Practical Malware Analysis & Triage
Malware Analysis Report

WannaCry Ransomware Malware

Oct 2022 | Vishal Pathak | v1.0

Table of Contents

Executive Summary

SHA256 hash	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c

WannaCry was the malware global epidemic that took place in May 2017. It sperad by combining a Windows vulnerability recently leaked from the National Security Agency's cyber arsenal and some simple programming to hunt down servers that interact with public networks, WannaCry spread itself further than any malware campaign has in the last 15 years. Once it ran in your system, it would encrypt all your files in the systema and would ask for ransom in form of cryptocurrency to decrypt all the files.

It is written in C++ programming language. When it executes it starts by checking for a url which if the malware is able to reach/access it then it doesn't executes and deletes itself from the system. But if the malware is not able to access it then it starts its execution and creates its payload at "C:/Windows/taskche.exe and it starts encrypting the files within your system and those encrypted file would have the .WNCRY extension to it. WannaCry also tries to speard to other Windows with the help of Eternal Blue Vulnerabilty.

Yara rule are attached in Rules & SIgnatures. Malware sample and hash are given for further examination on VirusTotal.

High-Level Technical Summary

WannaCry consists of two parts: stage 0 executable and an unpacked stage 2 encryption and worm program. It first attempts to contact its kill switch url (hxxp://iuqerfsodp9ifjaposdfjhgosurijfaewerwergwea.local). If the url is contacted it does not executes. But if the url is not contacted or not alive then it unpacks its second payload taskche.exe and creates a service to start the taskche.exe on startup. This executable enrypts all the files, shows popup ransom window and change the background of the Desktop. It creates a random folder inside C:/ProgramData to store all the wanna cry files. It exploits the EternalBlue Vulnerability on port 445 to spread to other computers.

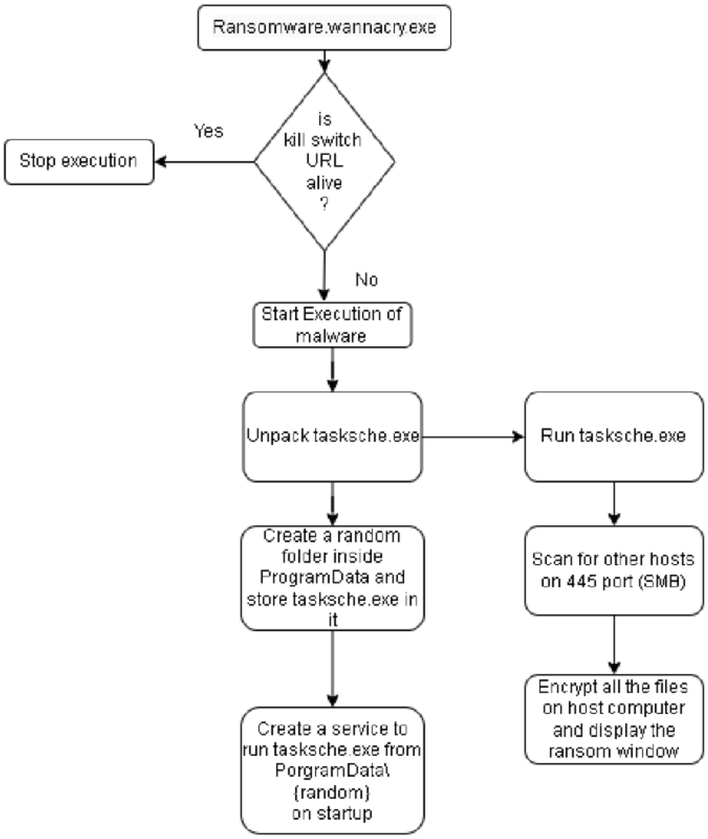

Ransomware.wannacry.exe
is kill switch URL alive ?
Yes
Stop execution
No
Start Execution of malware
Unpack tasksche.exe
Run tasksche.exe
Create a random folder inside ProgramData and store tasksche.exe in it
Scan for other hosts on 445 port (SMB)
Create a service to run tasksche.exe from PorgramData\{random} on startup
Encrypt all the files on host computer and display the ransom window

Fig- 1 – Flow of Malware

Malware Composition

DemoWare consists of the following components:

File Name	SHA256 Hash
Wannacry.exe	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
Taskche.exe	ED01EBFBC9EB5BBEA545AF4D01BF5F1071661840480439C6E5BABE8E080E41AA

Wannacry.exe

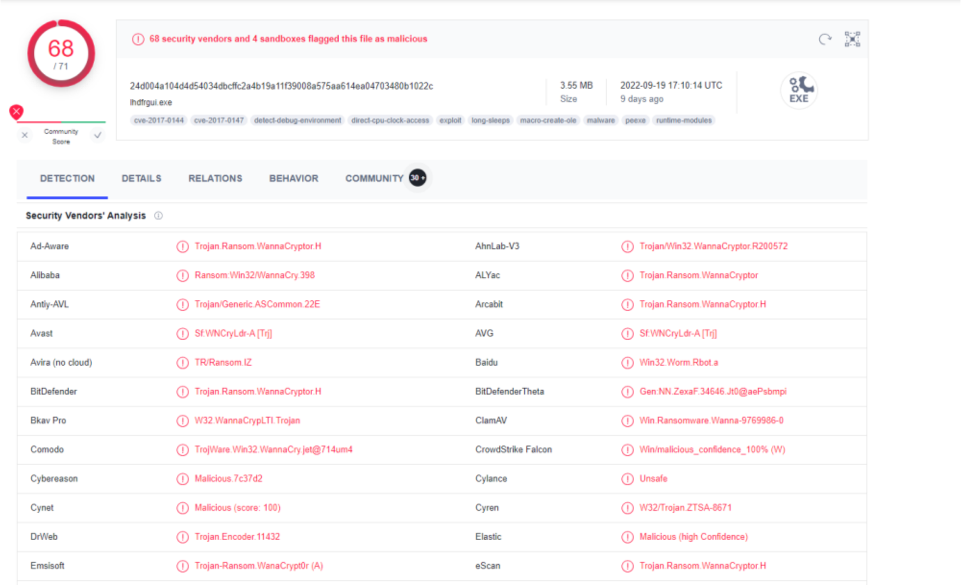
The initial executable that tries to contact the url. If url is alive it doesn’t execute else unpacks the taskche.exe.

Taskche.exe:

This program is used for presistence. It create random folder for wannacry staging area inside ProgramData. After execution of malware on host, it tries to speard to other computer via smb on port 445. It starts encrypting all the files and after that it displays the ransomware popup message.

