Practical Malware Analysis & Triage

Malware Analysis Report

WannaCry Dropper Malware

April 2022 | Ganoes | v1.0

Table of Contents

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

Executive Summary

SHA256 hash	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c

The WannaCry dropper malware was widely spread to at least 74 countries. Infections started on May 12th, 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.

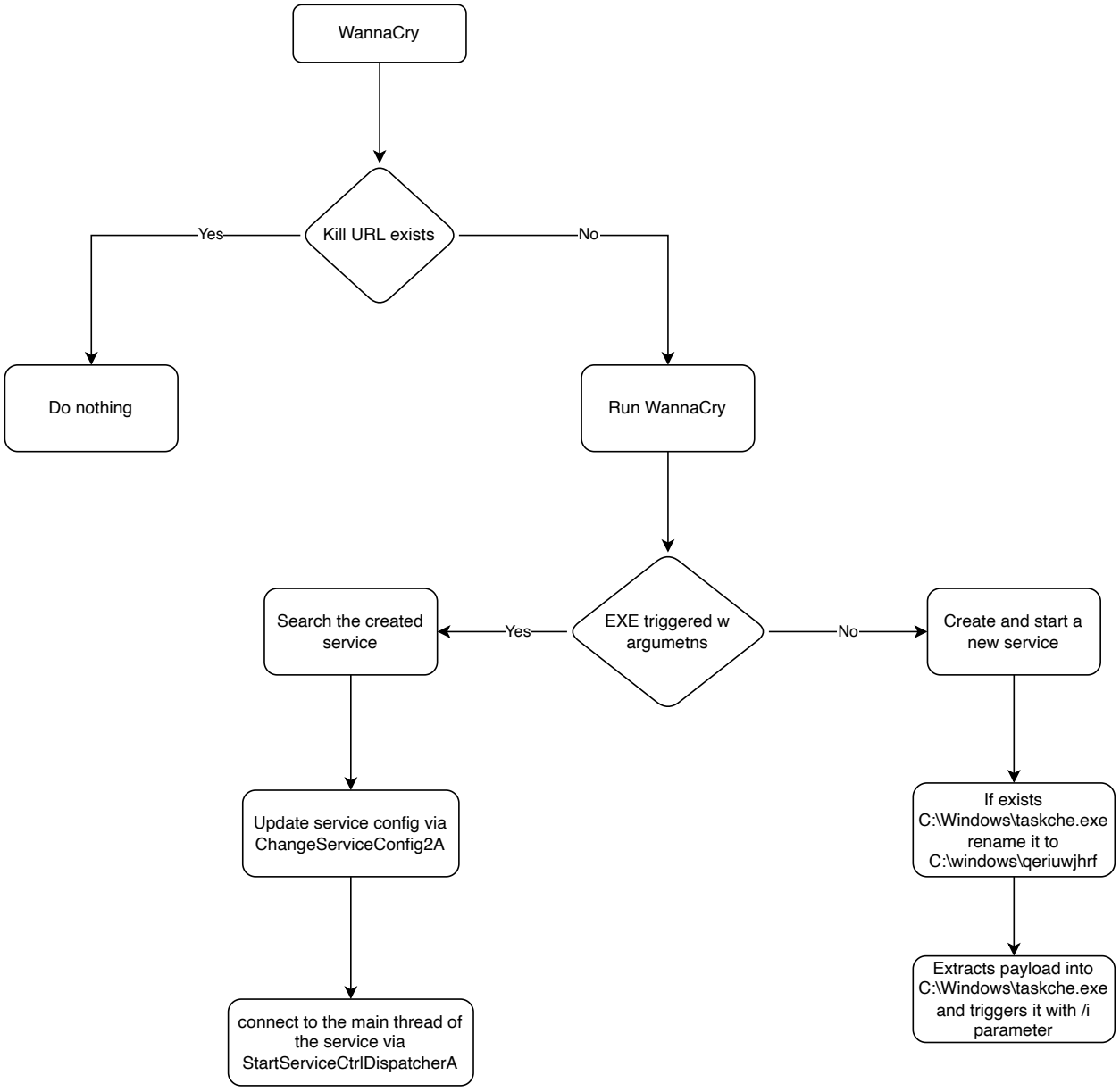
YARA signature rules are located at the end of the report. Malware sample and hashes have been submitted to VirusTotal for further examination.

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://iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.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.


WannaCry
Kill URL exists
Yes
No
Do nothing
Run WannaCry
EXE triggered w argumetns
Yes
No
Search the created service
Create and start a new service
Update service config via ChangeServiceConfig2A
If exists C:\Windows\taskche.exe rename it to C:\windows\qeriuwjhrf
connect to the main thread of the service via StartServiceCtrlDispatcherA
Extracts payload into C:\Windows\taskche.exe and triggers it with /i parameter

Malware Composition

WannaCry consists of the following components:

