MALWARE ANALYSIS REPORT

WannaCry Ransomware

MARCH 2022 | V2.0

Prepared by

Dipankar Lama (Zuk0)

Table of Contents

Executive Summary

28th February 2022

Wannacry is a ransomware cryptoworm which was used for WannaCry ransomware attack in the year 2017. To propogate this ransomware a well known vulnerability knows as EternalBlue was exploited which was developed by National Security Agency (NSA).

Wannacry ransomware is a x32 bit program written in C++ for Windows Operating system.

The attack consists of 3 stages.

1. Drops a 2nd executable by replacing tasksche.exe in the C:\Windows Directory
2. The 2nd executable drops the resources like encryption DLL and EXE file, cryptographic keys, bitcoin address etc..
3. Creates multiple thread to carry out encryption of files in the victim machine.

The Symptoms of infections include

1. Changing of Desktop image to black background with red text.
2. Encrypted File with WNCRY extension
3. Service with service name mssecsvc.exe and display name MIcrosoft Security Center (2.0) Service
4. Presence of Registry Key HKLM\SOFTWARE\Wow6432Node\WannaCrypt Or

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

High Level Technical Summary

28th February 2022

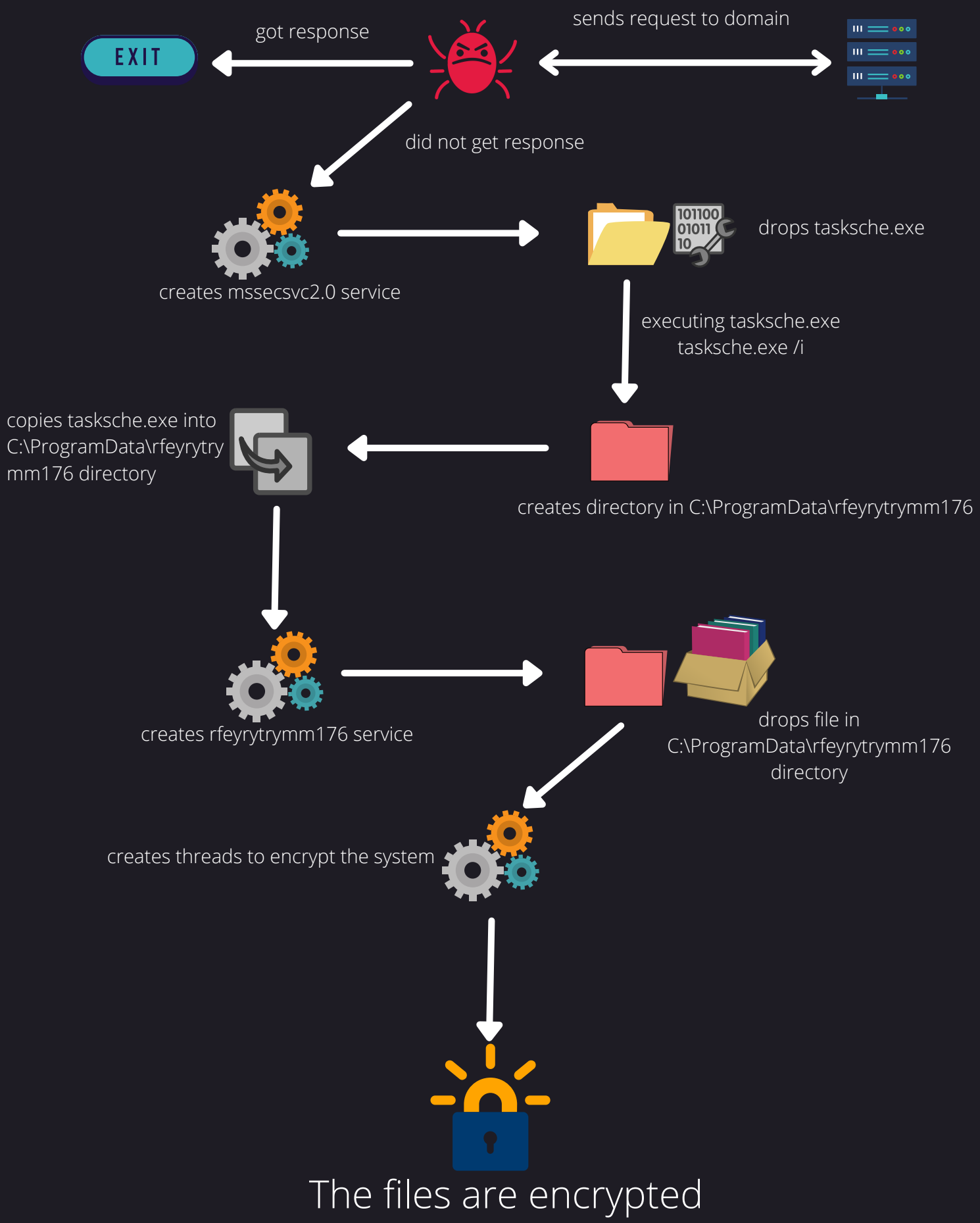
Wannacry ransomware works on 3 phases

In the 1st phase it tries to reach out to www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com domain which is a kill switch. If the domain respond to the request then wannacry immediately exits and does not execute. If the domain is not active then wannacry will begin the attack by creating a windows service with service name mssecsvc2.0, display name Microsoft Security Center (2.0) Service and binary path "<PATH_TO_WANNACRY>\wannacry.exe -m security". The service will constantly try to reach out to a range of IPv4 addresses.

After creating windows service it checks if tasksche.exe exists or not in C:\Windows directory. If the binary exists then it renames it to qeriuwjhrf.exe and them drops an executable in the C:\Windows directory with name tasksche.exe from it's resource section.

In the 2nd Phase it creates a new process with command line argument "C:\Windows\tasksche.exe /i". /i tells the process to begin the initialisation process. In this initialisation it creates a directory in "C:\ProgramData\rfeyrytrymm176". After creating the directory it will move copy itself to this newly created directory and then creates a service with binary path "C:\ProgramData\rfeyrytrymm176\tasksche.exe". The created service will then proceed with dropping encrypting EXE, DLL, cryptokeys, images, bitcoin address in the "C:\ProgramData\rfeyrytrymm176\" directory.

In the 3rd Phase it creates multiple threads which will process with encrypting all the important files in the local system, changing desktop background, copying instructions to desktop and many more.


