Practical Malware Analysis & Triage

Malware Analysis Report

WannaCry Ransomware Malware

Oct 2022 | Mubeen Gulzar | v1.0

Table of Contents

Executive Summary

File Name	SHA256 Hash
Trojan.Ransomware.WannaCrypt	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c

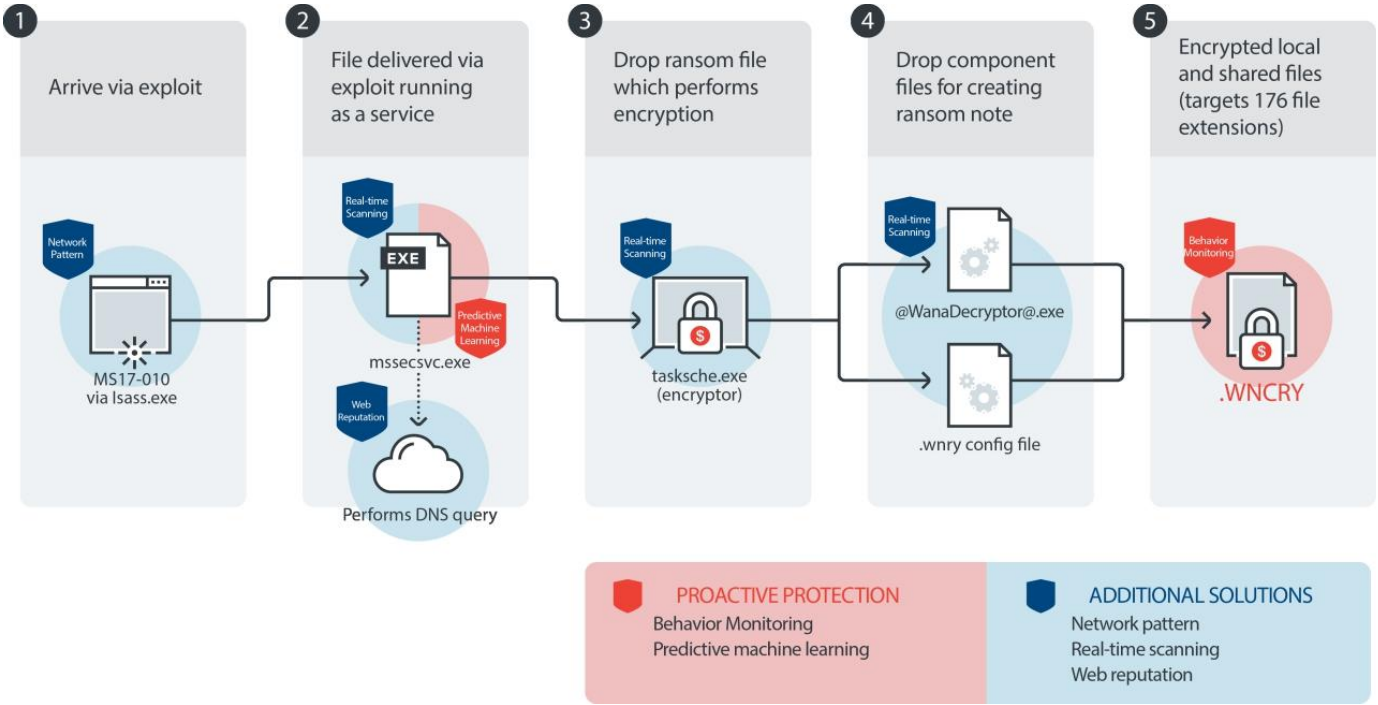
WannaCry is a ransomware cryptoworm first identified in May, 2017 as part of a massive worldwide cyberattack, which targeted computers running the Microsoft Windows operating system by encrypting (locking) data and demanding ransom payments in the Bitcoin cryptocurrency. The worm is also known as WannaCrypt, Wana Decrypt0r 2.0, WanaCrypt0r 2.0, and Wanna Decryptor. It is considered a network worm because it also includes a transport mechanism to automatically spread itself. This transport code scans for vulnerable systems, then uses the EternalBlue exploit to gain access, and the DoublePulsar tool to install and execute a copy of itself. WannaCry versions 0, 1, and 2 were created using Microsoft Visual C++ 6.0.

When executed, the WannaCry malware first checks the kill switch domain name; if it is not found, then the ransomware encrypts the computer's data, then attempts to exploit the SMB vulnerability to spread out to random computers on the Internet, and laterally to computers on the same network. As with other modern ransomware, the payload displays a message informing the user that their files have been encrypted, and demands a payment in bitcoin

YARA signature rules are attached in Appendix A. Malware sample and hashes have been submitted to VirusTotal for further examination.

High-Level Technical Summary

WannaCry Ransomware consists of a primary and a secondary payload. The initial payload tries to connect to a hardcoded domain (killswitch mechanism), if the connection is unsuccessful the payload spawns the secondary payload which is the actual WannaCry encryptor, it starts encrypting the victim's files while simultaneously exploiting the SMB Eternalblue vulnerability to propagate itself on the internet and computers on the same network.