File Name	SHA256 Hash
Ranswomware.wannacry.exe	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
tasksche.exe	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
```

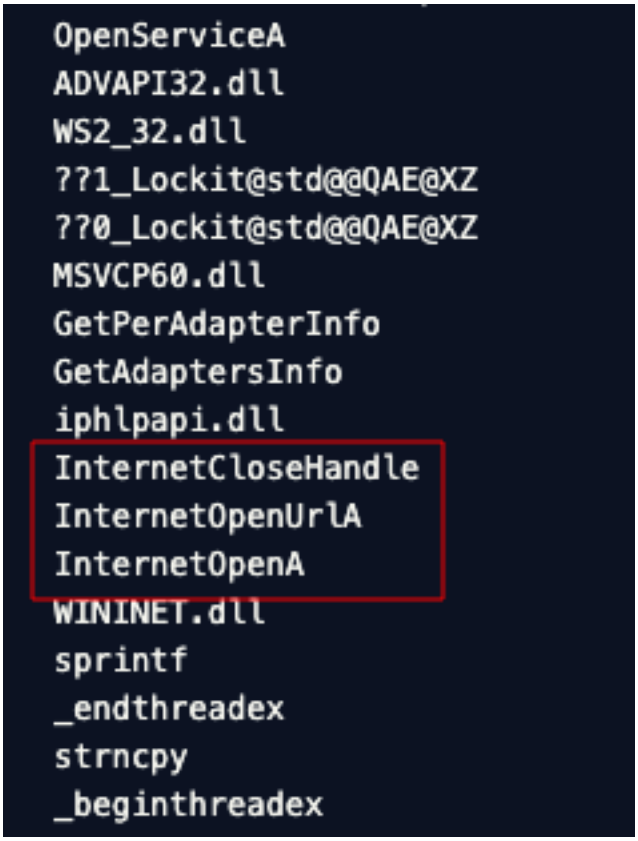


Fig 2: The binary opens the URL.

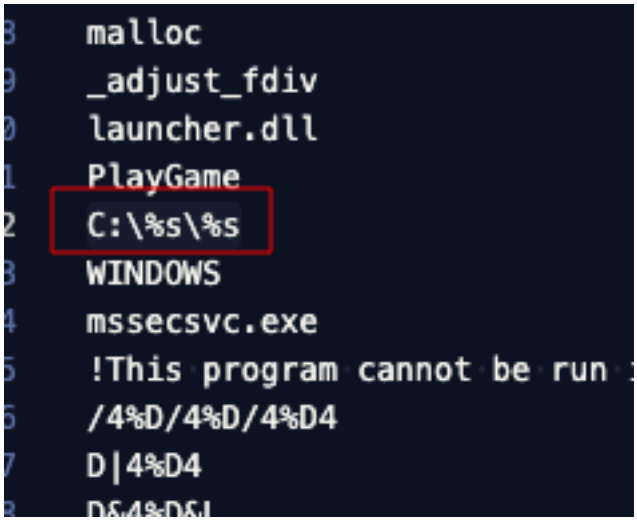


Fig 3: The binary dynamically generates path.

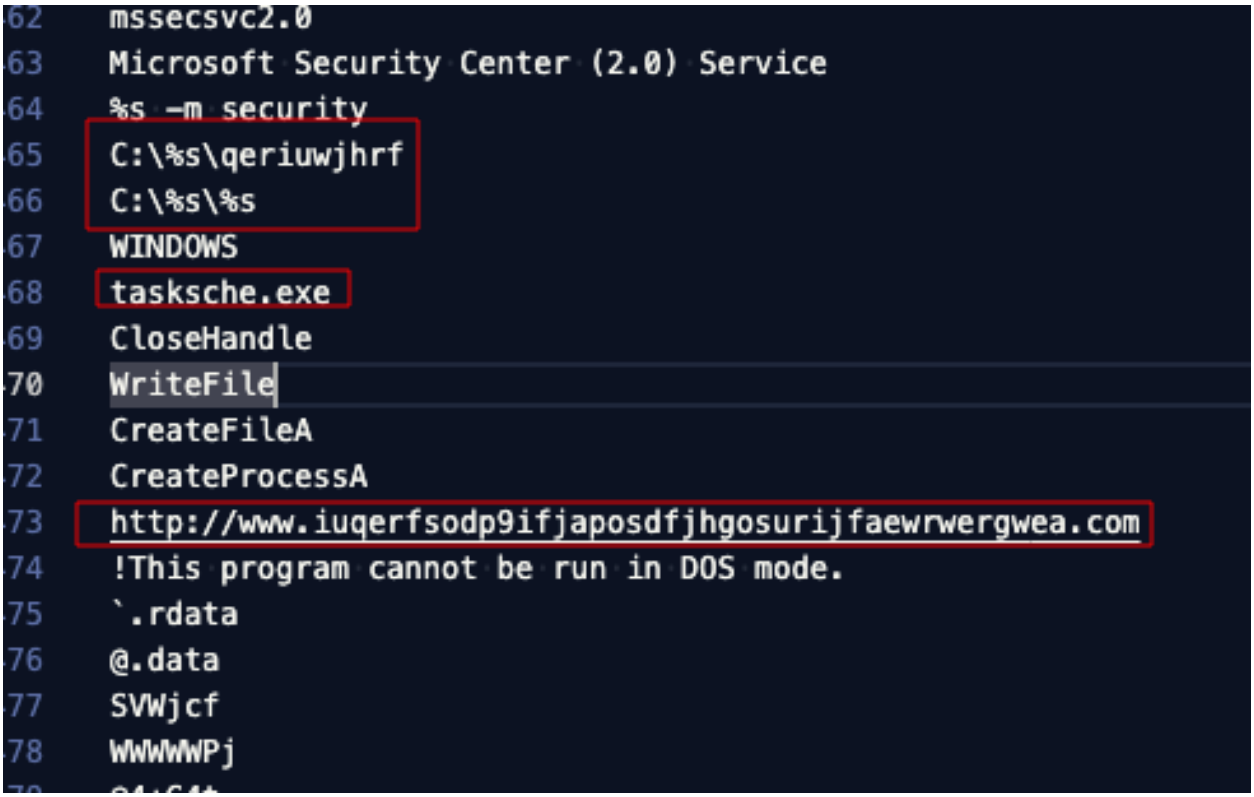


Fig 4: The kill-switch URL and another names

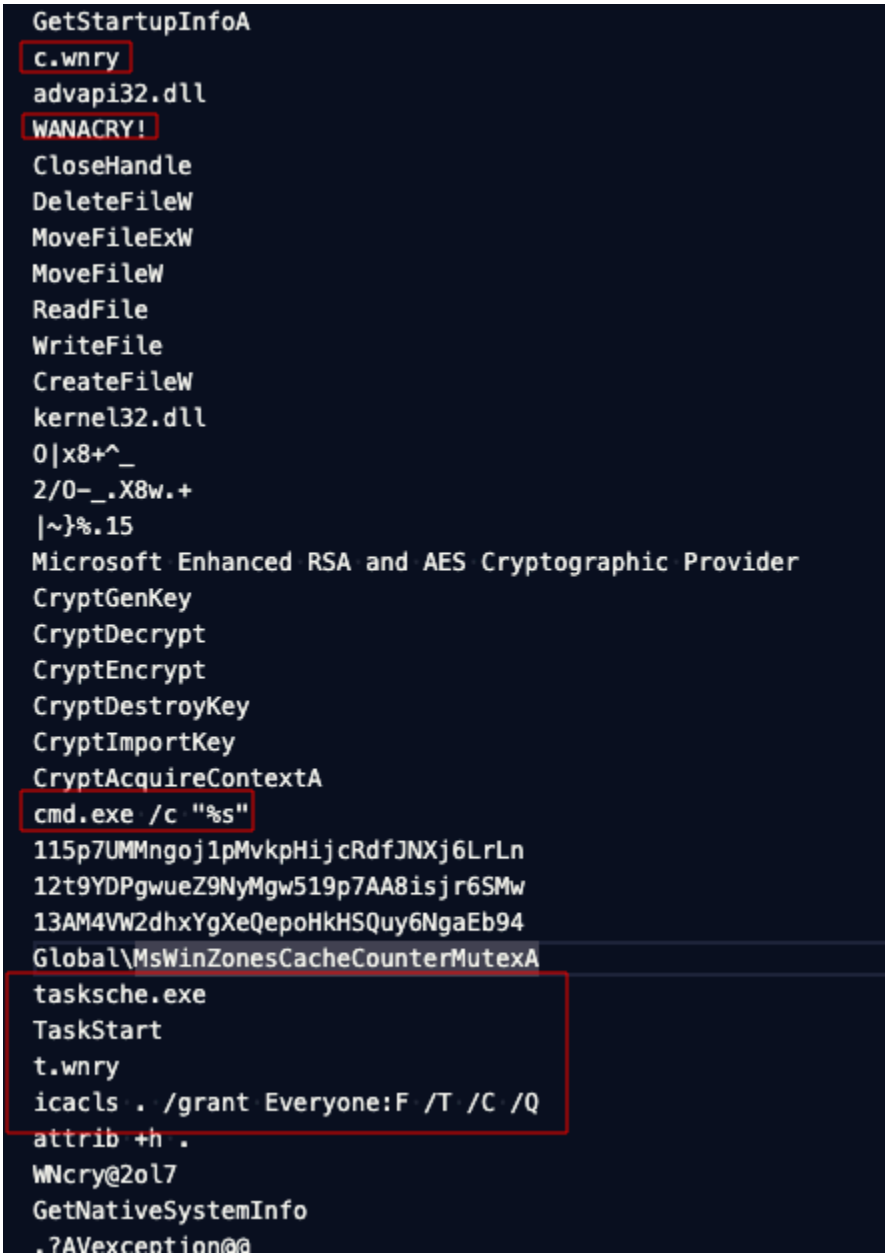


Fig 5: Suspicious setting of permissions and execution of command

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.

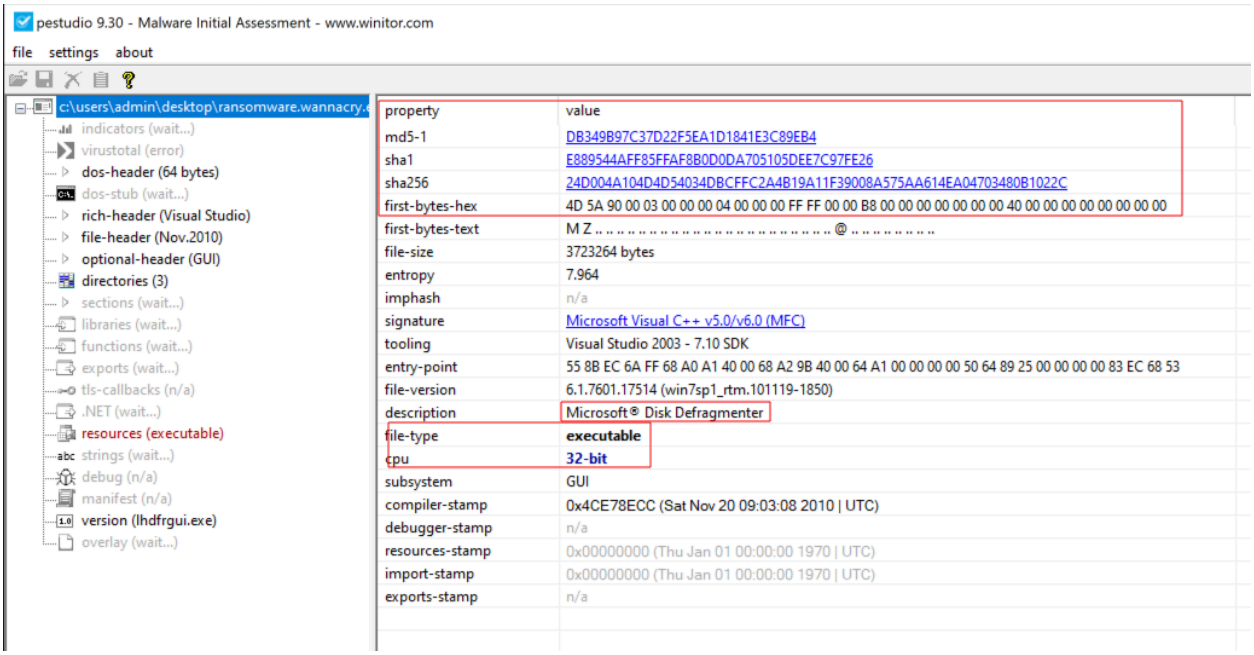


Fig 6: The overall information from PEStudio

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.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com”.

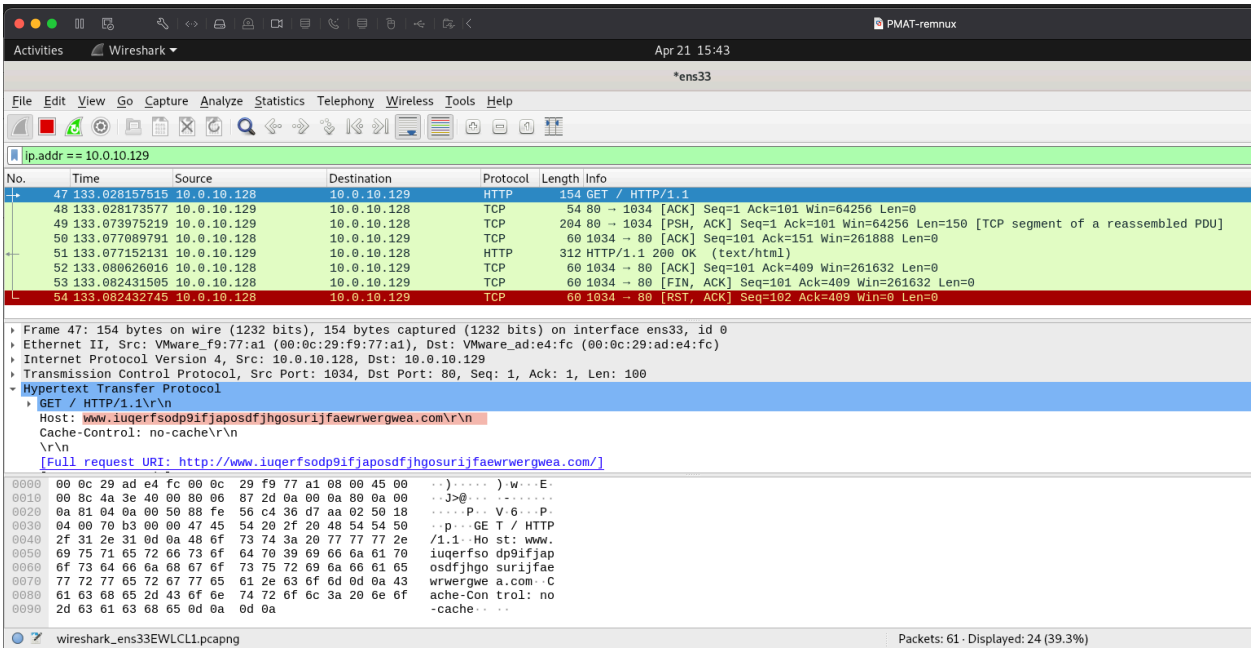
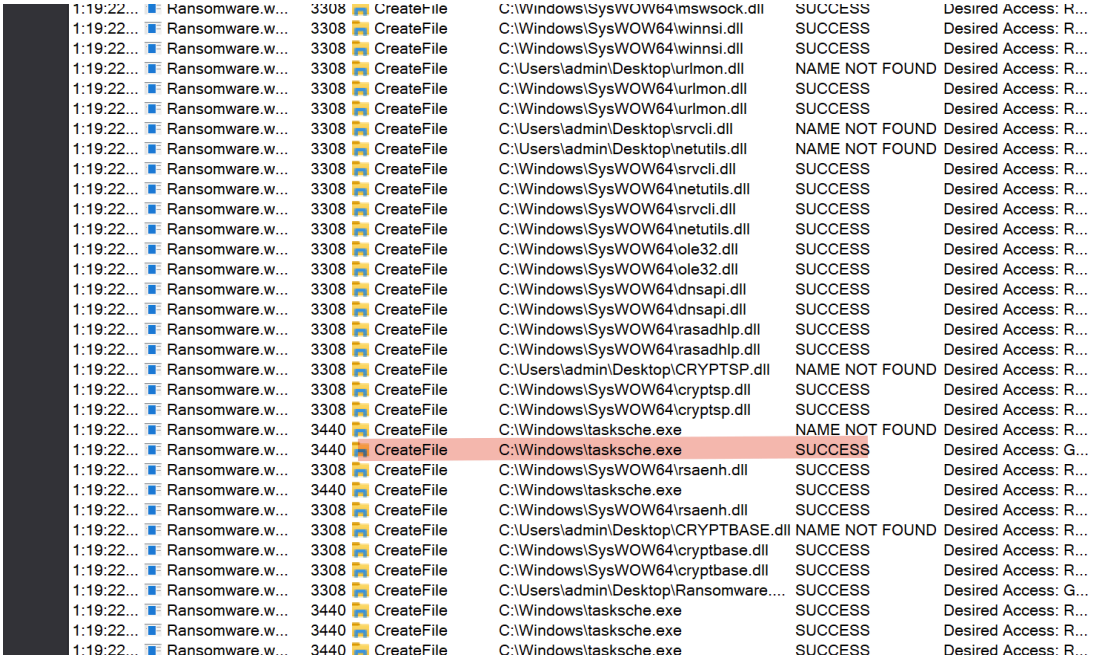