Basic Static Analysis

VirusTotal Analysis



68 / 71

Community Score

68 security vendors and 4 sandboxes flagged this file as malicious

24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
lhdfrgui.exe

3.55 MB
Size

2022-09-19 17:10:14 UTC
9 days ago

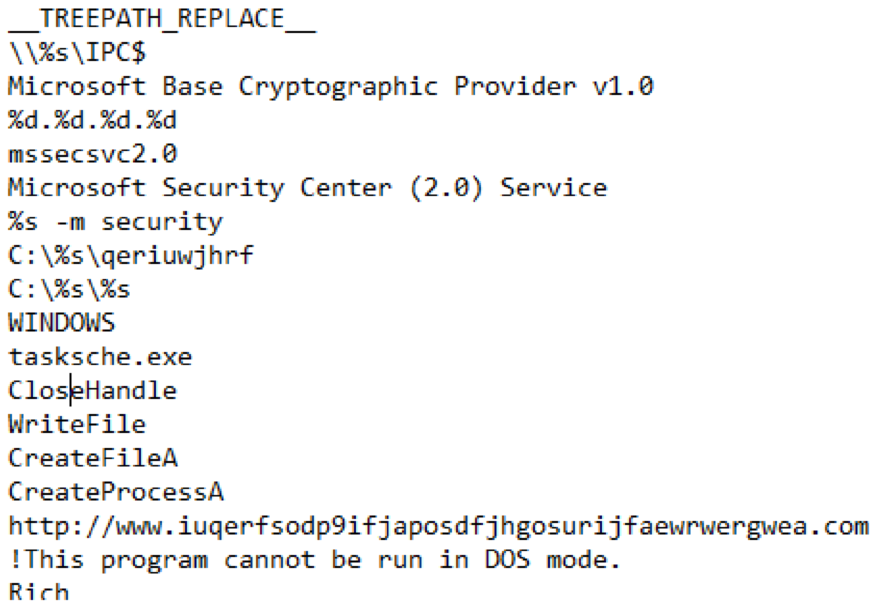
EXE

cve-2017-0144 cve-2017-0147 detect-debug-environment direct-cpu-clock-access exploit long-sleeps macro-create-ole malware peexe runtime-modules

Security Vendors' Analysis

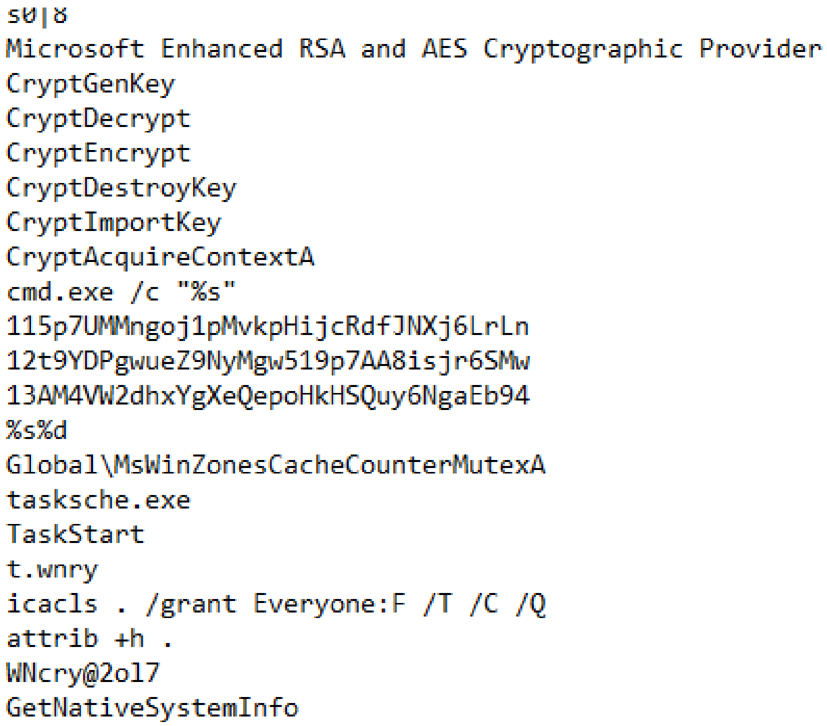
Ad-Aware	Trojan.Ransom.WannaCryptor.H	AhnLab-V3	Trojan/Win32.WannaCryptor.R200572
Alibaba	Ransom:Win32/WannaCry.398	ALYac	Trojan.Ransom.WannaCryptor
Antiy-AVL	Trojan/Generic.ASCommon.22E	Arcabit	Trojan.Ransom.WannaCryptor.H
Avast	Sf:WNCryLdr-A [Trj]	AVG	Sf:WNCryLdr-A [Trj]
Avira (no cloud)	TR/Ransom.IZ	Baidu	Win32.Worm.Rbot.a
BitDefender	Trojan.Ransom.WannaCryptor.H	BitDefenderTheta	Gen:NN.ZexaF.34646.Jt0@aePsbmpi
Bkav Pro	W32.WannaCrypLTI.Trojan	ClamAV	Win.Ransomware.Wanna-9769986-0
Comodo	TrojWare.Win32.WannaCry.jet@714um4	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cybereason	Malicious.7c37d2	Cylance	Unsafe
Cynet	Malicious (score: 100)	Cyren	W32/Trojan.ZTSA-8671
DrWeb	Trojan.Encoder.11432	Elastic	Malicious (high Confidence)
Emsisoft	Trojan-Ransom.WanaCrypt0r (A)	eScan	Trojan.Ransom.WannaCryptor.H

String./Floss Output



```
__TREEPATH_REPLACE__
\\%s\IPC$
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.
Rich
```