EXIT
got response
sends request to domain
did not get response
creates mssecsvc2.0 service
drops tasksche.exe
executing tasksche.exe
tasksche.exe /i
copies tasksche.exe into
C:\ProgramData\rfeyrytry
mm176 directory
creates directory in C:\ProgramData\rfeyrytrymm176
creates rfeyrytrymm176 service
drops file in
C:\ProgramData\rfeyrytrymm176
directory
creates threads to encrypt the system
The files are encrypted

Malware Composition

28 February 2022

Wannacry consists of following components

FileName	SHA-1 Hash
wannacry.exe	E889544AFF85FFAF8B0D0DA705105DEE7C97FE26
tasksche.exe	5FF465AFAABCBF0150D1A3AB2C2E74F3A4426467
tasksche_res.zip	30F8820CF93A627C66195F0D77D6A409024C6E52
taskdll.exe	47A9AD4125B6BD7C55E4E7DA251E23F089407B8F
taskse.exe	BE5D6279874DA315E3080B06083757AAD9B32C23

wannacry.exe

The initial executable that runs in the beginning

tasksche.exe

This executable is dropped by wannacry.exe file after execution. It is responsible for creating a directory in the C:\ProgramData directory and copies itself into it in order to drop more files.

tasksche_res.zip

Resides in the resource section of tasksche.exe file which contains executable and files for encryption

taskdll.exe and taskse.exe

These executable are responsible for encrypting files in the local system.

Static Analysis

28th February 2022

Basic information about the executable using CF Explorer

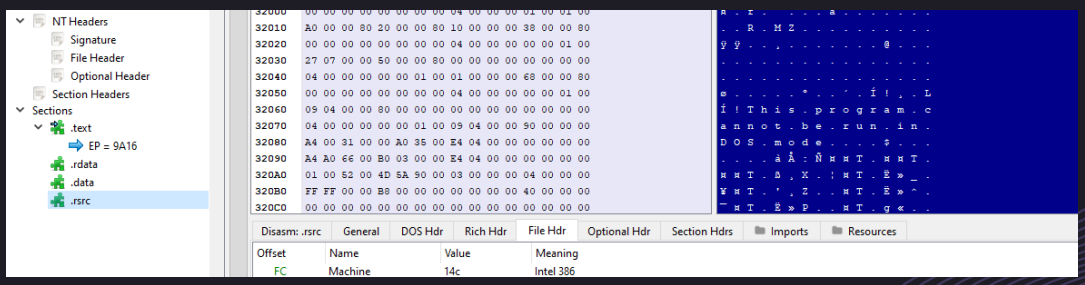
Property	Value
File Name	C:\Users\Analyst\Desktop\wannacry.exe
File Type	Portable Executable 32
File Info	Microsoft Visual C++ 6.0
File Size	3.55 MB (3723264 bytes)
PE Size	3.55 MB (3723264 bytes)
Created	Thursday 24 February 2022, 11.13.31
Modified	Tuesday 19 March 2019, 11.32.14
Accessed	Monday 28 February 2022, 10.53.58
MD5	DB349B97C37D22F5EA1D1841E3C89EB4
SHA-1	E889544AFF85FFAF8B0D0DA705105DEE7C97FE26

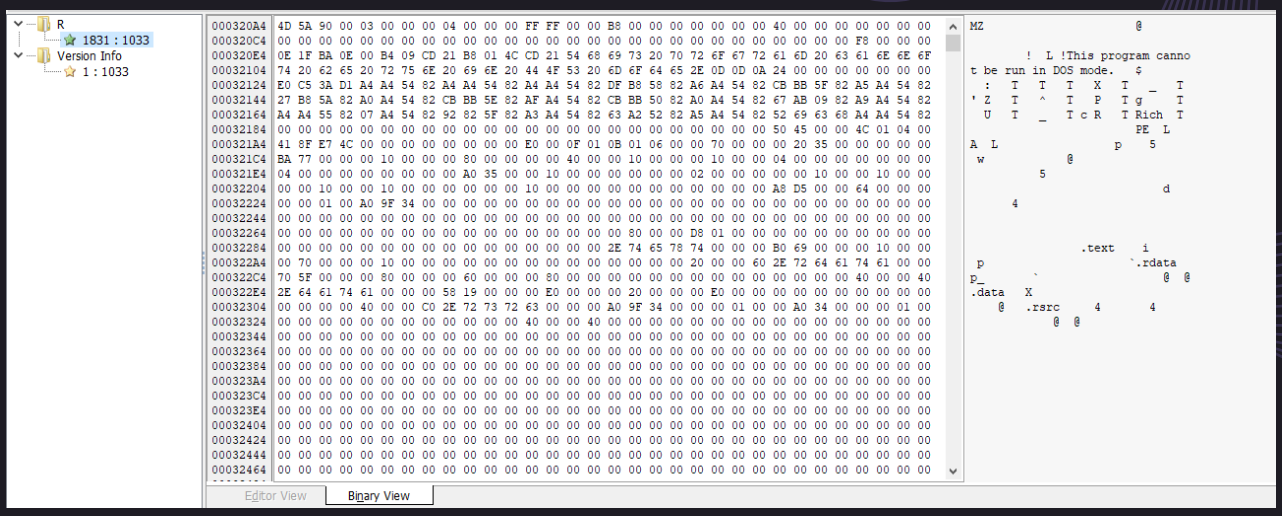
Property	Value
CompanyName	Microsoft Corporation
FileDescription	Microsoft® Disk Defragmenter
FileVersion	6.1.7601.17514 (win7sp1_rtm.101119-1850)
InternalName	lhdfrgui.exe
LegalCopyright	© Microsoft Corporation. All rights reserved.
OriginalFilename	lhdfrgui.exe
ProductName	Microsoft® Windows® Operating System

The Time Date Stamp was found using PEstudio tool.