Fig 8: Communication to the kill switch URL

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

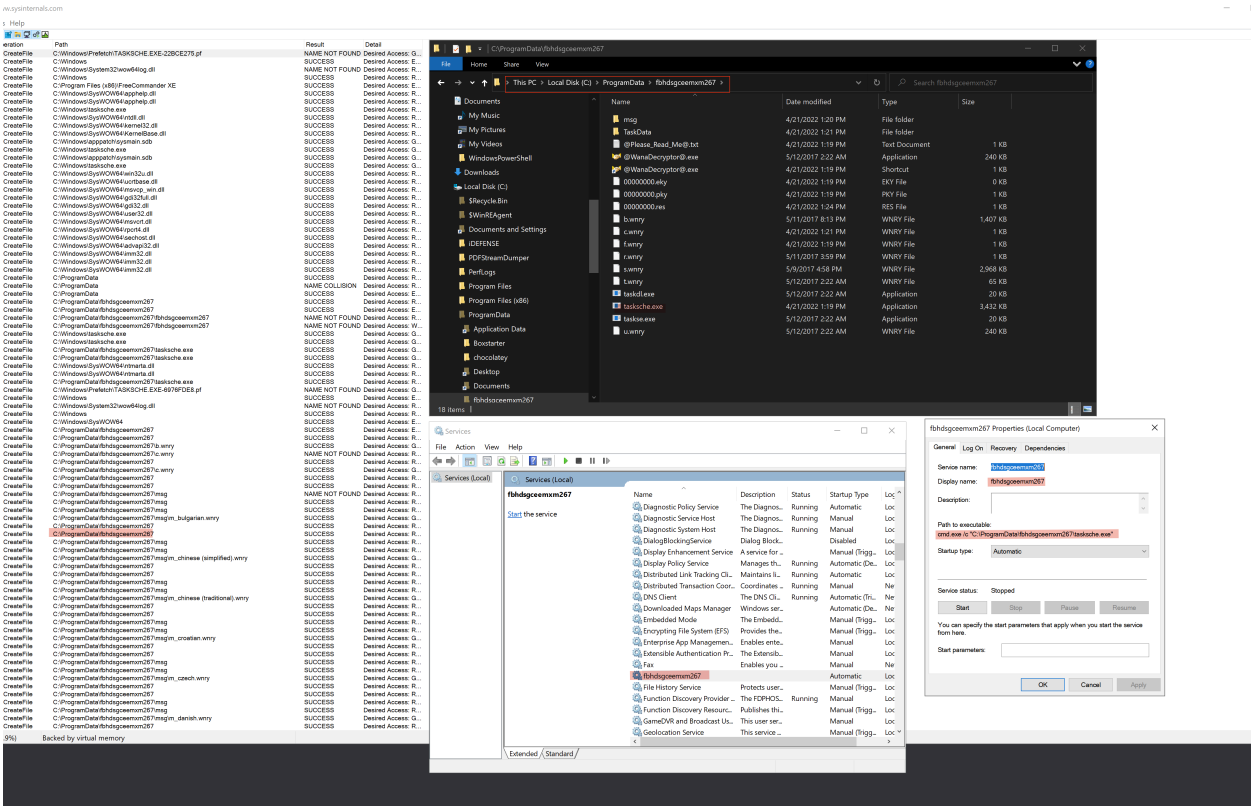


Fig 10: The created hidden folder and new service

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	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	mssecsvc2.0
Ransomware.wannacry...	5940	TCP	Syn Sent	169.254.44.118	1199	169.254.119.1	445	4/21/2022 1:12:47 PM	mssecsvc2.0
Ransomware.wannacry...	5940	TCP	Syn Sent	10.0.10.128	1200	17.12.234.232	445	4/21/2022 1:12:47 PM	mssecsvc2.0
Ransomware.wannacry...	5940	TCP	Syn Sent	10.0.10.128	1201	33.197.20.132	445	4/21/2022 1:12:47 PM	mssecsvc2.0
Ransomware.wannacry...	5940	TCP	Syn Sent	169.254.44.118	1202	169.254.120.1	445	4/21/2022 1:12:47 PM	mssecsvc2.0
Ransomware.wannacry...	5940	TCP	Syn Sent	169.254.44.118	1203	169.254.121.1	445	4/21/2022 1:12:47 PM	mssecsvc2.0