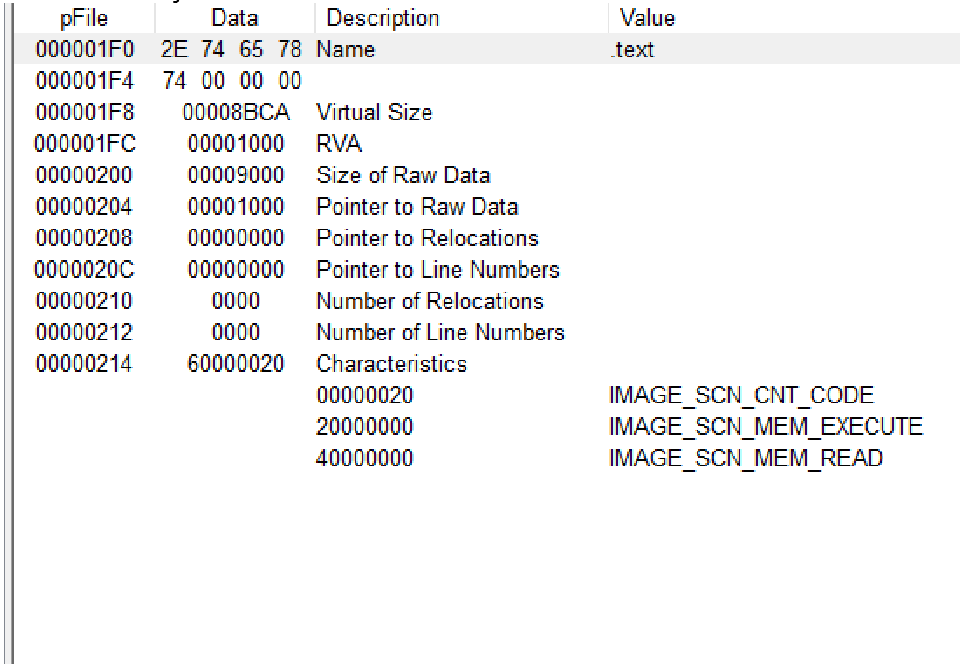
Fig –2 – Kill Switch Url and random paths



```
s0|8
Microsoft Enhanced RSA and AES Cryptographic Provider
CryptGenKey
CryptDecrypt
CryptEncrypt
CryptDestroyKey
CryptImportKey
CryptAcquireContextA
cmd.exe /c "%s"
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
%s%d
Global\MsWinZonesCacheCounterMutexA
tasksche.exe
TaskStart
t.wnry
icacls . /grant Everyone:F /T /C /Q
attrib +h .
WNcry@2ol7
GetNativeSystemInfo
```

Fig –3 – Some imports, ical used for modifying acess control on file ,attrib +h to hide file attribute

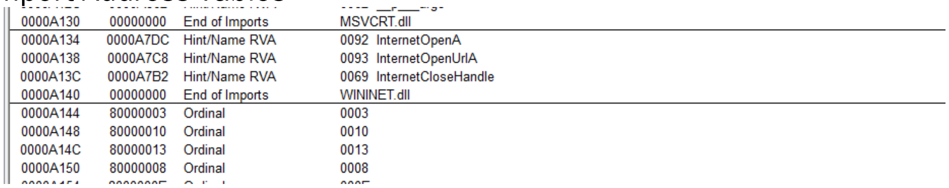
PE View Analysis



pFile	Data	Description	Value
000001F0	2E 74 65 78	Name	.text
000001F4	74 00 00 00		
000001F8	00008BCA	Virtual Size	
000001FC	00001000	RVA	
00000200	00009000	Size of Raw Data	
00000204	00001000	Pointer to Raw Data	
00000208	00000000	Pointer to Relocations	
0000020C	00000000	Pointer to Line Numbers	
00000210	0000	Number of Relocations	
00000212	0000	Number of Line Numbers	
00000214	60000020	Characteristics	
		00000020	IMAGE_SCN_CNT_CODE
		20000000	IMAGE_SCN_MEM_EXECUTE
		40000000	IMAGE_SCN_MEM_READ

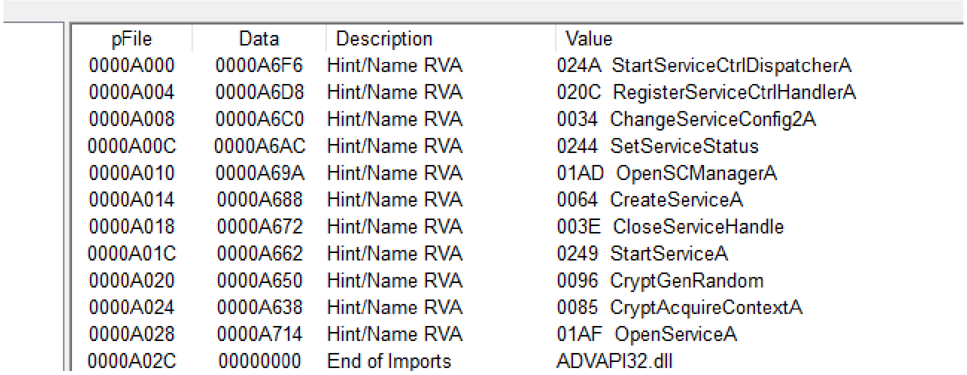
Fig – 4- (Unpacked Size)

Import Address Tables



0000A130	00000000	End of Imports	MSVCRT.dll
0000A134	0000A7DC	Hint/Name RVA	0092 InternetOpenA
0000A138	0000A7C8	Hint/Name RVA	0093 InternetOpenUrlA
0000A13C	0000A7B2	Hint/Name RVA	0069 InternetCloseHandle
0000A140	00000000	End of Imports	WININET.dll
0000A144	80000003	Ordinal	0003
0000A148	80000010	Ordinal	0010
0000A14C	80000013	Ordinal	0013
0000A150	80000008	Ordinal	0008

Fig –5 – Internet Connection Address/Imports

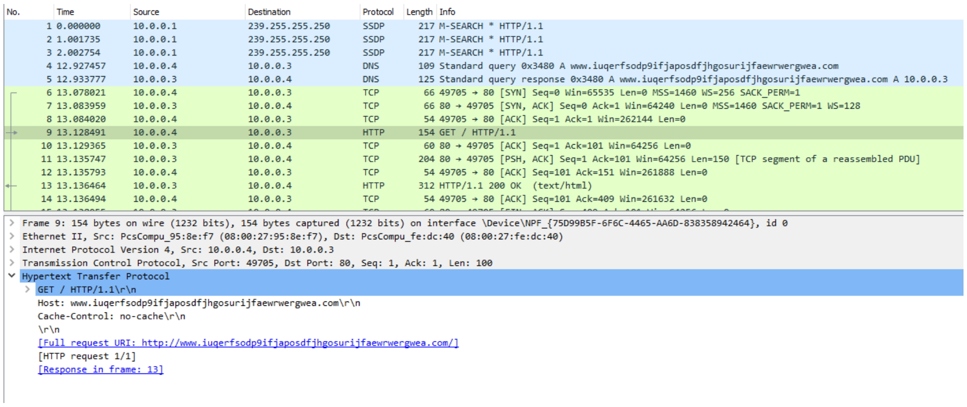


pFile	Data	Description	Value
0000A000	0000A6F6	Hint/Name RVA	024A StartServiceCtrlDispatcherA
0000A004	0000A6D8	Hint/Name RVA	020C RegisterServiceCtrlHandlerA
0000A008	0000A6C0	Hint/Name RVA	0034 ChangeServiceConfig2A
0000A00C	0000A6AC	Hint/Name RVA	0244 SetServiceStatus
0000A010	0000A69A	Hint/Name RVA	01AD OpenSCManagerA
0000A014	0000A688	Hint/Name RVA	0064 CreateServiceA
0000A018	0000A672	Hint/Name RVA	003E CloseServiceHandle
0000A01C	0000A662	Hint/Name RVA	0249 StartServiceA
0000A020	0000A650	Hint/Name RVA	0096 CryptGenRandom
0000A024	0000A638	Hint/Name RVA	0085 CryptAcquireContextA
0000A028	0000A714	Hint/Name RVA	01AF OpenServiceA
0000A02C	00000000	End of Imports	ADVAPI32.dll