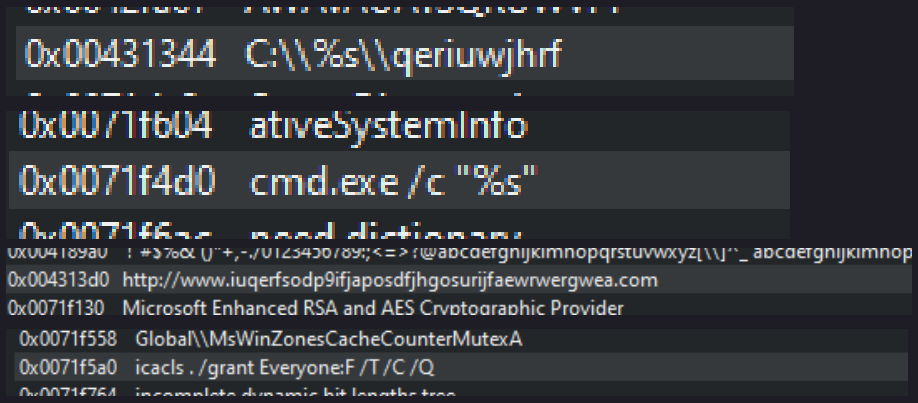
100	Time Date Stamp	4ce78ecc	Saturday, 20.11.2010 09:03:08 UTC

Examining sections of wannacry.exe I found out the .rsrc section contains an executable file





Using Cutter we found some intresting strings inside the binary



Some interesting Import functions

Call via	Name	Ordinal	Original Thunk	Thunk	Forwarder	Hint
A134	InternetOpenA	-	A7DC	A7DC	-	92
A138	InternetOpenUrlA	-	A7C8	A7C8	-	93
A13C	InternetCloseHandle	-	A7B2	A7B2	-	69

Call via	Name	Ordinal	Original Thunk	Thunk	Forwarder	Hint
A054	TerminateThread	-	A4E4	A4E4	-	35F
A058	LoadResource	-	A5A6	A5A6	-	257
A05C	FindResourceA	-	A5B6	A5B6	-	E3
A060	GetProcAddress	-	A5C6	A5C6	-	1A0
A064	GetModuleHandleW	-	A5D8	A5D8	-	182
A068	ExitProcess	-	A5EC	A5EC	-	B9
A06C	GetModuleFileNameA	-	A5FA	A5FA	-	17D

Call via	Name	Ordinal	Original Thunk	Thunk	Forwarder	Hint
A000	StartServiceCtrlDispatcherA	-	A6F6	A6F6	-	24A
A004	RegisterServiceCtrlHandlerA	-	A6D8	A6D8	-	20C
A008	ChangeServiceConfig2A	-	A6C0	A6C0	-	34
A00C	SetServiceStatus	-	A6AC	A6AC	-	244
A010	OpenSCManagerA	-	A69A	A69A	-	1AD
A014	CreateServiceA	-	A688	A688	-	64
A018	CloseServiceHandle	-	A672	A672	-	3E

Dynamic Analysis

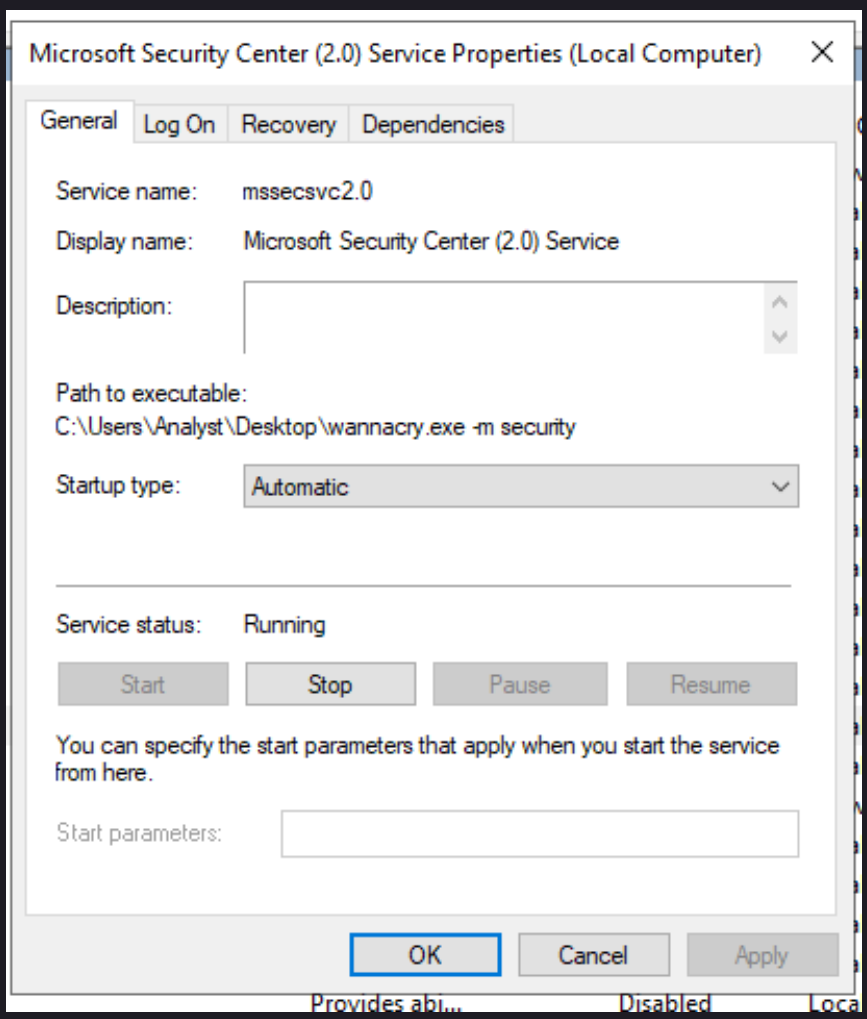
28th February 2022

When executed the wannacry.exe tries to make a DNS request

1	0.000000	192.168.56.3	192.168.56.4	DNS	109 Standard query 0xb472 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
2	0.000275	192.168.56.4	192.168.56.3	ICMP	137 Destination unreachable (Port unreachable)
3	0.000360	192.168.56.3	192.168.56.4	DNS	109 Standard query 0xb472 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
4	0.000563	192.168.56.4	192.168.56.3	ICMP	137 Destination unreachable (Port unreachable)
5	0.000625	192.168.56.3	192.168.56.4	DNS	109 Standard query 0xb472 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
6	0.000760	192.168.56.4	192.168.56.3	ICMP	137 Destination unreachable (Port unreachable)
7	0.000810	192.168.56.3	192.168.56.4	DNS	109 Standard query 0xb472 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
8	0.001062	192.168.56.4	192.168.56.3	ICMP	137 Destination unreachable (Port unreachable)
9	0.001114	192.168.56.3	192.168.56.4	DNS	109 Standard query 0xb472 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
10	0.001244	192.168.56.4	192.168.56.3	ICMP	137 Destination unreachable (Port unreachable)

After not getting any response it carries on to create a service.