Malware Composition

WannaCry consists of the following components:

File Name	SHA256 Hash
Ransomware.WannaCry.exe	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
tasksche.exe	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
@WannaDecryptor.exe	b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25

Ransomware.WannaCry.exe

This is the initial executable which checks the internet for the availability of a hardcoded domain which acts as a killswitch for the infection hence if the domain cannot be reached then the infection moves on to the 2nd stage, otherwise the infection stops.

tasksche.exe:

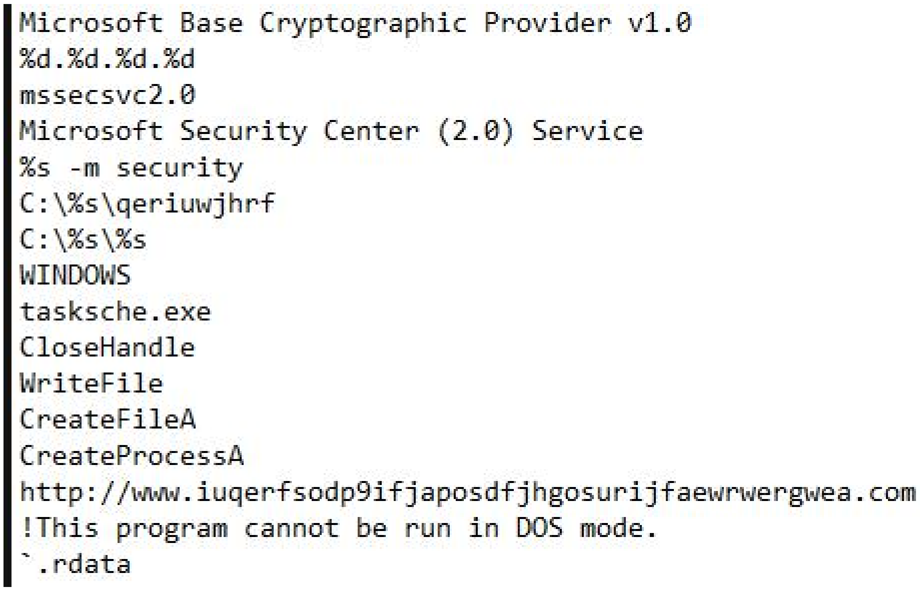
During the 2nd stage the malware starts encrypting the drives and looks for other PCs within the subnet through SMB so that it can infect those PCs. This process goes on until each and every PC is infected within the subnet with their files fully encrypted. This is achieved using the tasksche.exe executable created by the initial executable.

@WannaDecryptor.exe:

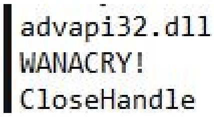
After the system files are fully encrypted, this executable is responsible for displaying a message to the user that the system has been infected with the ransomware and they need to pay a certain amount of bitcoins within a specific time period to recover the system files.

Basic Static Analysis

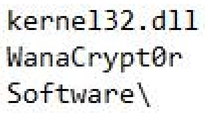
{Screenshots and description about basic static artifacts and methods}



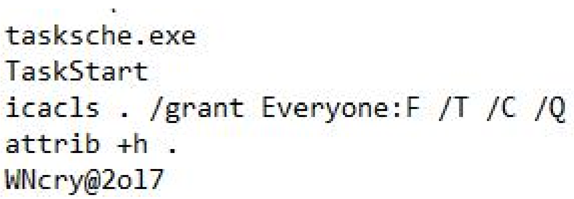
```
Microsoft Base Cryptographic Provider v1.0
%d.%d.%d.%d
mssecsvc2.0
Microsoft Security Center (2.0) Service
%s -m security
C:\%s\qeriuwjhrf
C:\%s\%s
WINDOWS
tasksche.exe
CloseHandle
WriteFile
CreateFileA
CreateProcessA
http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
!This program cannot be run in DOS mode.
`.rdata
```



```
advapi32.dll
WANACRY!
CloseHandle
```



```
kernel32.dll
WanaCrypt0r
Software\
```



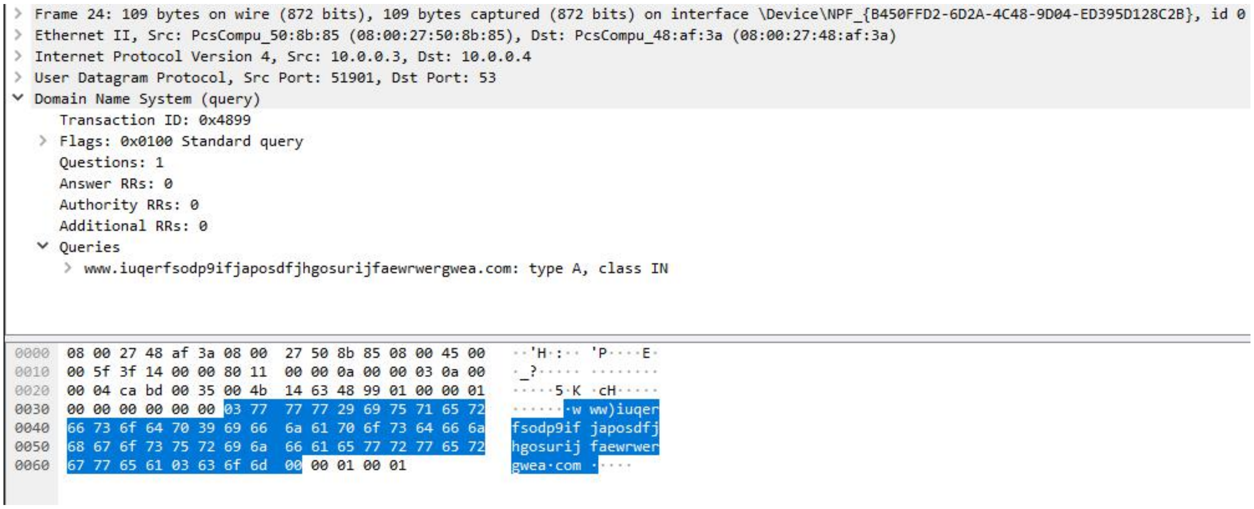
```
tasksche.exe
TaskStart
icacls . /grant Everyone:F /T /C /Q
attrib +h .
WNcry@2ol7
```