Ransomware.wannacry...	5940	TCP	Syn Sent	169.254.44.118	1204	169.254.122.1	445	4/21/2022 1:12:47 PM	mssecsvc2.0
Ransomware.wannacry...	5940	TCP	Syn Sent	10.0.10.128	1205	40.124.196.211	445	4/21/2022 1:12:47 PM	mssecsvc2.0
Ransomware.wannacry...	5940	TCP	Syn Sent	10.0.10.128	1206	175.91.35.3	445	4/21/2022 1:12:47 PM	mssecsvc2.0
Ransomware.wannacry...	5940	TCP	Syn Sent	169.254.44.118	1207	169.254.123.1	445	4/21/2022 1:12:47 PM	mssecsvc2.0
Ransomware.wannacry...	5940	TCP	Syn Sent	169.254.44.118	1208	169.254.124.1	445	4/21/2022 1:12:47 PM	mssecsvc2.0
Ransomware.wannacry...	5940	TCP	Syn Sent	10.0.10.128	1209	133.182.72.100	445	4/21/2022 1:12:47 PM	mssecsvc2.0
Ransomware.wannacry...	5940	TCP	Syn Sent	169.254.44.118	1210	169.254.125.1	445	4/21/2022 1:12:47 PM	mssecsvc2.0
Ransomware.wannacry...	5940	TCP	Syn Sent	169.254.44.118	1211	169.254.126.1	445	4/21/2022 1:12:48 PM	mssecsvc2.0
Ransomware.wannacry...	5940	TCP	Syn Sent	10.0.10.128	1212	25.128.196.194	445	4/21/2022 1:12:48 PM	mssecsvc2.0