Microsoft Security Center (2.0) Service	Running	Automatic	Local Syste...



The newly created service will try to connect to range of IPv4 addresses

1:53:...	wannacry.exe	2872	Thread Exit	
1:53:...	wannacry.exe	2872	TCP Reconnect	DESKTOP-98I24CQ:58632 -> 169.254.126.7:microsoft-ds
1:53:...	wannacry.exe	2872	TCP Reconnect	DESKTOP-98I24CQ:58633 -> 169.254.127.7:microsoft-ds
1:53:...	wannacry.exe	2872	TCP Disconnect	DESKTOP-98I24CQ:58632 -> 169.254.126.7:microsoft-ds
1:53:...	wannacry.exe	2872	Thread Exit	
1:53:...	wannacry.exe	2872	TCP Disconnect	DESKTOP-98I24CQ:58633 -> 169.254.127.7:microsoft-ds
1:53:...	wannacry.exe	2872	Thread Exit	
1:53:...	wannacry.exe	2872	TCP Reconnect	DESKTOP-98I24CQ:58634 -> 169.254.128.7:microsoft-ds
1:53:...	wannacry.exe	2872	TCP Disconnect	DESKTOP-98I24CQ:58634 -> 169.254.128.7:microsoft-ds
1:53:...	wannacry.exe	2872	Thread Exit	
1:53:...	wannacry.exe	2872	TCP Disconnect	DESKTOP-98I24CQ:58705 -> 169.254.129.7:microsoft-ds
1:53:...	wannacry.exe	2872	Thread Exit	
1:53:...	wannacry.exe	2872	TCP Reconnect	DESKTOP-98I24CQ:58706 -> 169.254.130.7:microsoft-ds
1:53:...	wannacry.exe	2872	TCP Disconnect	DESKTOP-98I24CQ:58706 -> 169.254.130.7:microsoft-ds
1:53:...	wannacry.exe	2872	Thread Exit	
1:53:...	wannacry.exe	2872	TCP Reconnect	DESKTOP-98I24CQ:58707 -> 169.254.131.7:microsoft-ds
1:53:...	wannacry.exe	2872	TCP Disconnect	DESKTOP-98I24CQ:58707 -> 169.254.131.7:microsoft-ds
1:53:...	wannacry.exe	2872	Thread Exit	
1:53:...	wannacry.exe	2872	TCP Reconnect	DESKTOP-98I24CQ:58728 -> 169.254.132.7:microsoft-ds
1:53:...	wannacry.exe	2872	TCP Disconnect	DESKTOP-98I24CQ:58728 -> 169.254.132.7:microsoft-ds
1:53:...	wannacry.exe	2872	Thread Exit	
1:53:...	wannacry.exe	2872	Thread Create	
1:53:...	wannacry.exe	2872	Thread Create	
1:53:...	wannacry.exe	2872	TCP Disconnect	DESKTOP-98I24CQ:58819 -> 169.254.133.7:microsoft-ds

after creating service it will go on and replace the original tasksche.exe binary with it's own malicious executable

12:26:...	wannacry.exe	3348	CreateFile	C:\Windows\tasksche.exe
12:34:...	wannacry.exe	3348	CreateFile	C:\Windows\tasksche.exe
12:34:...	wannacry.exe	3348	CreateFile	C:\Windows\tasksche.exe
12:34:...	wannacry.exe	3348	QueryBasicInfor...	C:\Windows\tasksche.exe
12:34:...	wannacry.exe	3348	CloseFile	C:\Windows\tasksche.exe
12:34:...	wannacry.exe	3348	QueryNameInfo...	C:\Windows\tasksche.exe
12:34:...	wannacry.exe	3348	QueryNameInfo...	C:\Windows\tasksche.exe
12:34:...	wannacry.exe	3348	QueryNormalize...	C:\Windows\tasksche.exe

tasksche.exe	2/25/2022 10:25 AM	Application	3,432 KB

and then create a new process with newly dropped executable

```
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                                   edx:"C:\\WINDOWS\\tasksche.exe /i"
push ebx
mov dword ptr ss:[esp+4C],44               44:'D'
mov word ptr ss:[esp+7C],bx
mov dword ptr ss:[esp+78],81
call dword ptr ds:[<&CreateProcessA>]
test eax,eax
je wannacry.407F08
mov eax,dword ptr ss:[esp+18]
push eax
```

The newly created process will first generate a random string by getting the hostname of the local machine and then multiplying their ascii value to get seed for random function

```
0x0040125e  push    eax         ; LPWSTR lpBuffer
0x0040125f  call    dword [GetComputerNameW] ; 0x4080d0 ; Gets the hostname of the local machine
0x00401265  mov     esi, dword [wcslen] ; 0x408138
0x0040126b  and     dword [var_4h], 0
0x0040126f  push    1           ; 1
0x00401271  lea     eax, [lpBuffer]
0x00401277  pop     ebx
0x00401278  push    eax
0x00401279  call    esi         ; wcslen (Returns the length of the wide string)
0x0040127b  test    eax, eax
0x0040127d  pop     ecx
0x0040127e  jbe     0x4012a0
0x00401280  lea     edi, [lpBuffer]
0x00401286  movzx   eax, word [edi]
0x00401289  imul    ebx, eax    ; gets the hostname and multiplies the ascii value of all the character to get a seed for srand generator
0x0040128c  inc     dword [var_4h]
0x0040128f  lea     eax, [lpBuffer]
0x00401295  inc     edi
0x00401296  push    eax
0x00401297  inc     edi
0x00401298  call    esi
0x0040129a  cmp     dword [var_4h], eax
0x0040129d  pop     ecx
0x0040129e  jb      0x401286
0x004012a0  push    ebx         ; int seed
0x004012a1  call    dword [srand] ; 0x408124 ; generates random value ; void srand(int seed)
0x004012a7  mov     ebx, dword [rand] ; 0x408120
```

```
0x004012be  jle     0x4012d6
0x004012c0  call    ebx
0x004012c2  push    0x1a        ; 26
0x004012c4  cdq
0x004012c5  pop     ecx
0x004012c6  idiv    ecx
0x004012c8  mov     eax, dword [arg_8h]
0x004012cb  add     dl, 0x61    ; 97
0x004012ce  mov     byte [edi + eax], dl
0x004012d1  inc     edi
0x004012d2  cmp     edi, esi
0x004012d4  jl      0x4012c0
0x004012d6  add     esi, 3      ; Generates a string "rfeyrytrymm176"
0x004012d9  cmp     edi, esi
0x004012db  jge     0x4012f1
```