A lot of suspicious strings within the FLOSS output including the hardcoded url, tasksche.exe and WanaCRY!/WanaCrypt0r/WNcry@2o17 strings

Theres also a “icacls” command executing with a hidden attribute which is granting all user permissions to the current and sub-directories (For File Encryption)

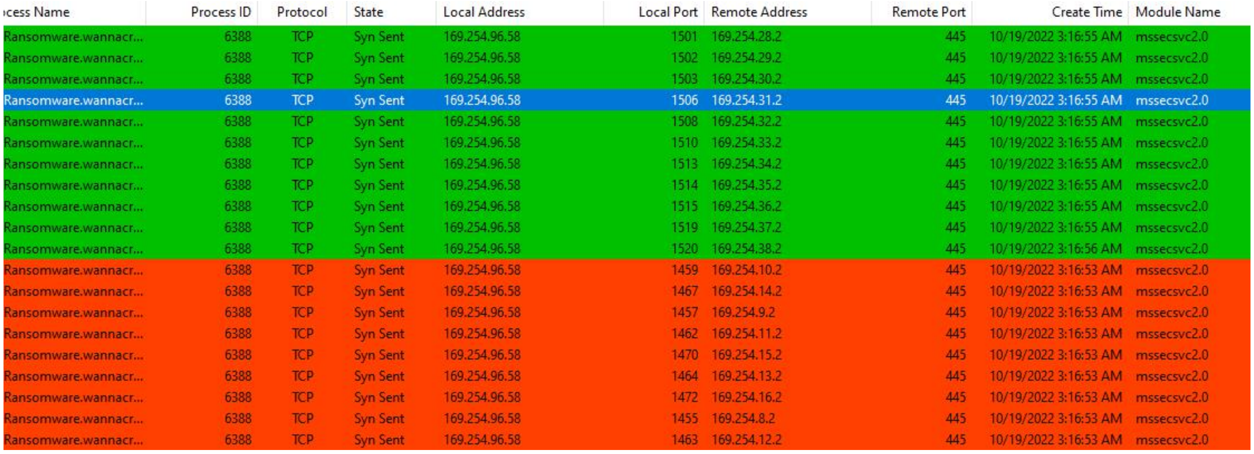
Basic Dynamic Analysis

{Screenshots and description about basic dynamic artifacts and methods}



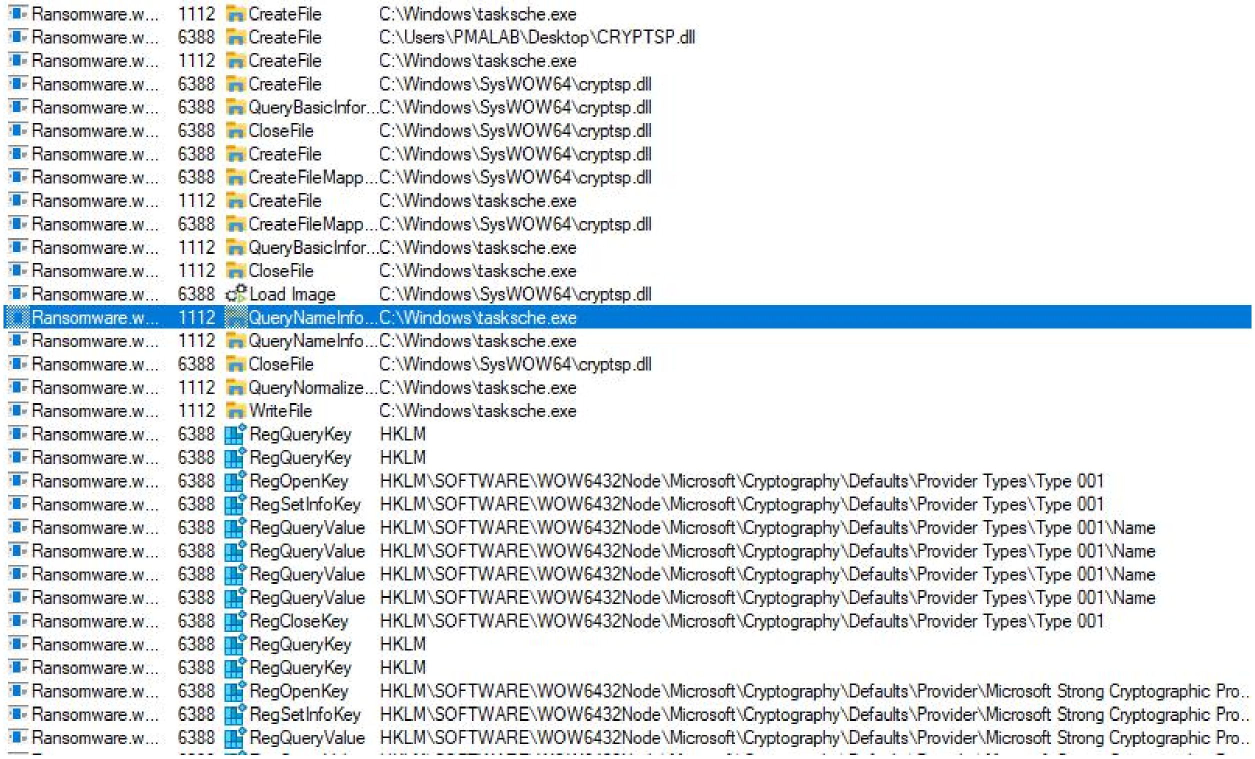
```
> Frame 24: 109 bytes on wire (872 bits), 109 bytes captured (872 bits) on interface \Device\NPF_{B450FFD2-6D2A-4C48-9D04-ED395D128C2B}, id 0
> Ethernet II, Src: PcsCompu_50:8b:85 (08:00:27:50:8b:85), Dst: PcsCompu_48:af:3a (08:00:27:48:af:3a)
> Internet Protocol Version 4, Src: 10.0.0.3, Dst: 10.0.0.4
> User Datagram Protocol, Src Port: 51901, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x4899
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com: type A, class IN

0000  08 00 27 48 af 3a 08 00  27 50 8b 85 08 00 45 00   ··'H·:·· 'P····E·
0010  00 5f 3f 14 00 00 80 11  00 00 0a 00 00 03 0a 00   ·_?····· ········
0020  00 04 ca bd 00 35 00 4b  14 63 48 99 01 00 00 01   ·····5·K ·cH·····
0030  00 00 00 00 00 00 03 77  77 77 29 69 75 71 65 72   ·······w ww)iuqer
0040  66 73 6f 64 70 39 69 66  6a 61 70 6f 73 64 66 6a   fsodp9if japosdfj
0050  68 67 6f 73 75 72 69 6a  66 61 65 77 72 77 65 72   hgosurij faewrwer
0060  67 77 65 61 03 63 6f 6d  00 00 01 00 01            gwea·com ·····
```