Fig – 6- Encrptying Import Address/Imports

Basic Dynamic Analysis

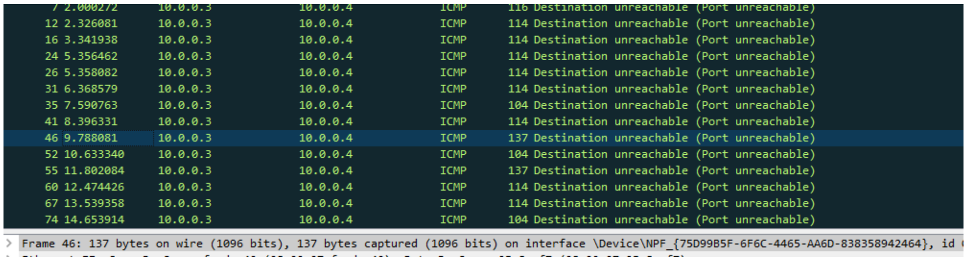
Analysis with InetSim – ON



```
No.     Time         Source       Destination       Protocol  Length Info
      1 0.000000     10.0.0.1     239.255.255.250   SSDP       217 M-SEARCH * HTTP/1.1
      2 1.001735     10.0.0.1     239.255.255.250   SSDP       217 M-SEARCH * HTTP/1.1
      3 2.002754     10.0.0.1     239.255.255.250   SSDP       217 M-SEARCH * HTTP/1.1
      4 12.927457    10.0.0.4     10.0.0.3          DNS        109 Standard query 0x3480 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
      5 12.933777    10.0.0.3     10.0.0.4          DNS        125 Standard query response 0x3480 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com A 10.0.0.3
      6 13.078021    10.0.0.4     10.0.0.3          TCP         66 49705 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
      7 13.083959    10.0.0.3     10.0.0.4          TCP         66 80 → 49705 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
      8 13.084020    10.0.0.4     10.0.0.3          TCP         54 49705 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
      9 13.128491    10.0.0.4     10.0.0.3          HTTP       154 GET / HTTP/1.1
     10 13.129365    10.0.0.3     10.0.0.4          TCP         60 80 → 49705 [ACK] Seq=1 Ack=101 Win=64256 Len=0
     11 13.135747    10.0.0.3     10.0.0.4          TCP        204 80 → 49705 [PSH, ACK] Seq=1 Ack=101 Win=64256 Len=150 [TCP segment of a reassembled PDU]
     12 13.135793    10.0.0.4     10.0.0.3          TCP         54 49705 → 80 [ACK] Seq=101 Ack=151 Win=261888 Len=0
     13 13.136464    10.0.0.3     10.0.0.4          HTTP       312 HTTP/1.1 200 OK  (text/html)
     14 13.136494    10.0.0.4     10.0.0.3          TCP         54 49705 → 80 [ACK] Seq=101 Ack=409 Win=261632 Len=0

> Frame 9: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) on interface \Device\NPF_{75D99B5F-6F6C-4465-AA6D-838358942464}, id 0
> Ethernet II, Src: PcsCompu_95:8e:f7 (08:00:27:95:8e:f7), Dst: PcsCompu_fe:dc:40 (08:00:27:fe:dc:40)
> Internet Protocol Version 4, Src: 10.0.0.4, Dst: 10.0.0.3
> Transmission Control Protocol, Src Port: 49705, Dst Port: 80, Seq: 1, Ack: 1, Len: 100
v 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: 13]
```

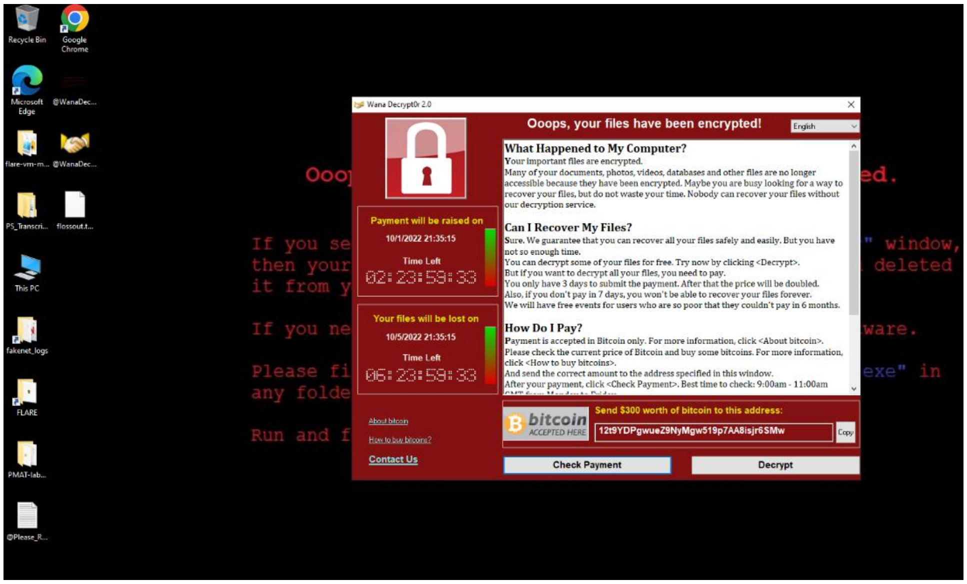
Fig - 7- Network Traffic when malware is executed
Here , you can see that it is contacting the url and receving something in return. So, it is not executing in the system.