the random function will generate the string and then will create a new directory with that name inside C:\ProgramData directory. It will also create a registry key as below

```
0x00401b02    push    0
0x00401b04    push    dword [format] ; C:\ProgramData
0x00401b07    call    esi            ; CreateDirectoryW
0x00401b09    push    dword [format]
0x00401b0c    mov     edi, dword [SetCurrentDirectoryW] ; 0x408058 ; C:\ProgramData
0x00401b12    call    edi            ; SetCurrentDirectoryW
0x00401b14    test    eax, eax
0x00401b16    je      0x401b27
0x00401b18    mov     ebx, dword [arg_ch]
0x00401b1b    push    0
0x00401b1d    push    ebx            ; Randomly generated string "rfeyrytrymm176"
0x00401b1e    call    esi            ; CreateDirectoryW
0x00401b20    push    ebx
0x00401b21    call    edi
0x00401b23    test    eax, eax
0x00401b25    jne     0x401b2b
0x00401b27    xor     eax, eax
```

rfeyrytrymm176	2/27/2022 1:25 AM	File folder
shimgen	11/14/2021 8:28 PM	File folder

Registry Editor

File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\WanaCrypt0r

- Policies
- Python
- RegisteredApplications
- Vim
- Windows
- WOW6432Node
  - AccessData

Name	Type	Data
(Default)	REG_SZ	(value not set)
wd	REG_SZ	C:\ProgramData\rfeyrytrymm176

and copy itself to this new directory.

This PC › Local Disk (C:) › ProgramData › rfeyrytrymm176

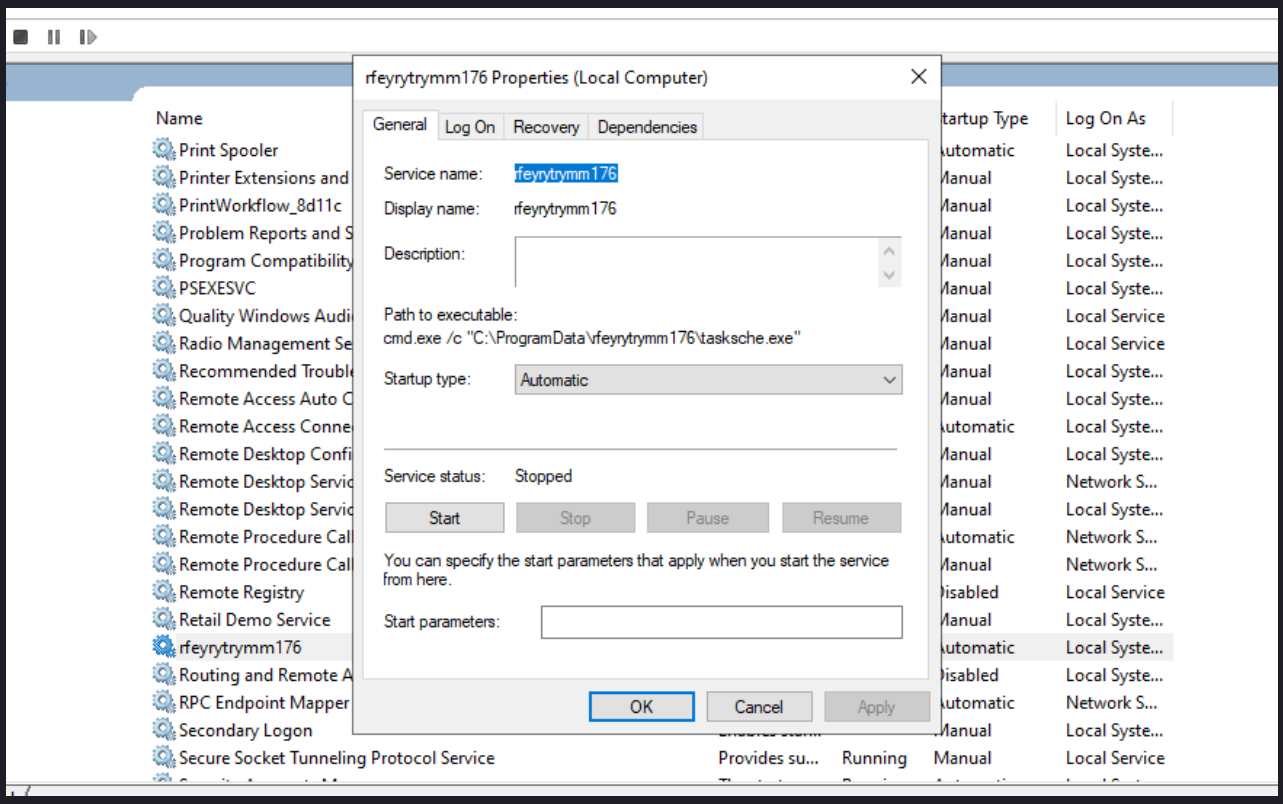
Name	Date modified	Type	Size
tasksche.exe	2/27/2022 12:42 AM	Application	3,432 KB

After copying itself it will create a new service

```
lea eax,dword ptr ss:[ebp-40C]
push edi
push edi
push edi
push edi
push edi
push eax                                   eax:"cmd.exe /c \"C:\\ProgramData\\rfeyrytrymm176\\t
push 1
push 2
push 10
push ebx
push esi                                   esi:"rfeyrytrymm176"
push esi                                   esi:"rfeyrytrymm176"
push dword ptr ss:[ebp-4]
call dword ptr ds:[<&CreateServiceA>]
mov esi,eax                                esi:"rfeyrytrymm176", eax:"cmd.exe /c \"C:\\ProgramD
cmp esi,edi                                esi:"rfeyrytrymm176"
```

with following binary path

```
eax:"cmd.exe /c \"C:\\ProgramData\\rfeyrytrymm176\\tasksche.exe\""
```