The Initial Malware trying to reach the hardcoded domain - (Wireshark)



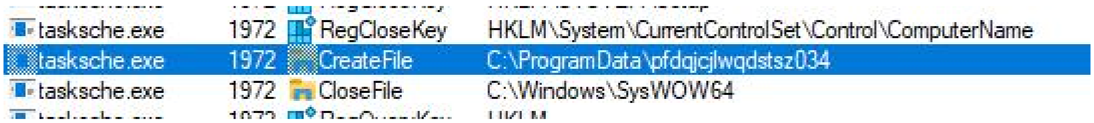
›cess Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
Ransomware.wannacr...	6388	TCP	Syn Sent	169.254.96.58	1501	169.254.28.2	445	10/19/2022 3:16:55 AM	mssecsvc2.0
Ransomware.wannacr...	6388	TCP	Syn Sent	169.254.96.58	1502	169.254.29.2	445	10/19/2022 3:16:55 AM	mssecsvc2.0
Ransomware.wannacr...	6388	TCP	Syn Sent	169.254.96.58	1503	169.254.30.2	445	10/19/2022 3:16:55 AM	mssecsvc2.0
Ransomware.wannacr...	6388	TCP	Syn Sent	169.254.96.58	1506	169.254.31.2	445	10/19/2022 3:16:55 AM	mssecsvc2.0
Ransomware.wannacr...	6388	TCP	Syn Sent	169.254.96.58	1508	169.254.32.2	445	10/19/2022 3:16:55 AM	mssecsvc2.0
Ransomware.wannacr...	6388	TCP	Syn Sent	169.254.96.58	1510	169.254.33.2	445	10/19/2022 3:16:55 AM	mssecsvc2.0
Ransomware.wannacr...	6388	TCP	Syn Sent	169.254.96.58	1513	169.254.34.2	445	10/19/2022 3:16:55 AM	mssecsvc2.0
Ransomware.wannacr...	6388	TCP	Syn Sent	169.254.96.58	1514	169.254.35.2	445	10/19/2022 3:16:55 AM	mssecsvc2.0
Ransomware.wannacr...	6388	TCP	Syn Sent	169.254.96.58	1515	169.254.36.2	445	10/19/2022 3:16:55 AM	mssecsvc2.0
Ransomware.wannacr...	6388	TCP	Syn Sent	169.254.96.58	1519	169.254.37.2	445	10/19/2022 3:16:55 AM	mssecsvc2.0
Ransomware.wannacr...	6388	TCP	Syn Sent	169.254.96.58	1520	169.254.38.2	445	10/19/2022 3:16:56 AM	mssecsvc2.0
Ransomware.wannacr...	6388	TCP	Syn Sent	169.254.96.58	1459	169.254.10.2	445	10/19/2022 3:16:53 AM	mssecsvc2.0
Ransomware.wannacr...	6388	TCP	Syn Sent	169.254.96.58	1467	169.254.14.2	445	10/19/2022 3:16:53 AM	mssecsvc2.0
Ransomware.wannacr...	6388	TCP	Syn Sent	169.254.96.58	1457	169.254.9.2	445	10/19/2022 3:16:53 AM	mssecsvc2.0
Ransomware.wannacr...	6388	TCP	Syn Sent	169.254.96.58	1462	169.254.11.2	445	10/19/2022 3:16:53 AM	mssecsvc2.0
Ransomware.wannacr...	6388	TCP	Syn Sent	169.254.96.58	1470	169.254.15.2	445	10/19/2022 3:16:53 AM	mssecsvc2.0
Ransomware.wannacr...	6388	TCP	Syn Sent	169.254.96.58	1464	169.254.13.2	445	10/19/2022 3:16:53 AM	mssecsvc2.0
Ransomware.wannacr...	6388	TCP	Syn Sent	169.254.96.58	1472	169.254.16.2	445	10/19/2022 3:16:53 AM	mssecsvc2.0
Ransomware.wannacr...	6388	TCP	Syn Sent	169.254.96.58	1455	169.254.8.2	445	10/19/2022 3:16:53 AM	mssecsvc2.0
Ransomware.wannacr...	6388	TCP	Syn Sent	169.254.96.58	1463	169.254.12.2	445	10/19/2022 3:16:53 AM	mssecsvc2.0