Analysis with InetSim – Off



```
      7 2.000272     10.0.0.3     10.0.0.4     ICMP     116 Destination unreachable (Port unreachable)
     12 2.326081     10.0.0.3     10.0.0.4     ICMP     114 Destination unreachable (Port unreachable)
     16 3.341938     10.0.0.3     10.0.0.4     ICMP     114 Destination unreachable (Port unreachable)
     24 5.356462     10.0.0.3     10.0.0.4     ICMP     114 Destination unreachable (Port unreachable)
     26 5.358082     10.0.0.3     10.0.0.4     ICMP     114 Destination unreachable (Port unreachable)
     31 6.368579     10.0.0.3     10.0.0.4     ICMP     114 Destination unreachable (Port unreachable)
     35 7.590763     10.0.0.3     10.0.0.4     ICMP     104 Destination unreachable (Port unreachable)
     41 8.396331     10.0.0.3     10.0.0.4     ICMP     114 Destination unreachable (Port unreachable)
     46 9.788081     10.0.0.3     10.0.0.4     ICMP     137 Destination unreachable (Port unreachable)
     52 10.633340    10.0.0.3     10.0.0.4     ICMP     104 Destination unreachable (Port unreachable)
     55 11.802084    10.0.0.3     10.0.0.4     ICMP     137 Destination unreachable (Port unreachable)
     60 12.474426    10.0.0.3     10.0.0.4     ICMP     114 Destination unreachable (Port unreachable)
     67 13.539358    10.0.0.3     10.0.0.4     ICMP     114 Destination unreachable (Port unreachable)
     74 14.653914    10.0.0.3     10.0.0.4     ICMP     104 Destination unreachable (Port unreachable)

> Frame 46: 137 bytes on wire (1096 bits), 137 bytes captured (1096 bits) on interface \Device\NPF_{75D99B5F-6F6C-4465-AA6D-838358942464}, id
```

Fig – 8 – Network Traffic when malware execute. The request are unreachable since inetsim is off.



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
10/1/2022 21:35:15
Time Left
02:23:59:33

Your files will be lost on
10/5/2022 21:35:15
Time Left
06:23:59:33

bitcoin ACCEPTED HERE

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

About bitcoin

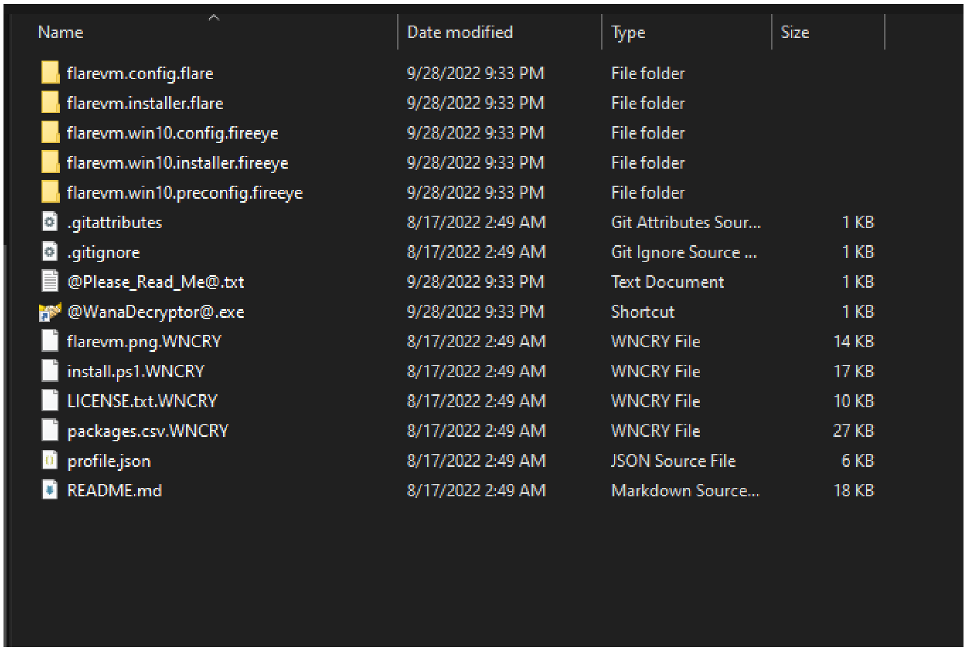
How to buy bitcoins?

Contact Us

Check Payment

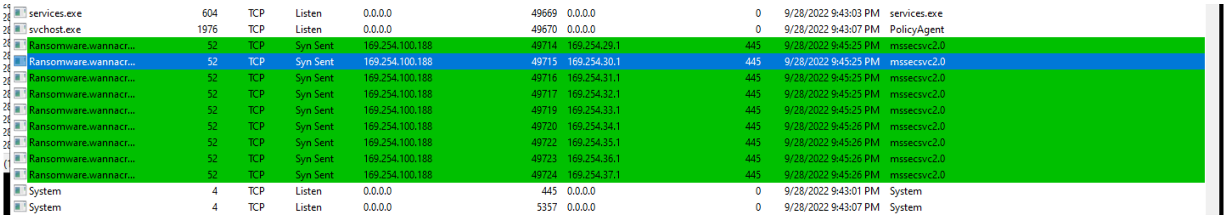
Decrypt

Fig – 9 – After infection, the desktop and payment screen.



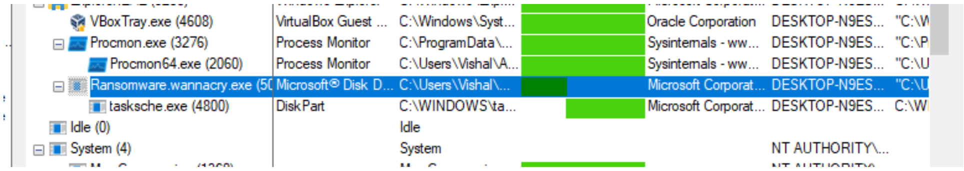
Name	Date modified	Type	Size
flarevm.config.flare	9/28/2022 9:33 PM	File folder	
flarevm.installer.flare	9/28/2022 9:33 PM	File folder	
flarevm.win10.config.fireeye	9/28/2022 9:33 PM	File folder	
flarevm.win10.installer.fireeye	9/28/2022 9:33 PM	File folder	
flarevm.win10.preconfig.fireeye	9/28/2022 9:33 PM	File folder	
.gitattributes	8/17/2022 2:49 AM	Git Attributes Sour...	1 KB
.gitignore	8/17/2022 2:49 AM	Git Ignore Source ...	1 KB
@Please_Read_Me@.txt	9/28/2022 9:33 PM	Text Document	1 KB
@WanaDecryptor@.exe	9/28/2022 9:33 PM	Shortcut	1 KB
flarevm.png.WNCRY	8/17/2022 2:49 AM	WNCRY File	14 KB
install.ps1.WNCRY	8/17/2022 2:49 AM	WNCRY File	17 KB
LICENSE.txt.WNCRY	8/17/2022 2:49 AM	WNCRY File	10 KB
packages.csv.WNCRY	8/17/2022 2:49 AM	WNCRY File	27 KB
profile.json	8/17/2022 2:49 AM	JSON Source File	6 KB
README.md	8/17/2022 2:49 AM	Markdown Source...	18 KB

Fig – 10 – Encrypted file with extension .WNCRY and New files added.