Ransomware.wannacry...	5940	TCP	Syn Sent	169.254.44.118	1213	169.254.127.1	445	4/21/2022 1:12:48 PM	mssecsvc2.0
Ransomware.wannacry...	5940	TCP	Syn Sent	169.254.44.118	1214	169.254.128.1	445	4/21/2022 1:12:48 PM	mssecsvc2.0
svchost.exe	6068	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	4/21/2022 7:14:42 AM	CDPSvc
lsass.exe	696	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	4/21/2022 7:12:30 AM	lsass.exe
wininit.exe	556	TCP	Listen	0.0.0.0	49665	0.0.0.0	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.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.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.

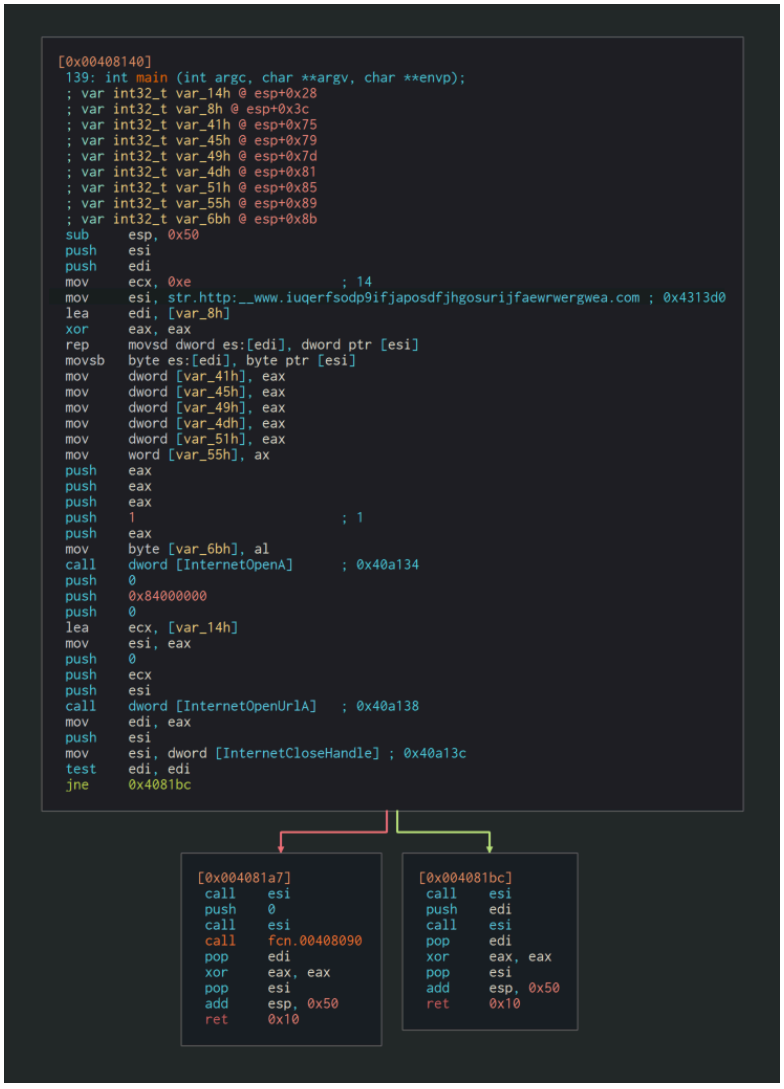


Fig 13: Check of the URL existence

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.

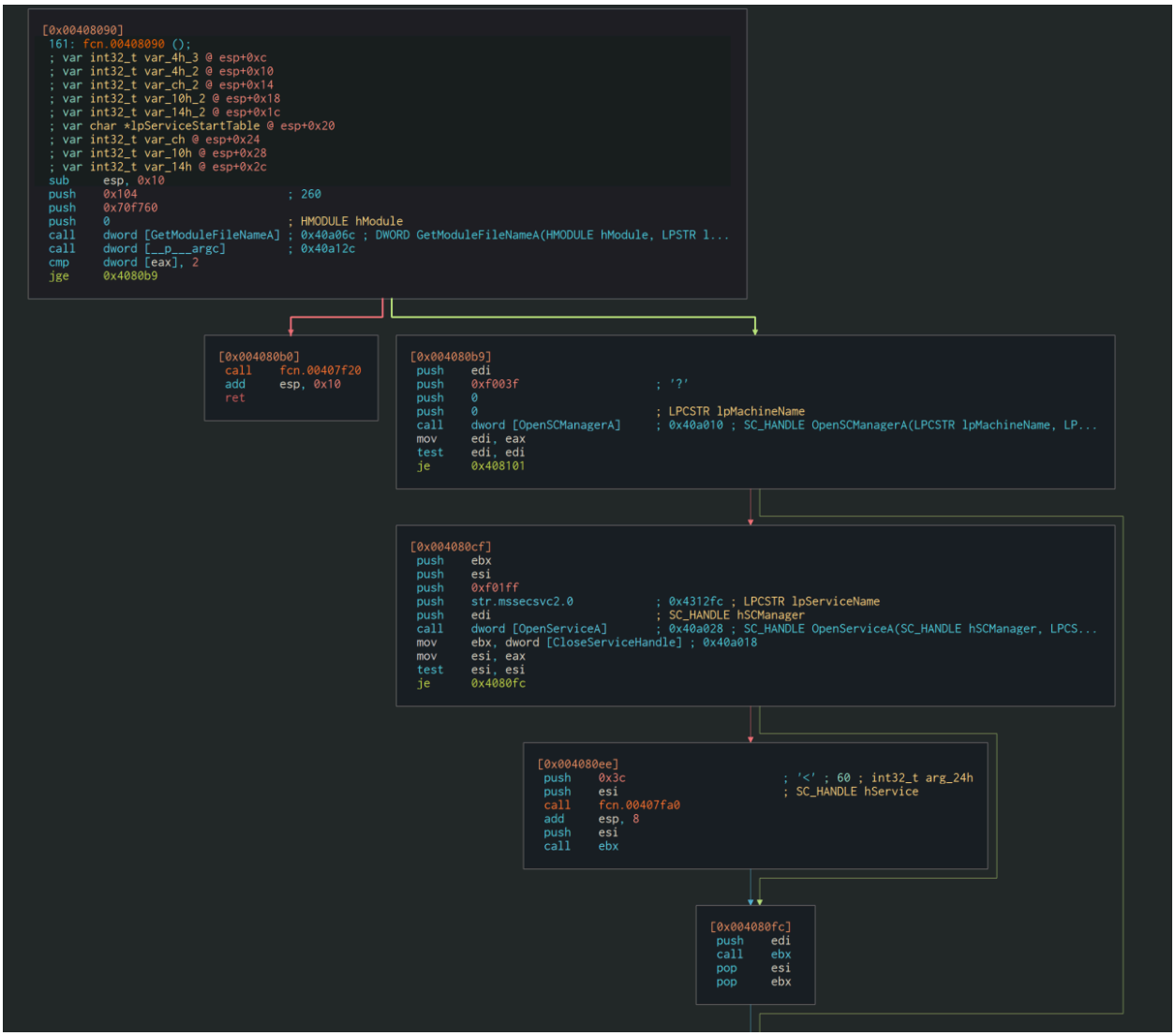


Fig 14: The detection of the first run

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
2  undefined4 wannacryCreateAndStartService(void)
3
4  {
5    SC_HANDLE hSCManager;
6    SC_HANDLE hService;
7    char local_104 [260];
8
9    sprintf(local_104,s_%s_-m_security_00431330,&wannacryFileName);
.0   hSCManager = OpenSCManagerA((LPCSTR)0x0,(LPCSTR)0x0,0xf003f);
.1   if (hSCManager != (SC_HANDLE)0x0) {
.2     hService = CreateServiceA(hSCManager,s_mssecsvc2.0_004312fc,
.3                               s_Microsoft_Security_Center_(2.0)_S_00431308,0xf01ff,0x10,2,1,
.4                               local_104,(LPCSTR)0x0,(LPDWORD)0x0,(LPCSTR)0x0,(LPCSTR)0x0,(LPCSTR)0x0
.5                              );
.6     if (hService != (SC_HANDLE)0x0) {
.7       StartServiceA(hService,0,(LPCSTR *)0x0);
.8       CloseServiceHandle(hService);
.9     }
:0     CloseServiceHandle(hSCManager);
:1     return 0;
:2   }
:3   return 0;
:4 }
:5
```