Now the activated service will drop new files from the resource section. The resource section contains a zip file which contains the dropped file. Some files like 00000000.eky, 00000000.pky contains cryptographic keys which will be used for the encryption. The password for zip file is "WNcry@2ol7"

Name	Date modified	Type	Size
msg	2/28/2022 11:57 AM	File folder	
@Please_Read_Me@.txt	2/28/2022 11:57 AM	Text Document	1 KB
@WanaDecryptor@.exe	5/12/2017 3:22 AM	Application	240 KB
00000000.eky	2/28/2022 11:57 AM	EKY File	0 KB
00000000.pky	2/28/2022 11:57 AM	PKY File	1 KB
00000000.res	2/28/2022 11:57 AM	Compiled Resourc...	1 KB
269231646078247.bat	2/28/2022 11:57 AM	Windows Batch File	1 KB
b.wnry	5/11/2017 9:13 PM	WNRY File	1,407 KB
c.wnry	2/28/2022 11:57 AM	WNRY File	1 KB
r.wnry	5/11/2017 4:59 PM	WNRY File	1 KB
s.wnry	5/9/2017 5:58 PM	WNRY File	2,968 KB
t.wnry	5/12/2017 3:22 AM	WNRY File	65 KB
taskdl.exe	5/12/2017 3:22 AM	Application	20 KB
tasksche.exe	2/28/2022 11:57 AM	Application	3,432 KB
taskse.exe	5/12/2017 3:22 AM	Application	20 KB
u.wnry	5/12/2017 3:22 AM	WNRY File	240 KB

After extracting all the resource it will begin the encryption process by finding all the important files in the victim machine and encrypt them.

Below are some import functions from taskdll.exe which will be use to find files in the victim machine

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
00002204	00002204	01D6	GetTempPathW
00002214	00002214	01F4	GetWindowsDirectoryW
0000222C	0000222C	0084	DeleteFileW
0000223A	0000223A	00CE	FindClose
00002246	00002246	00DD	FindNextFileW
00002256	00002256	00D5	FindFirstFileW
00002268	00002268	0356	Sleep
00002270	00002270	0154	GetDriveTypeW
00002280	00002280	0178	GetLogicalDrives
00002654	00002654	017F	GetModuleHandleA
00002668	00002668	01B7	GetStartupInfoA

in the end after all the encryption process is done the victim desktop will look like below image.

Indicators of Compromise

1st March 2022

Network Indicators

1. Making request to www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com

```
▸ Frame 5: 109 bytes on wire (872 bits), 109 bytes captured (872 bits) on interface enp0s3, id 0
▸ Ethernet II, Src: PcsCompu_09:ea:4b (08:00:27:09:ea:4b), Dst: PcsCompu_b8:16:a4 (08:00:27:b8:16:a4)
▸ Internet Protocol Version 4, Src: 192.168.56.3, Dst: 192.168.56.4
▸ User Datagram Protocol, Src Port: 59998, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0x5717
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▸ www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com: type A, class IN
```

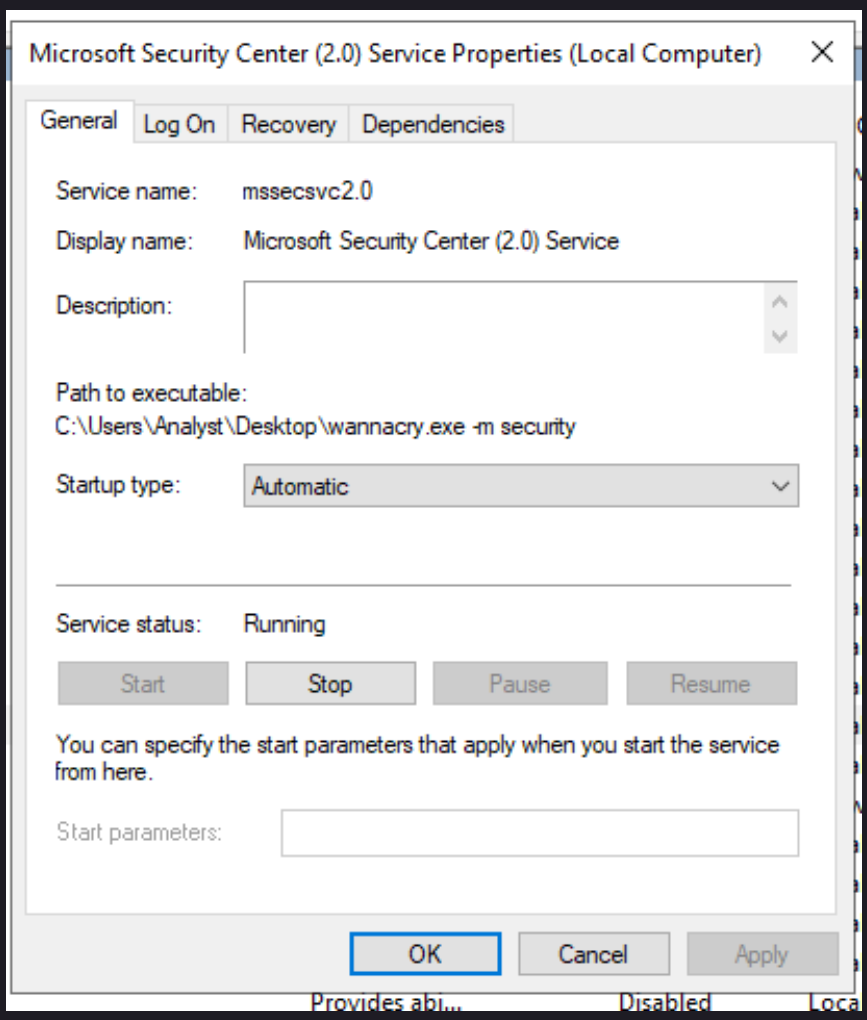
```
▸ Frame 10: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) on interface enp0s3, id 0
▸ Ethernet II, Src: PcsCompu_09:ea:4b (08:00:27:09:ea:4b), Dst: PcsCompu_b8:16:a4 (08:00:27:b8:16:a4)
▸ Internet Protocol Version 4, Src: 192.168.56.3, Dst: 192.168.56.4
▸ Transmission Control Protocol, Src Port: 49678, Dst Port: 80, Seq: 1, Ack: 1, Len: 100
▾ Hypertext Transfer Protocol
  ▸ GET / HTTP/1.1\r\n
    Host: www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com\r\n
    Cache-Control: no-cache\r\n
    \r\n
    [Full request URI: http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com/]
    [HTTP request 1/1]
    [Response in frame: 14]
```