The Malware executes the mssesvc2.0.exe for Windows SMB Remote Host Exploitation - (tcpview)



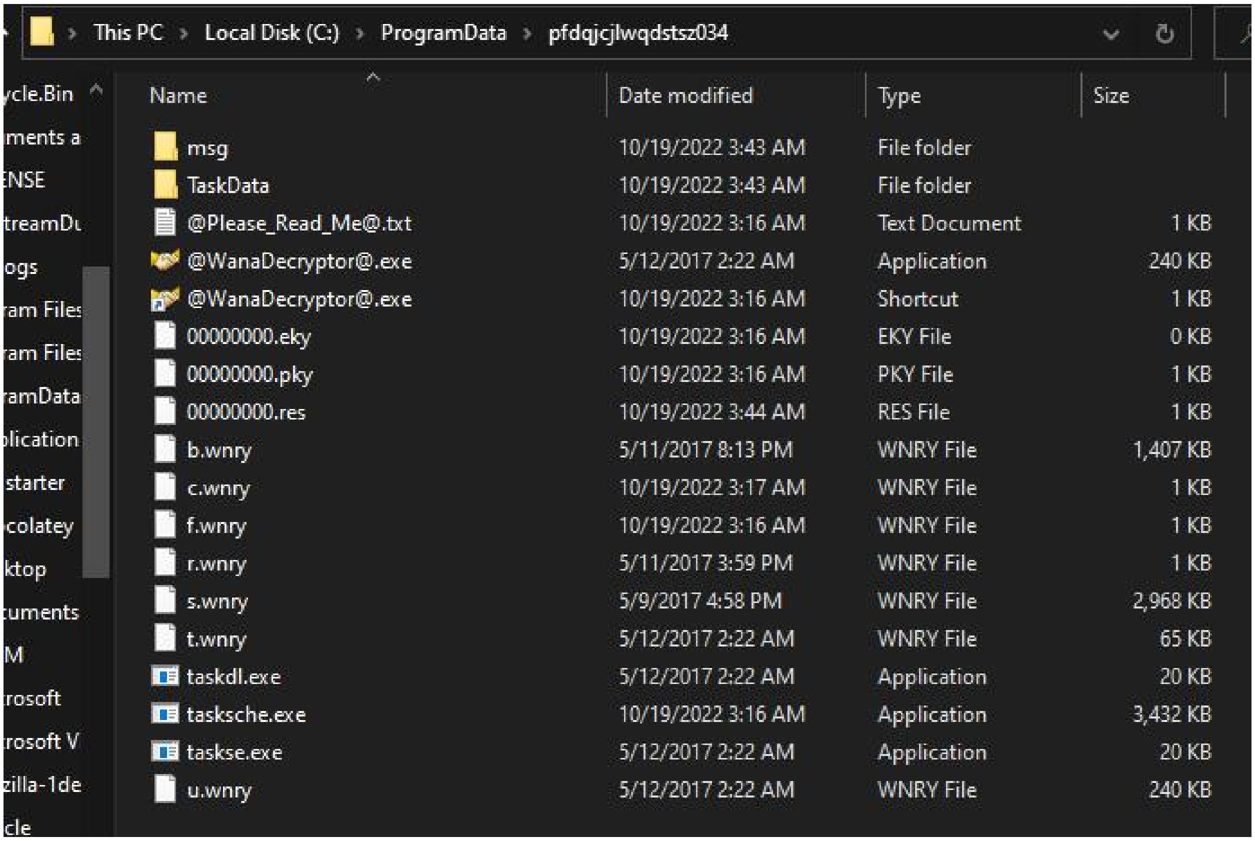
```
Ransomware.w...  1112  CreateFile         C:\Windows\tasksche.exe
Ransomware.w...  6388  CreateFile         C:\Users\PMALAB\Desktop\CRYPTSP.dll
Ransomware.w...  1112  CreateFile         C:\Windows\tasksche.exe
Ransomware.w...  6388  CreateFile         C:\Windows\SysWOW64\cryptsp.dll
Ransomware.w...  6388  QueryBasicInfor...C:\Windows\SysWOW64\cryptsp.dll
Ransomware.w...  6388  CloseFile          C:\Windows\SysWOW64\cryptsp.dll
Ransomware.w...  6388  CreateFile         C:\Windows\SysWOW64\cryptsp.dll
Ransomware.w...  6388  CreateFileMapp...C:\Windows\SysWOW64\cryptsp.dll
Ransomware.w...  1112  CreateFile         C:\Windows\tasksche.exe
Ransomware.w...  6388  CreateFileMapp...C:\Windows\SysWOW64\cryptsp.dll
Ransomware.w...  1112  QueryBasicInfor...C:\Windows\tasksche.exe
Ransomware.w...  1112  CloseFile          C:\Windows\tasksche.exe
Ransomware.w...  6388  Load Image         C:\Windows\SysWOW64\cryptsp.dll
Ransomware.w...  1112  QueryNameInfo...C:\Windows\tasksche.exe
Ransomware.w...  1112  QueryNameInfo...C:\Windows\tasksche.exe
Ransomware.w...  6388  CloseFile          C:\Windows\SysWOW64\cryptsp.dll
Ransomware.w...  1112  QueryNormalize...C:\Windows\tasksche.exe
Ransomware.w...  1112  WriteFile          C:\Windows\tasksche.exe
Ransomware.w...  6388  RegQueryKey        HKLM