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)0x
     (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 = 0x40; 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.

```
00407E97   F7D1                    not ecx
00407E99   2BF9                    sub edi,ecx
00407E9B   895C24 14               mov dword ptr ss:[esp+14],ebx
00407E9F   8BF7                    mov esi,edi                    esi:"C:\\%s\\qeriuwjhrf"
00407EA1   8BE9                    mov ebp,ecx
00407EA3   8BFA                    mov edi,edx                    edx:"C:\\WINDOWS\\tasksche.exe /i"
00407EA5   83C9 FF                 or ecx,FFFFFFFF
00407EA8   F2:AE                   repne scasb
00407EAA   8BCD                    mov ecx,ebp
00407EAC   4F                      dec edi
00407EAD   C1E9 02                 shr ecx,2
00407EB0   F3:A5                   rep movsd
00407EB2   8BCD                    mov ecx,ebp
00407EB4   8D4424 14               lea eax,dword ptr ss:[esp+14]
00407EB8   83E1 03                 and ecx,3
00407EBB   50                      push eax
00407EBC   F3:A4                   rep movsb
00407EBE   8D4C24 28               lea ecx,dword ptr ss:[esp+28]
00407EC2   8D5424 6C               lea edx,dword ptr ss:[esp+6C]
00407EC6   51                      push ecx
00407EC7   53                      push ebx
00407EC8   53                      push ebx
00407EC9   68 00000008             push 8000000
00407ECE   53                      push ebx
00407ECF   53                      push ebx
00407ED0   53                      push ebx
00407ED1   52                      push edx                       edx:"C:\\WINDOWS\\tasksche.exe /i"
00407ED2   53                      push ebx
00407ED3   C74424 4C 44000000      mov dword ptr ss:[esp+4C],44   44:'D'
00407EDB   66:895C24 7C            mov word ptr ss:[esp+7C],bx
00407EE0   C74424 78 81000000      mov dword ptr ss:[esp+78],81
00407EE8   FF15 78144300           call dword ptr ds:[<&CreateProcessA> ]
00407EEE   85C0                    test eax,eax
00407EF0   74 16                   je ransomware.wannacry.407F08
```