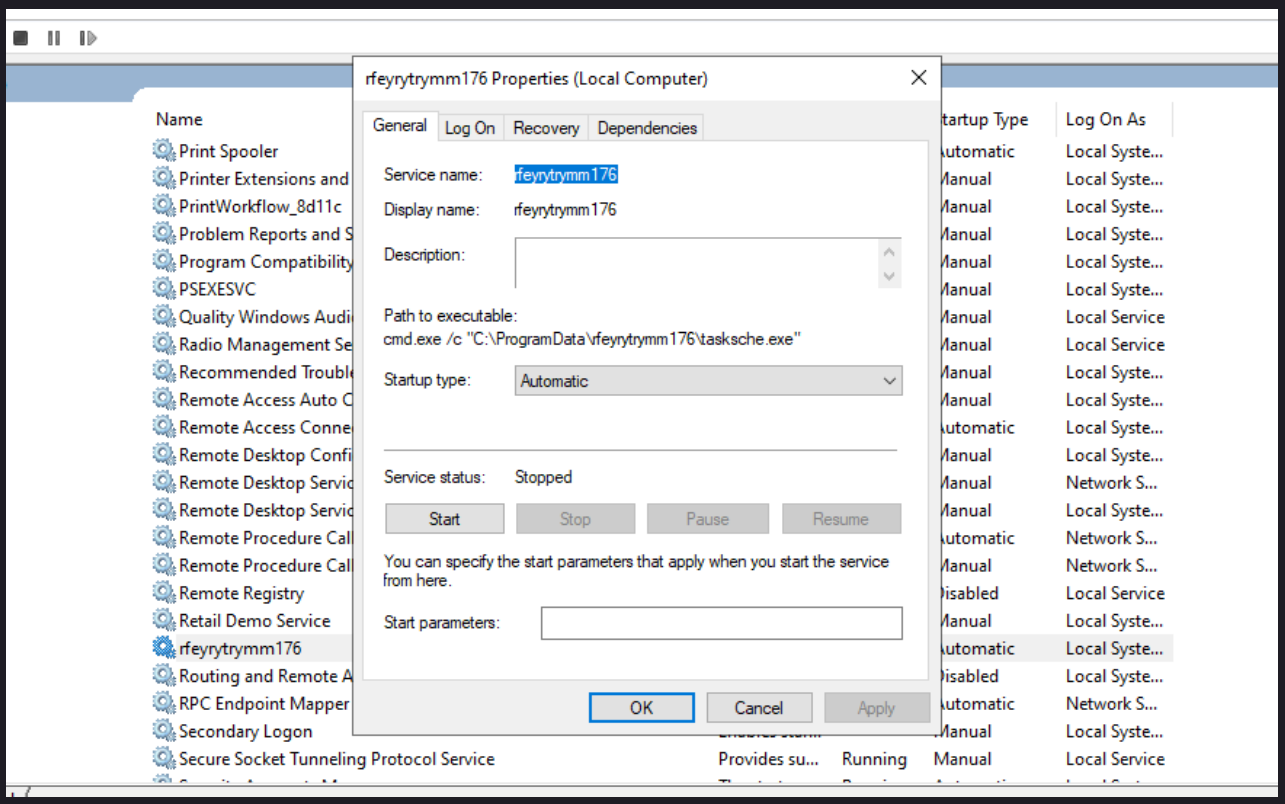
Host Indicators

- Presence of following files "qeriuwjhrf" and "tasksche.exe".

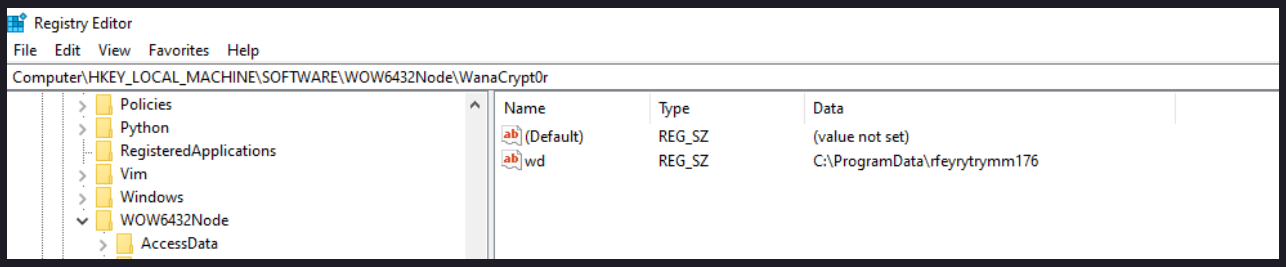
Name	Date modified	Type	Size
msscript.ocx	4/14/2008 5:40 AM	ActiveX control	108 KB
notepad.exe	3/18/2019 9:45 PM	Application	177 KB
PFRO.log	2/20/2022 3:23 PM	Text Document	8 KB
Professional.xml	3/18/2019 9:46 PM	XML Document	35 KB
ProfessionalEducation.xml	3/18/2019 9:46 PM	XML Document	35 KB
ProfessionalWorkstation.xml	3/18/2019 9:46 PM	XML Document	35 KB
PSEXESVC.exe	1/23/2022 11:29 PM	Application	375 KB
py.exe	8/17/2020 7:02 PM	Application	884 KB
pyshellext.amd64.dll	8/17/2020 7:04 PM	Application exten...	57 KB
pyw.exe	8/17/2020 7:02 PM	Application	885 KB
qeriuwjhrf	3/18/2019 9:45 PM	File	177 KB
regedit.exe	3/18/2019 9:45 PM	Application	350 KB
richtx32.ocx	3/12/2001 4:07 PM	ActiveX control	254 KB
splwow64.exe	10/6/2019 7:56 PM	Application	129 KB
system.ini	3/18/2019 9:49 PM	Configuration sett...	1 KB
tasksche.exe	3/1/2022 11:01 AM	Application	3,432 KB
twain_32.dll	3/18/2019 9:46 PM	Application exten...	63 KB
win.ini	3/18/2019 9:49 PM	Configuration sett...	1 KB
WindowsShell.Manifest	3/18/2019 9:44 PM	MANIFEST File	1 KB
WindowsUpdate.log	3/1/2022 11:00 AM	Text Document	1 KB
winhlp32.exe	3/18/2019 9:46 PM	Application	12 KB
WMSysPr9.prx	3/18/2019 11:23 PM	PRX File	310 KB
write.exe	3/18/2019 9:45 PM	Application	11 KB