Ransomware.w...  6388  RegQueryKey        HKLM
Ransomware.w...  6388  RegOpenKey         HKLM\SOFTWARE\WOW6432Node\Microsoft\Cryptography\Defaults\Provider Types\Type 001
Ransomware.w...  6388  RegSetInfoKey      HKLM\SOFTWARE\WOW6432Node\Microsoft\Cryptography\Defaults\Provider Types\Type 001
Ransomware.w...  6388  RegQueryValue      HKLM\SOFTWARE\WOW6432Node\Microsoft\Cryptography\Defaults\Provider Types\Type 001\Name
Ransomware.w...  6388  RegQueryValue      HKLM\SOFTWARE\WOW6432Node\Microsoft\Cryptography\Defaults\Provider Types\Type 001\Name
Ransomware.w...  6388  RegQueryValue      HKLM\SOFTWARE\WOW6432Node\Microsoft\Cryptography\Defaults\Provider Types\Type 001\Name
Ransomware.w...  6388  RegQueryValue      HKLM\SOFTWARE\WOW6432Node\Microsoft\Cryptography\Defaults\Provider Types\Type 001\Name
Ransomware.w...  6388  RegCloseKey        HKLM\SOFTWARE\WOW6432Node\Microsoft\Cryptography\Defaults\Provider Types\Type 001
Ransomware.w...  6388  RegQueryKey        HKLM
Ransomware.w...  6388  RegQueryKey        HKLM
Ransomware.w...  6388  RegOpenKey         HKLM\SOFTWARE\WOW6432Node\Microsoft\Cryptography\Defaults\Provider\Microsoft Strong Cryptographic Pro..
Ransomware.w...  6388  RegSetInfoKey      HKLM\SOFTWARE\WOW6432Node\Microsoft\Cryptography\Defaults\Provider\Microsoft Strong Cryptographic Pro..
Ransomware.w...  6388  RegQueryValue      HKLM\SOFTWARE\WOW6432Node\Microsoft\Cryptography\Defaults\Provider\Microsoft Strong Cryptographic Pro..
```

