LPCSTR)0x0,(LPCSTR)0x0,0xf003f);
10    if (hSCManager != (SC_HANDLE)0x0) {
11        hService = CreateServiceA(hSCManager,s_mssecsvc2.0_004312fc,
12                                s_Microsoft_Security_Center_(2.0)_S_00431308,0xf01ff,0x10,2,1,
13                                local_104,(LPCSTR)0x0,(LPDWORD)0x0,(LPCSTR)0x0,(LPCSTR)0x0,
14                                );
15
16        if (hService != (SC_HANDLE)0x0) {
17            StartServiceA(hService,0,(LPCSTR *)0x0);
18            CloseServiceHandle(hService);
19        }
20        CloseServiceHandle(hSCManager);
21        return 0;
22    }
23    return 0;
24 }
25 }
```

*Fig 15: The creation of the new service*



## The extraction of the tasksche.exe

In the figure below, we can see the extraction of the resource into the tasksche.exe file.

```
if (((((addressCreateProcessA != (FARPROC) 0x0) && (addressCreateFileA != (FARPROC) 0x0)
        (addressWriteFile != (FARPROC) 0x0)) && (addressCloseHandle != (FARPROC) 0x0)) {
    hResInfo = FindResourceA((HMODULE) 0x0, (LPCSTR) 0x727, &DAT_0043137c);
    if (hResInfo != (HRSRC) 0x0) {
        hResData = LoadResource((HMODULE) 0x0, hResInfo);
        if (hResData != (HGLOBAL) 0x0) {
            pvVar2 = LockResource(hResData);
            if (pvVar2 != (LPVOID) 0x0) {
                DVar3 = SizeofResource((HMODULE) 0x0, hResInfo);
                if (DVar3 != 0) {
                    stringC:\Windows\tasksche.exe = '\0';
                    puVar6 = &local_207;
                    for (CreateFileA = 0xA0 * CreateFileA + 0 * CreateFileA = CreateFileA + -1
```

Fig 16: The extraction of the resource into tasksche.exe

The extracted binary is later triggered with the “/i” parameter. After that, the malware tries to spread to another computers and also encrypts all files on the system.

The screenshot shows a debugger interface with assembly code and register values. The assembly code includes instructions like repne scasd, mov ecx, ebp, dec edi, shr ecx,2, rep movsd, lea eax,dword ptr ss:[esp+14], and ecx,3, push eax, rep movsb, lea ecx,dword ptr ss:[esp+28], lea edx,dword ptr ss:[esp+6C], push ecx, push ebx, push ebx, push 8000000, push ebx, push ebx, push ebx, push edx, push ebx, mov dword ptr ss:[esp+4C],44, mov word ptr ss:[esp+7C],bx, mov dword ptr ss:[esp+78],81, call dword ptr ds:[<&CreateProcessA> ], test eax,eax, je ransomware.wannacry.407F08, and mov byte dword ptr [eax+10]. The registers show values such as 'esi:"C:\\%s\\qeriuwjhrf"', 'edx:"C:\\WINDOWS\\tasksche.exe /i"', '44:'D', and '407F08'. The memory dump pane shows the extracted binary data.