- Presence of following services

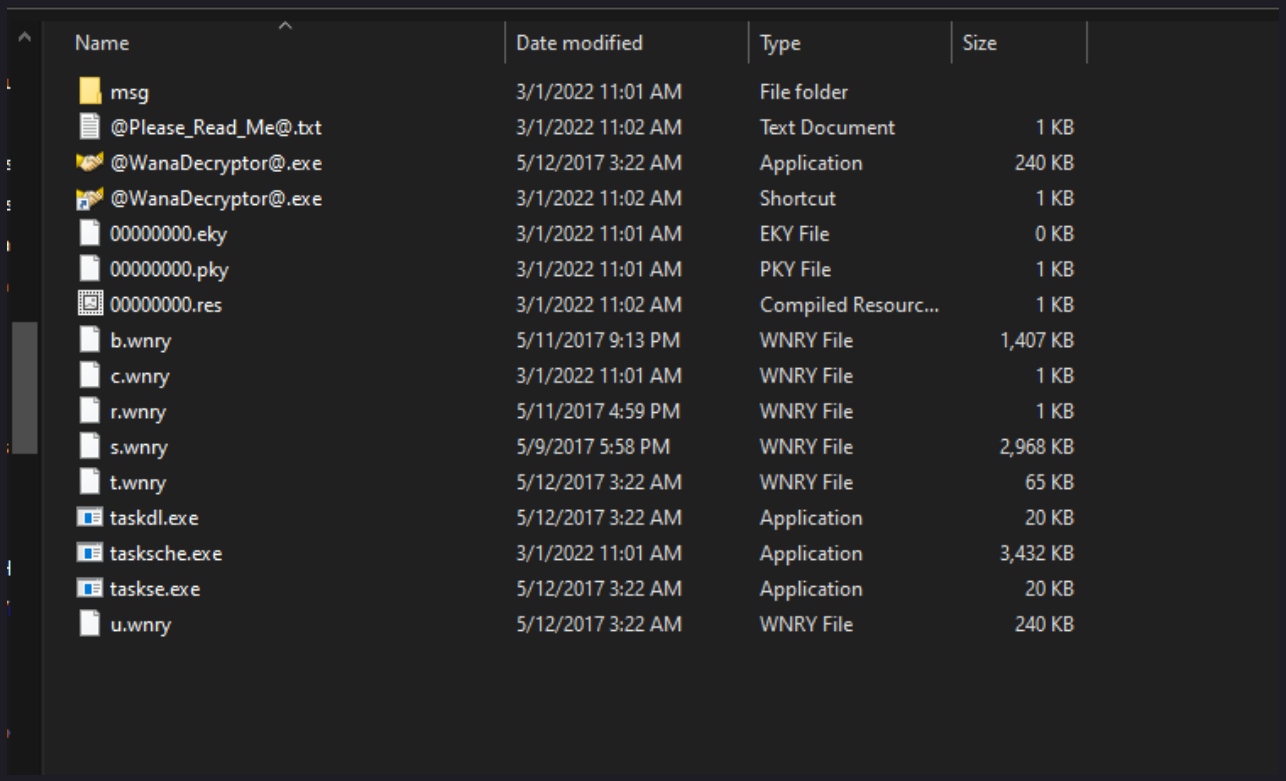




- Presence of following Registry Key



- Presence of following files the directory saved in the registry key shown above



Name	Date modified	Type	Size
msg	3/1/2022 11:01 AM	File folder	
@Please_Read_Me@.txt	3/1/2022 11:02 AM	Text Document	1 KB
@WanaDecryptor@.exe	5/12/2017 3:22 AM	Application	240 KB
@WanaDecryptor@.exe	3/1/2022 11:02 AM	Shortcut	1 KB
00000000.eky	3/1/2022 11:01 AM	EKY File	0 KB
00000000.pky	3/1/2022 11:01 AM	PKY File	1 KB
00000000.res	3/1/2022 11:02 AM	Compiled Resourc...	1 KB
b.wnry	5/11/2017 9:13 PM	WNRY File	1,407 KB
c.wnry	3/1/2022 11:01 AM	WNRY File	1 KB
r.wnry	5/11/2017 4:59 PM	WNRY File	1 KB
s.wnry	5/9/2017 5:58 PM	WNRY File	2,968 KB
t.wnry	5/12/2017 3:22 AM	WNRY File	65 KB
taskdl.exe	5/12/2017 3:22 AM	Application	20 KB
tasksche.exe	3/1/2022 11:01 AM	Application	3,432 KB
taskse.exe	5/12/2017 3:22 AM	Application	20 KB
u.wnry	5/12/2017 3:22 AM	WNRY File	240 KB

Yara Rule and Signature

1st March 2022

Full Yara rules can be found in the following github link
https://github.com/0xZuk0/rules-of-yaras/blob/main/wannacry.yara

```
import "hash"
import "pe"

rule WannaCry
{
    meta :
        last_updated = "01-03-2022"
        author = "Zuk0"
        description = "Yara rule to detect wannacry ransomware"

    strings :
        $killswitch_domain = "www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com" ascii
        $string1 = "C:\\%s\\qeriuwjhrf" ascii
        $reg_name = "WanaCrypt0r" wide
        $password = "WNcry@2ol7" ascii
        $exe1 = "taskdl.exe" ascii
        $exe2 = "taskse.exe" ascii
        $service_name = "Microsoft Security Center (2.0) Service" ascii

    condition :
        pe.is_pe and
        hash.sha256(0, filesize) == "24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c" and
        hash.sha256(204964, 3514368) == "ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa" and
        $killswitch_domain and
        $string1 and
        $reg_name and
        $password and
        $exe1 and
        $exe2 and
```