tasksche.exe is executed so that the encryption process can begin! - (procmon)



```
tasksche.exe    1972  RegCloseKey   HKLM\System\CurrentControlSet\Control\ComputerName
tasksche.exe    1972  CreateFile    C:\ProgramData\pfdqjcjlwqdstsz034
tasksche.exe    1972  CloseFile     C:\Windows\SysWOW64
```

A folder within %ProgramData% is created with a random string as its name - (procmon)

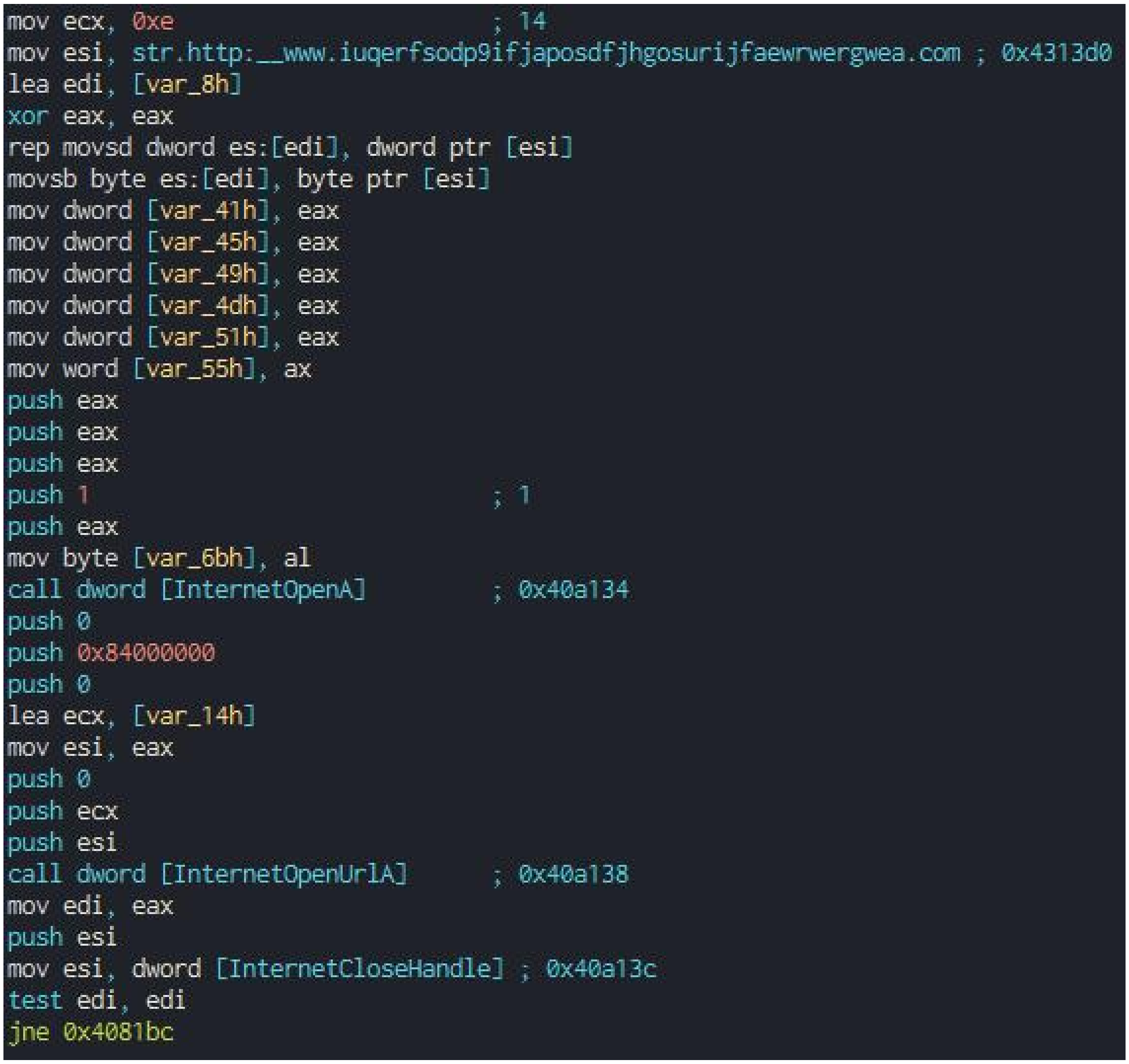


Name	Date modified	Type	Size
msg	10/19/2022 3:43 AM	File folder	
TaskData	10/19/2022 3:43 AM	File folder	
@Please_Read_Me@.txt	10/19/2022 3:16 AM	Text Document	1 KB
@WanaDecryptor@.exe	5/12/2017 2:22 AM	Application	240 KB
@WanaDecryptor@.exe	10/19/2022 3:16 AM	Shortcut	1 KB
00000000.eky	10/19/2022 3:16 AM	EKY File	0 KB
00000000.pky	10/19/2022 3:16 AM	PKY File	1 KB
00000000.res	10/19/2022 3:44 AM	RES File	1 KB
b.wnry	5/11/2017 8:13 PM	WNRY File	1,407 KB
c.wnry	10/19/2022 3:17 AM	WNRY File	1 KB
f.wnry	10/19/2022 3:16 AM	WNRY File	1 KB
r.wnry	5/11/2017 3:59 PM	WNRY File	1 KB
s.wnry	5/9/2017 4:58 PM	WNRY File	2,968 KB
t.wnry	5/12/2017 2:22 AM	WNRY File	65 KB
taskdl.exe	5/12/2017 2:22 AM	Application	20 KB
tasksche.exe	10/19/2022 3:16 AM	Application	3,432 KB
taskse.exe	5/12/2017 2:22 AM	Application	20 KB
u.wnry	5/12/2017 2:22 AM	WNRY File	240 KB

This folder contains all the necessary files for the WannaCry Ransomware including the ReadME.txt and WanaDecryptor.exe

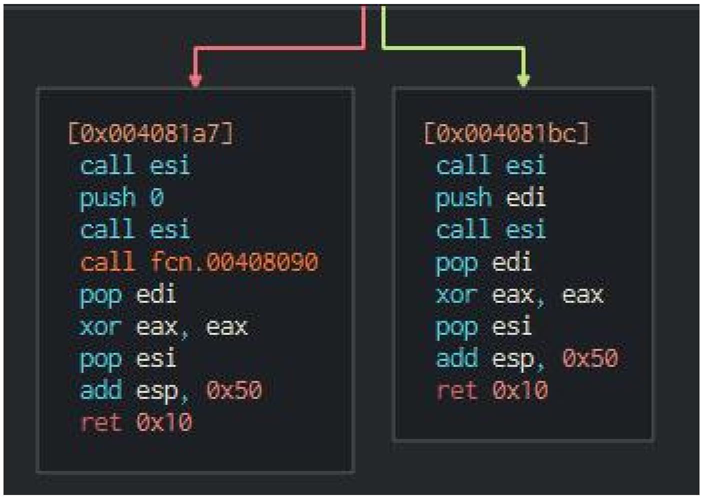
Advanced Static Analysis

{Screenshots and description about findings during advanced static analysis}



```
mov ecx, 0xe                      ; 14
mov esi, str.http:__www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.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                            ; 1
push eax
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
```