Fig 17: Triggering of the tasksche.exe



taskhostw.exe	3.548 K	7,640 K	7448 Host Process for Windows T...	Microsoft Corporation
Taskmgr.exe	3.42	22,800 K	52,596 K 4504 Task Manager	Microsoft Corporation
tasksche.exe	19.01	18,768 K	26,496 K 5904 DiskPart	Microsoft Corporation
TextInputHost.exe		13,284 K	38,256 K 4572	Microsoft Corporation
uhsvc.exe		1,300 K	6,128 K 4284 Microsoft Update Health Ser...	Microsoft Corporation
VGAuthService.exe		2,892 K	7,544 K 3164 VMware Guest Authenticatio...	VMware, Inc.

Fig 18: Triggered tasksche.exe

# Indicators of Compromise

## Network Indicators

There are two main network based indicators of compromise. The first is the communication with the kill switch URL which is specific for the WannaCry ransomware.

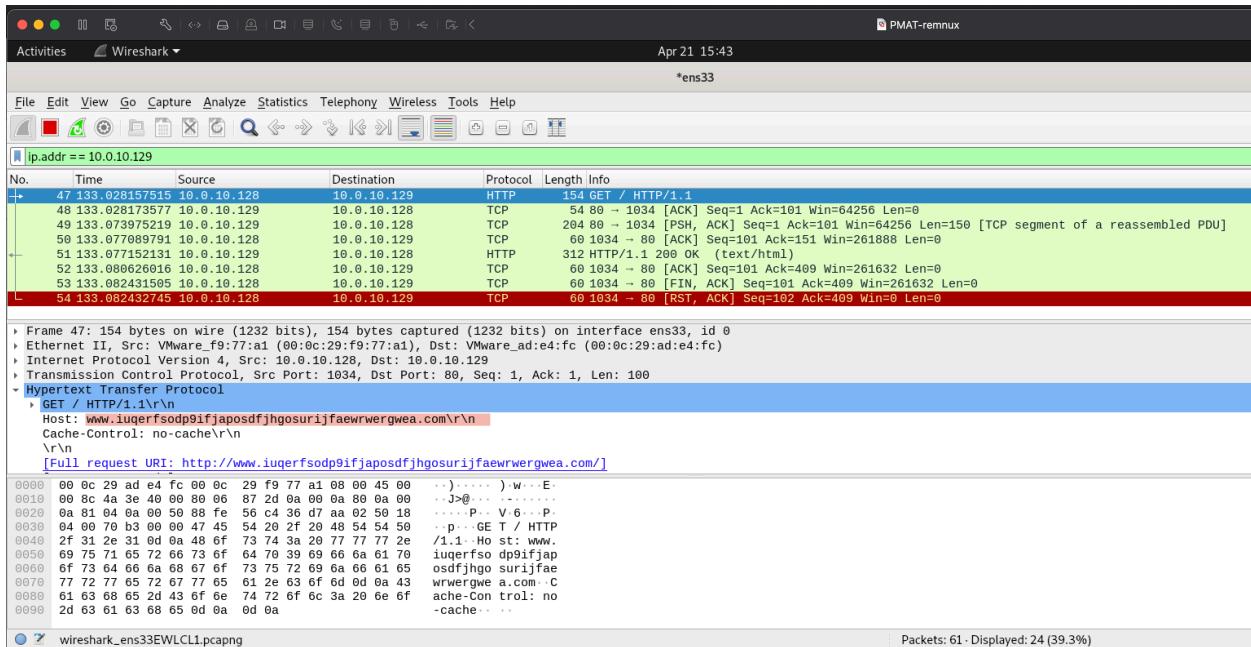


Fig 19: Wireshark Packet Capture of kill switch URL



The second are attempts to discover machines with opened port 445/TCP on the local network.

System	4	TCP	Listen	169.254.44.118	139	0.0.0	0	4/21/2022 7:12:34 AM	System
<b>[Time Wait]</b>									
Ransomware.wannacry-	5940	TCP	Syn Sent	169.254.44.118	1048	10.0.10.1	445	4/21/2022 1:12:47 PM	mssecsvc20
Ransomware.wannacry-	5940	TCP	Syn Sent	169.254.44.118	1198	169.254.119.1	445	4/21/2022 1:12:47 PM	mssecsvc20
Ransomware.wannacry-	5940	TCP	Syn Sent	169.254.44.118	1199	169.254.119.1	445	4/21/2022 1:12:47 PM	mssecsvc20
Ransomware.wannacry-	5940	TCP	Syn Sent	10.0.10.128	1200	17.12.234.232	445	4/21/2022 1:12:47 PM	mssecsvc20
Ransomware.wannacry-	5940	TCP	Syn Sent	169.254.44.118	1201	33.197.20.132	445	4/21/2022 1:12:47 PM	mssecsvc20
Ransomware.wannacry-	5940	TCP	Syn Sent	169.254.44.118	1202	169.254.120.1	445	4/21/2022 1:12:47 PM	mssecsvc20
Ransomware.wannacry-	5940	TCP	Syn Sent	169.254.44.118	1203	169.254.121.1	445	4/21/2022 1:12:47 PM	mssecsvc20
Ransomware.wannacry-	5940	TCP	Syn Sent	169.254.44.118	1204	169.254.122.1	445	4/21/2022 1:12:47 PM	mssecsvc20
Ransomware.wannacry-	5940	TCP	Syn Sent	10.0.10.128	1205	40.124.196.211	445	4/21/2022 1:12:47 PM	mssecsvc20
Ransomware.wannacry-	5940	TCP	Syn Sent	10.0.10.128	1206	175.91.35.3	445	4/21/2022 1:12:47 PM	mssecsvc20
Ransomware.wannacry-	5940	TCP	Syn Sent	169.254.44.118	1207	169.254.123.1	445	4/21/2022 1:12:47 PM	mssecsvc20
Ransomware.wannacry-	5940	TCP	Syn Sent	169.254.44.118	1208	169.254.124.1	445	4/21/2022 1:12:47 PM	mssecsvc20