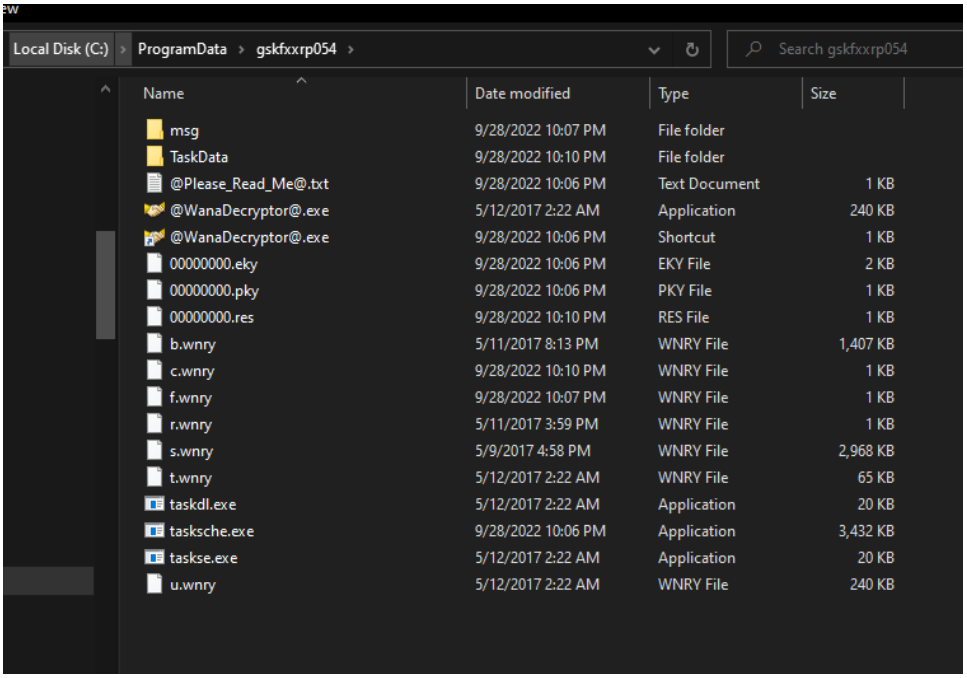
```
services.exe              604   TCP   Listen     0.0.0.0           49669  0.0.0.0          0    9/28/2022 9:43:03 PM  services.exe
svchost.exe              1976   TCP   Listen     0.0.0.0           49670  0.0.0.0          0    9/28/2022 9:43:07 PM  PolicyAgent
Ransomware.wannacr...      52   TCP   Syn Sent   169.254.100.188   49714  169.254.29.1   445    9/28/2022 9:45:25 PM  mssecsvc2.0
Ransomware.wannacr...      52   TCP   Syn Sent   169.254.100.188   49715  169.254.30.1   445    9/28/2022 9:45:25 PM  mssecsvc2.0
Ransomware.wannacr...      52   TCP   Syn Sent   169.254.100.188   49716  169.254.31.1   445    9/28/2022 9:45:25 PM  mssecsvc2.0
Ransomware.wannacr...      52   TCP   Syn Sent   169.254.100.188   49717  169.254.32.1   445    9/28/2022 9:45:25 PM  mssecsvc2.0
Ransomware.wannacr...      52   TCP   Syn Sent   169.254.100.188   49719  169.254.33.1   445    9/28/2022 9:45:25 PM  mssecsvc2.0
Ransomware.wannacr...      52   TCP   Syn Sent   169.254.100.188   49720  169.254.34.1   445    9/28/2022 9:45:26 PM  mssecsvc2.0
Ransomware.wannacr...      52   TCP   Syn Sent   169.254.100.188   49722  169.254.35.1   445    9/28/2022 9:45:26 PM  mssecsvc2.0
Ransomware.wannacr...      52   TCP   Syn Sent   169.254.100.188   49723  169.254.36.1   445    9/28/2022 9:45:26 PM  mssecsvc2.0
Ransomware.wannacr...      52   TCP   Syn Sent   169.254.100.188   49724  169.254.37.1   445    9/28/2022 9:45:26 PM  mssecsvc2.0
System                      4   TCP   Listen     0.0.0.0             445  0.0.0.0          0    9/28/2022 9:43:01 PM  System
System                      4   TCP   Listen     0.0.0.0            5357  0.0.0.0          0    9/28/2022 9:43:07 PM  System
```

Fig –11 – Taskche.exe tries to locate and infect computer using port 445(SMB)



```
      VBoxTray.exe (4608)            VirtualBox Guest ...   C:\Windows\Syst...    Oracle Corporation     DESKTOP-N9ES...   "C:\W
   ⊟  Procmon.exe (3276)             Process Monitor        C:\ProgramData\...    Sysinternals - ww...   DESKTOP-N9ES...   "C:\P
        Procmon64.exe (2060)         Process Monitor        C:\Users\Vishal\A...  Sysinternals - ww...   DESKTOP-N9ES...   "C:\U
   ⊟  Ransomware.wannacry.exe (50    Microsoft® Disk D...   C:\Users\Vishal\...   Microsoft Corporat...  DESKTOP-N9ES...   "C:\U
        tasksche.exe (4800)          DiskPart               C:\WINDOWS\ta...      Microsoft Corporat...  DESKTOP-N9ES...   C:\W
   Idle (0)                                                 Idle
⊟  System (4)                                               System                                       NT AUTHORITY\...
```

Fig – 12 – Procmon Process tree for wannacry.