Fig 17: Triggering of the tasksche.exe

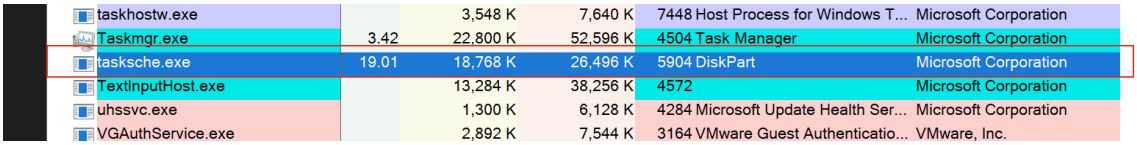


Fig 18: Triggered tasksche.exe

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.

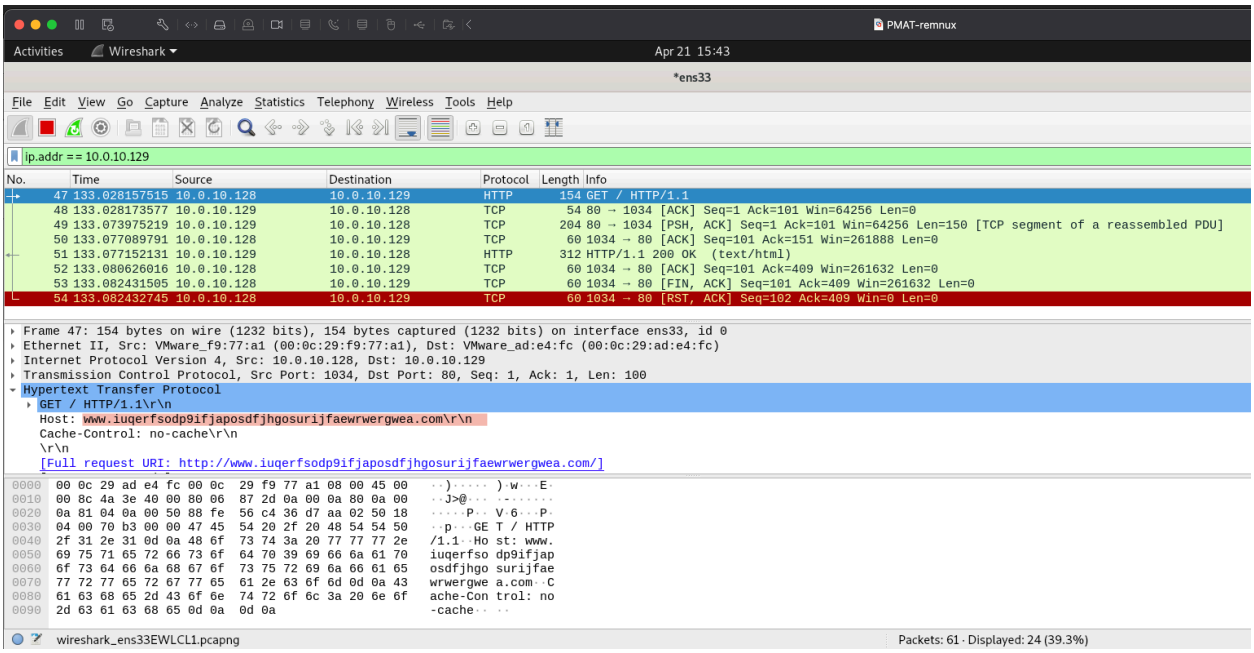


Fig 19: WireShark Packet Capture of kill switch URL

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	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	mssecsvc2.0
Ransomware.wannacry...	5940	TCP	Syn Sent	169.254.44.118	1199	169.254.119.1	445	4/21/2022 1:12:47 PM	mssecsvc2.0
Ransomware.wannacry...	5940	TCP	Syn Sent	10.0.10.128	1200	17.12.234.232	445	4/21/2022 1:12:47 PM	mssecsvc2.0
Ransomware.wannacry...	5940	TCP	Syn Sent	10.0.10.128	1201	33.197.20.132	445	4/21/2022 1:12:47 PM	mssecsvc2.0
Ransomware.wannacry...	5940	TCP	Syn Sent	169.254.44.118	1202	169.254.120.1	445	4/21/2022 1:12:47 PM	mssecsvc2.0
Ransomware.wannacry...	5940	TCP	Syn Sent	169.254.44.118	1203	169.254.121.1	445	4/21/2022 1:12:47 PM	mssecsvc2.0
Ransomware.wannacry...	5940	TCP	Syn Sent	169.254.44.118	1204	169.254.122.1	445	4/21/2022 1:12:47 PM	mssecsvc2.0
Ransomware.wannacry...	5940	TCP	Syn Sent	10.0.10.128	1205	40.124.196.211	445	4/21/2022 1:12:47 PM	mssecsvc2.0
Ransomware.wannacry...	5940	TCP	Syn Sent	10.0.10.128	1206	175.91.35.3	445	4/21/2022 1:12:47 PM	mssecsvc2.0
Ransomware.wannacry...	5940	TCP	Syn Sent	169.254.44.118	1207	169.254.123.1	445	4/21/2022 1:12:47 PM	mssecsvc2.0
Ransomware.wannacry...	5940	TCP	Syn Sent	169.254.44.118	1208	169.254.124.1	445	4/21/2022 1:12:47 PM	mssecsvc2.0
Ransomware.wannacry...	5940	TCP	Syn Sent	10.0.10.128	1209	133.182.72.100	445	4/21/2022 1:12:47 PM	mssecsvc2.0
Ransomware.wannacry...	5940	TCP	Syn Sent	169.254.44.118	1210	169.254.125.1	445	4/21/2022 1:12:47 PM	mssecsvc2.0
Ransomware.wannacry...	5940	TCP	Syn Sent	169.254.44.118	1211	169.254.126.1	445	4/21/2022 1:12:48 PM	mssecsvc2.0
Ransomware.wannacry...	5940	TCP	Syn Sent	10.0.10.128	1212	25.128.196.194	445	4/21/2022 1:12:48 PM	mssecsvc2.0
Ransomware.wannacry...	5940	TCP	Syn Sent	169.254.44.118	1213	169.254.127.1	445	4/21/2022 1:12:48 PM	mssecsvc2.0
Ransomware.wannacry...	5940	TCP	Syn Sent	169.254.44.118	1214	169.254.128.1	445	4/21/2022 1:12:48 PM	mssecsvc2.0
svchost.exe	6068	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	4/21/2022 7:14:42 AM	CDPSvc
lsass.exe	696	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	4/21/2022 7:12:30 AM	lsass.exe
wininit.exe	556	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	4/21/2022 7:12:30 AM	wininit.exe

Fig 20: Attempted communication to anther 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

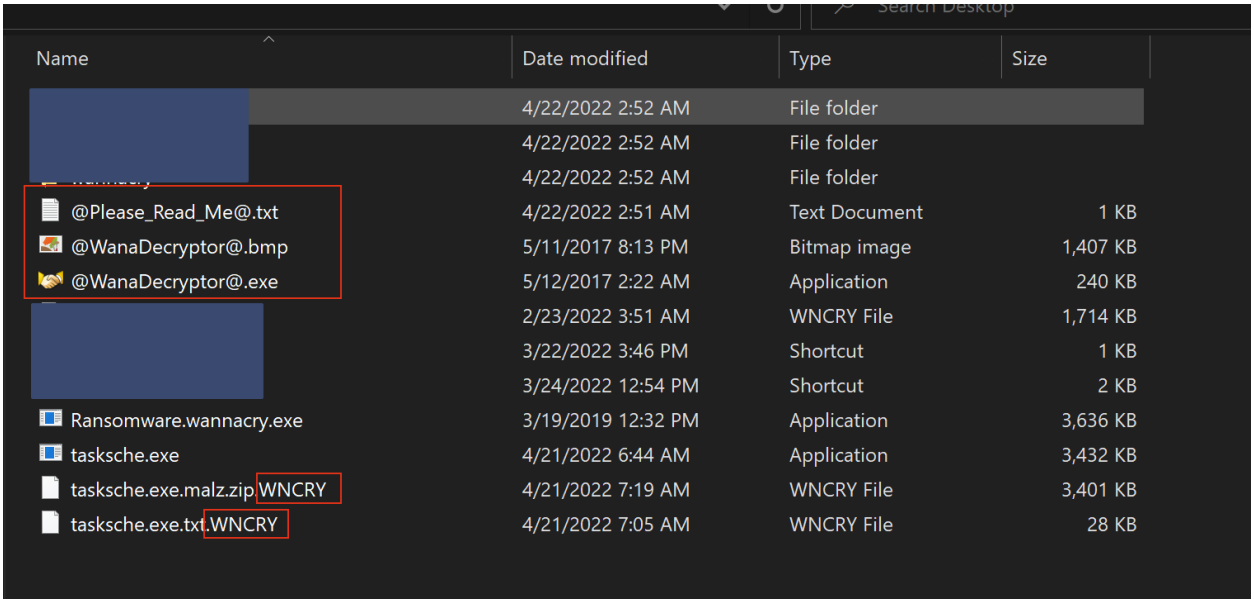


Fig 21: Files on the user's desktop

Rules & Signatures

```
rule wannacry_detection {

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

    strings:
        $url = "www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.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)
}
```