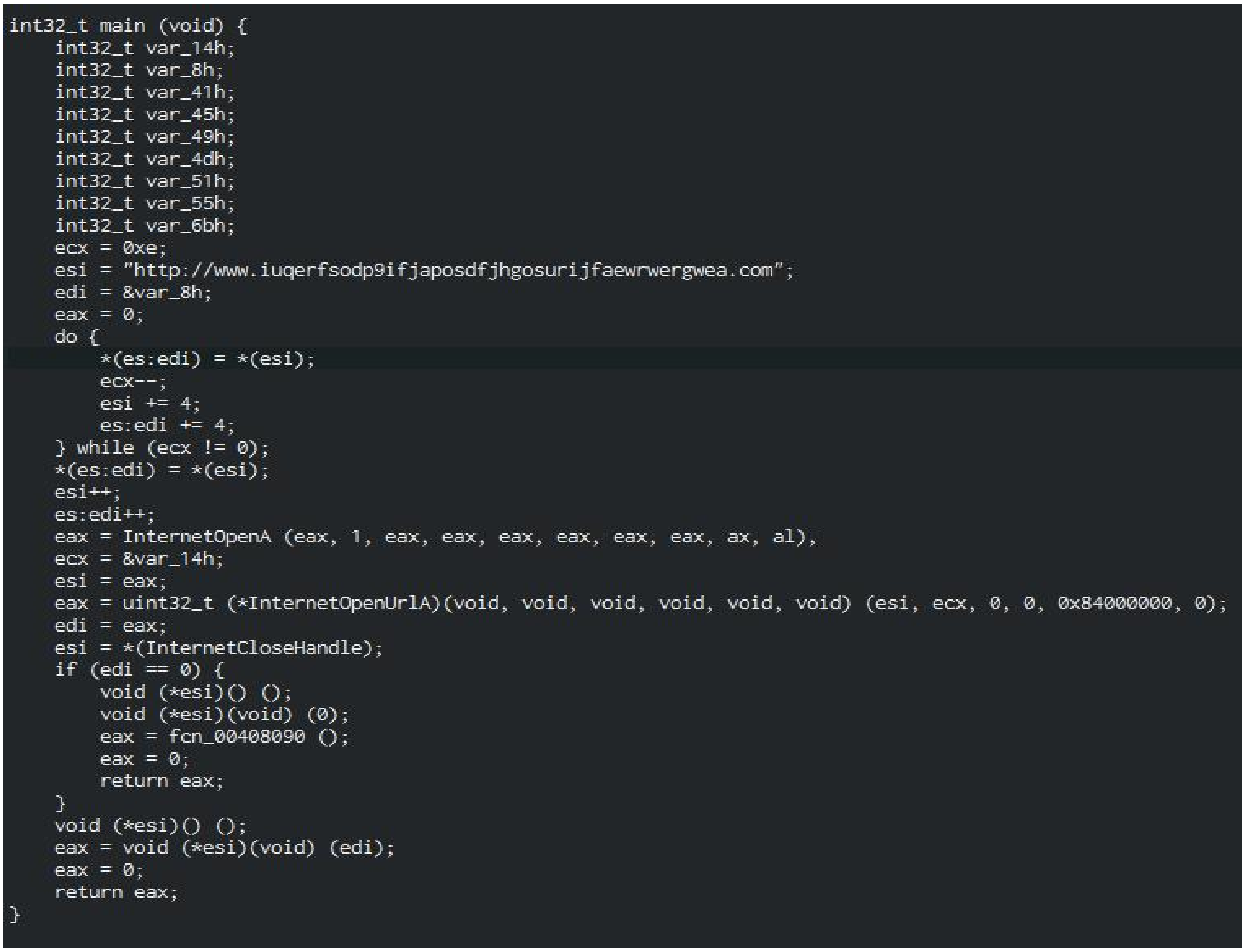
If we summarize our Advanced Static analysis then the malware is basically looking to the hardcoded URL using the InternetOpenIUrlA and InternetCloseHandle Windows API libraries - (Cutter)



```
[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
```

If the URL is reached then the execution stops otherwise the malware continues executing by encrypting system files and checking Remote PCs for exploitable SMB Shares, like we previously discussed in the Basic Dynamic Analysis Portion - (Cutter)



```
int32_t main (void) {
    int32_t var_14h;
    int32_t var_8h;
    int32_t var_41h;
    int32_t var_45h;
    int32_t var_49h;
    int32_t var_4dh;
    int32_t var_51h;
    int32_t var_55h;
    int32_t var_6bh;
    ecx = 0xe;
    esi = "http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com";
    edi = &var_8h;
    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_14h;
    esi = eax;
    eax = uint32_t (*InternetOpenUrlA)(void, void, void, void, void, void) (esi, ecx, 0, 0, 0x84000000, 0);
    edi = eax;
    esi = *(InternetCloseHandle);
    if (edi == 0) {
        void (*esi)() ();
        void (*esi)(void) (0);
        eax = fcn_00408090 ();
        eax = 0;
        return eax;
    }
    void (*esi)() ();
    eax = void (*esi)(void) (edi);
    eax = 0;
    return eax;
}
```

The Decompiled source code of the binary also leads to the same conclusion

Rules & Signatures

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

{Information on specific signatures, i.e. strings, URLs, etc}

Appendices

A. Yara Rules

```
rule WannaCryRansomware {
meta:
last_updated = ‘2022-10-25‘
author = ‘Mubeen Gulzar‘
description = ‘Yara rule for WannaCry Ransomware Malware‘

strings:
// Fill out identifying strings and other criteria
   strings1 = ‘iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea‘ fullword ascii
   strings2 = ‘icacls . /grant Everyone:F /T /C /Q‘ fullword ascii
   strings3 = ‘tasksche.exe‘ fullword ascii
   PE_magic_byte = ‘MZ‘
condition:
// Fill out the conditions that must be met to identify the binary
   PE_magic_byte at 0 and
(   strings1 and    strings2 ) or
(   strings1 and    strings3 )
}
```

B. Callback URLs

Domain	Port
hxxp://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com	**80**