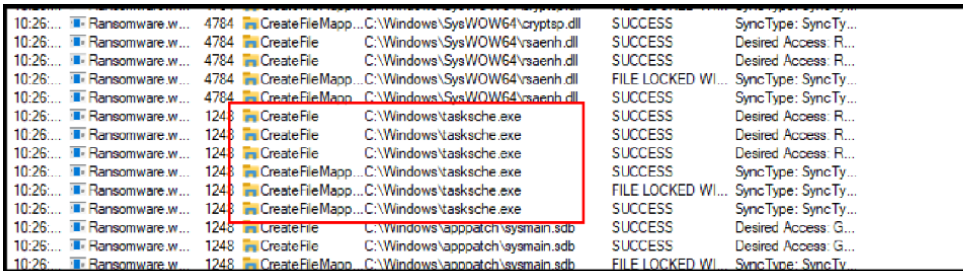
ew

Local Disk (C:) › ProgramData › gskfxxrp054 ›

Search gskfxxrp054

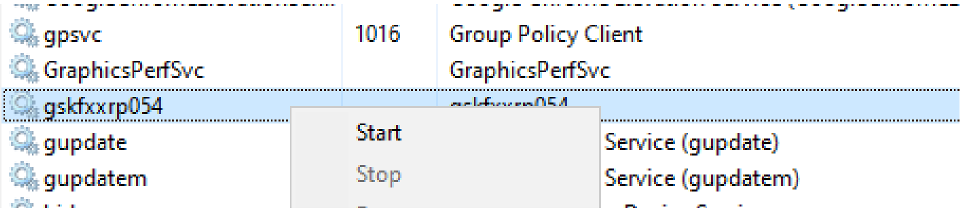
Name	Date modified	Type	Size
msg	9/28/2022 10:07 PM	File folder	
TaskData	9/28/2022 10:10 PM	File folder	
@Please_Read_Me@.txt	9/28/2022 10:06 PM	Text Document	1 KB
@WanaDecryptor@.exe	5/12/2017 2:22 AM	Application	240 KB
@WanaDecryptor@.exe	9/28/2022 10:06 PM	Shortcut	1 KB
00000000.eky	9/28/2022 10:06 PM	EKY File	2 KB
00000000.pky	9/28/2022 10:06 PM	PKY File	1 KB
00000000.res	9/28/2022 10:10 PM	RES File	1 KB
b.wnry	5/11/2017 8:13 PM	WNRY File	1,407 KB
c.wnry	9/28/2022 10:10 PM	WNRY File	1 KB
f.wnry	9/28/2022 10:07 PM	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	9/28/2022 10:06 PM	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

Fig – 13 – New Folder Created with random name in C:/ProgramData/{random name}



```
10:26:...  Ransomware.w...  4784  CreateFileMapp...C:\Windows\SysWOW64\cryptsp.dll    SUCCESS          SyncType: SyncTy...
10:26:...  Ransomware.w...  4784  CreateFile       C:\Windows\SysWOW64\rsaenh.dll     SUCCESS          Desired Access: R...
10:26:...  Ransomware.w...  4784  CreateFile       C:\Windows\SysWOW64\rsaenh.dll     SUCCESS          Desired Access: R...
10:26:...  Ransomware.w...  4784  CreateFileMapp...C:\Windows\SysWOW64\rsaenh.dll     FILE LOCKED WI...  SyncType: SyncTy...
10:26:...  Ransomware.w...  4784  CreateFileMapp   C:\Windows\SysWOW64\rsaenh.dll     SUCCESS          SyncType: SyncTy...
10:26:...  Ransomware.w...  1248  CreateFile       C:\Windows\tasksche.exe            SUCCESS          Desired Access: R...
10:26:...  Ransomware.w...  1248  CreateFile       C:\Windows\tasksche.exe            SUCCESS          Desired Access: R...
10:26:...  Ransomware.w...  1248  CreateFile       C:\Windows\tasksche.exe            SUCCESS          Desired Access: R...
10:26:...  Ransomware.w...  1248  CreateFileMapp...C:\Windows\tasksche.exe            SUCCESS          SyncType: SyncTy...
10:26:...  Ransomware.w...  1248  CreateFileMapp...C:\Windows\tasksche.exe            FILE LOCKED WI...  SyncType: SyncTy...
10:26:...  Ransomware.w...  1248  CreateFileMapp...C:\Windows\tasksche.exe            SUCCESS          SyncType: SyncTy...
10:26:...  Ransomware.w...  1248  CreateFile       C:\Windows\apppatch\sysmain.sdb    SUCCESS          Desired Access: G...
10:26:...  Ransomware.w...  1248  CreateFile       C:\Windows\apppatch\sysmain.sdb    SUCCESS          Desired Access: G...
10:26:...  Ransomware.w...  1248  CreateFileMapp   C:\Windows\apppatch\sysmain.sdb    FILE LOCKED WI...  SyncType: SyncTy...
```

Fig – 14 – Creation of taskche.exe file

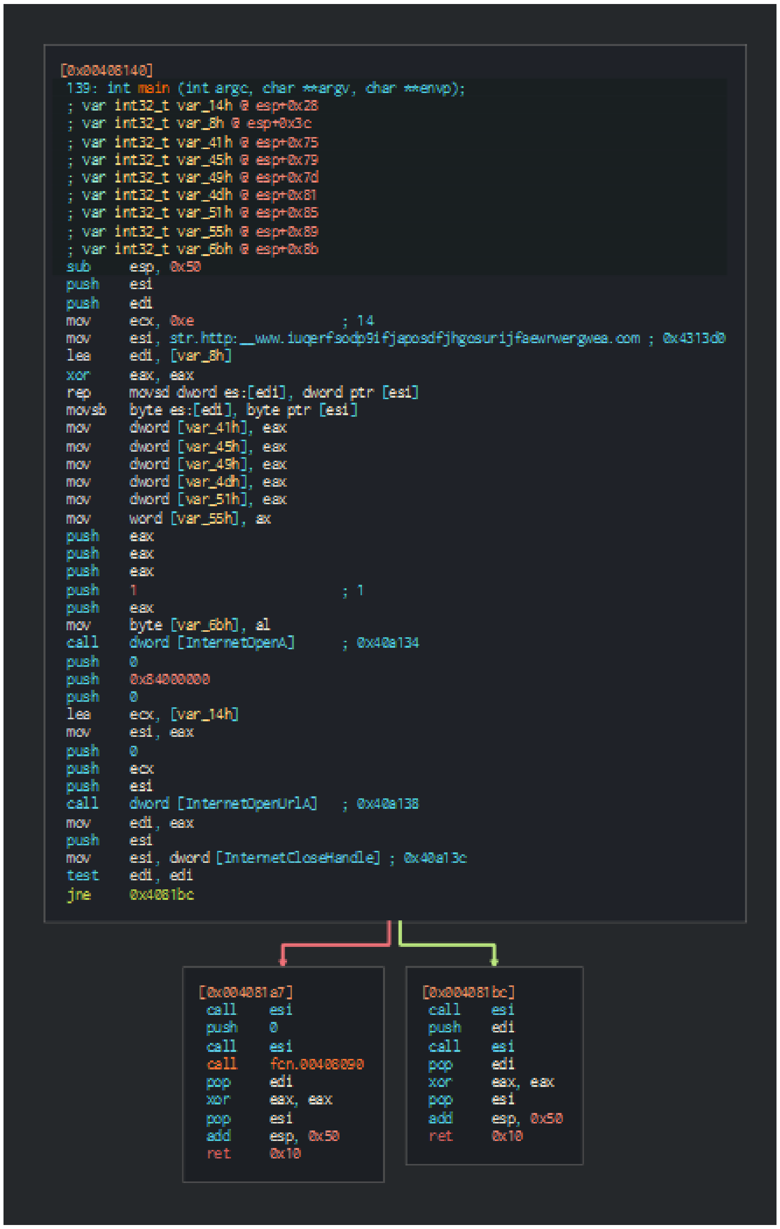


gpsvc	1016	Group Policy Client
GraphicsPerfSvc		GraphicsPerfSvc
gskfxxrp054		gskfxxrp054
gupdate		Service (gupdate)
gupdatem		Service (gupdatem)

Fig – 15- Task Manager. A service named as the random folder created by malware.