Ransomware.wannacry-	5940	TCP	Syn Sent	10.0.10.128	1209	133.182.72.100	445	4/21/2022 1:12:47 PM	mssecsvc20
Ransomware.wannacry-	5940	TCP	Syn Sent	169.254.44.118	1210	169.254.125.1	445	4/21/2022 1:12:47 PM	mssecsvc20
Ransomware.wannacry-	5940	TCP	Syn Sent	169.254.44.118	1211	169.254.126.1	445	4/21/2022 1:12:48 PM	mssecsvc20
Ransomware.wannacry-	5940	TCP	Syn Sent	10.0.10.128	1212	25.128.196.194	445	4/21/2022 1:12:48 PM	mssecsvc20
Ransomware.wannacry-	5940	TCP	Syn Sent	169.254.44.118	1213	169.254.127.1	445	4/21/2022 1:12:48 PM	mssecsvc20
Ransomware.wannacry-	5940	TCP	Syn Sent	169.254.44.118	1214	169.254.128.1	445	4/21/2022 1:12:48 PM	mssecsvc20
svchost.exe	6068	TCP	Listen	0.0.0	5040	0.0.0	0	4/21/2022 7:14:42 AM	CDPSvc
lsass.exe	696	TCP	Listen	0.0.0	49664	0.0.0	0	4/21/2022 7:12:30 AM	lsass.exe
wininit.exe	556	TCP	Listen	0.0.0	49665	0.0.0	0	4/21/2022 7:12:30 AM	wininit.exe

Fig 20: Attempted communication to another windows machines on the network

## Host-based Indicators

The main indicator of compromise on the system are encrypted files with the WNCRY extension. Except of that, we can see on the Desktop folder the triplet of files, which are generated every time:

- @Please\_Read\_Me@.txt
- @WanaDecryptor@.bpm
- @WanaDecryptor@.exe



Name	Date modified	Type	Size
	4/22/2022 2:52 AM	File folder	
	4/22/2022 2:52 AM	File folder	
	4/22/2022 2:52 AM	File folder	
@Please_Read_Me@.txt	4/22/2022 2:51 AM	Text Document	1 KB
@WanaDecryptor@.bmp	5/11/2017 8:13 PM	Bitmap image	1,407 KB
@WanaDecryptor@.exe	5/12/2017 2:22 AM	Application	240 KB
Ransomware.wannacry.exe	2/23/2022 3:51 AM	WNCRY File	1,714 KB
tasksche.exe	3/22/2022 3:46 PM	Shortcut	1 KB
tasksche.exe.malz.zip	3/24/2022 12:54 PM	Shortcut	2 KB
tasksche.exe.txt	3/19/2019 12:32 PM	Application	3,636 KB
WNCRY	4/21/2022 6:44 AM	Application	3,432 KB
WNCRY	4/21/2022 7:19 AM	WNCRY File	3,401 KB
WNCRY	4/21/2022 7:05 AM	WNCRY File	28 KB

Fig 21: Files on the user's desktop



## Rules & Signatures

```
rule wannacry_detection {

    meta:
        last_updated = "2022-04-22"
        author = "Ganoes"
        description = "The Yara rule for PMAT - WannaCry"

    strings:
        $url = "www.iuquerfsodp9ifjaposdfjhgosurijfaewrwegwea.com"
        $backup_file = "qeriuwjhrf"
        $payload_file = "tasksche.exe"
        $PE_magic_byte = "MZ"
        $sus_hex_string = { FF E4 ?? 00 FF }

    condition:
        $PE_magic_byte at 0 and
        ($url or $backup_file and $payload_file)
}
```