Advanced Static Analysis

Cutter



```
[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     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
```

```
[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 – 16 –main function Code in Cutter

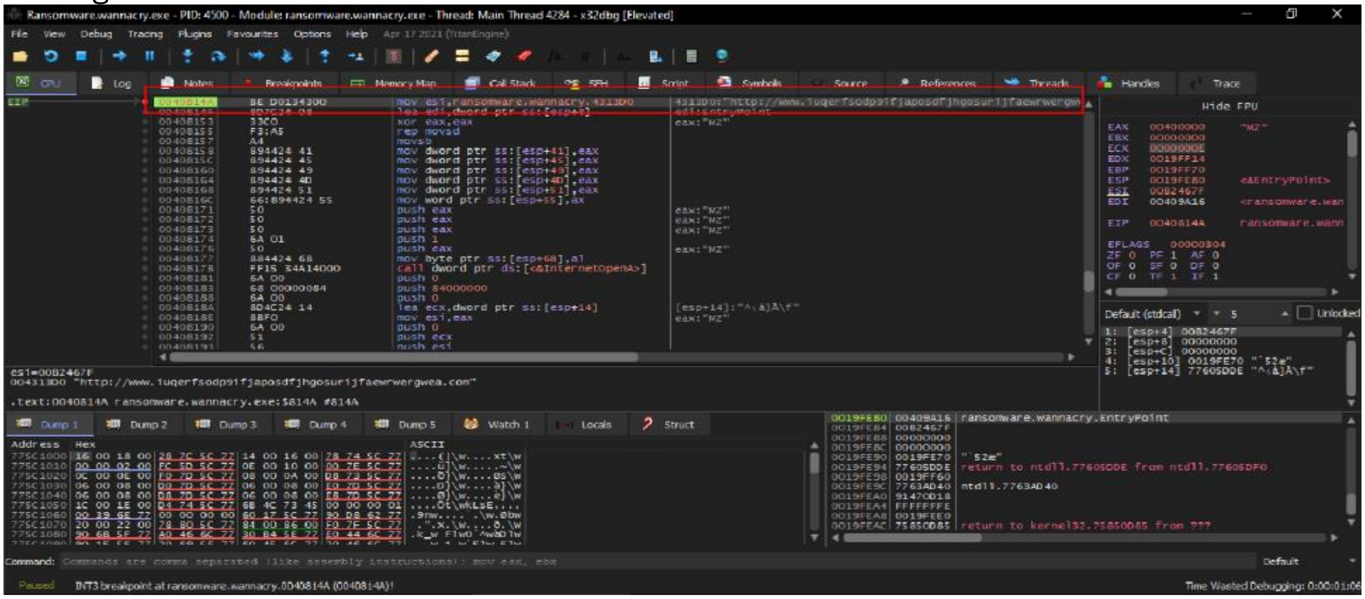
The kill Switch URL is located in the main method. When the exe file is executed , it runs the InternetOpenA API which requires a URL and result of is in form of boolean which is stored in the edi.

Once that is stored then it checks the edi value if its true that is the malware was able to contact the url then it would not execute and goto the right side of code.

On the other hand if it did not contact the url then it will goto the left side of code and execute the rest of malware functionality.

Advanced Dynamic Analysis

X32dbg



Ransomware.wannacry.exe - PID: 4500 - Module: ransomware.wannacry.exe - Thread: Main Thread 4284 - x32dbg [Elevated]

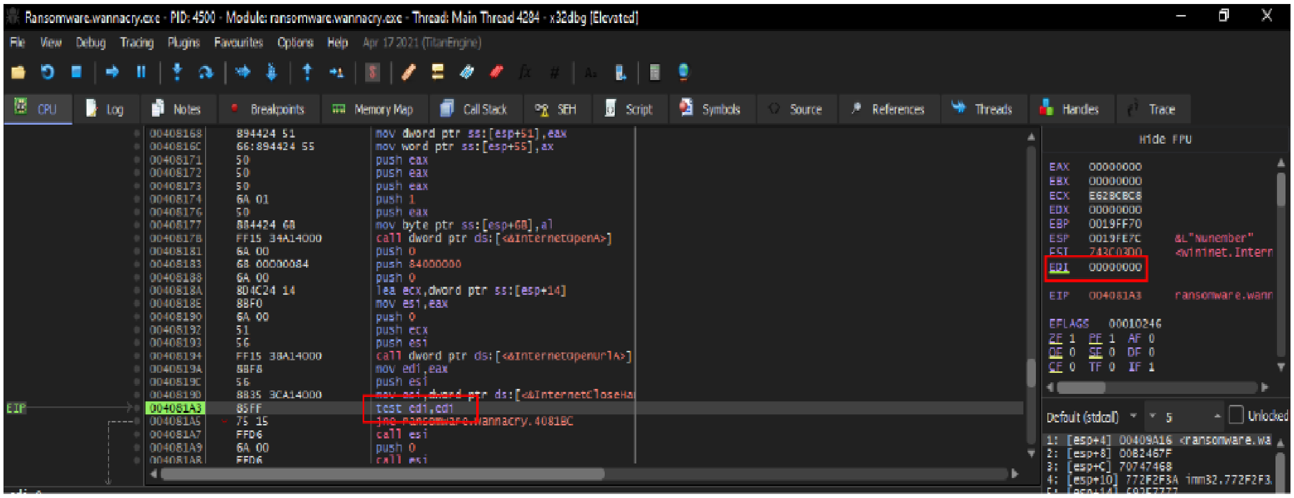
```
0040814A   BE D0134300        mov esi,ransomware.wannacry.4313D0           4313D0:"http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com"
0040814F   8D7C24 08          lea edi,dword ptr ss:[esp+8]                 edi:EntryPoint
00408153   33C0               xor eax,eax                                  eax:"MZ"
00408155   F3:A5              rep movsd
00408157   A4                 movsb
00408158   894424 41          mov dword ptr ss:[esp+41],eax
0040815C   894424 45          mov dword ptr ss:[esp+45],eax
00408160   894424 49          mov dword ptr ss:[esp+49],eax
00408164   894424 4D          mov dword ptr ss:[esp+4D],eax
00408168   894424 51          mov dword ptr ss:[esp+51],eax
0040816C   66:894424 55       mov word ptr ss:[esp+55],ax
00408171   50                 push eax                                     eax:"MZ"
00408172   50                 push eax                                     eax:"MZ"
00408173   50                 push eax                                     eax:"MZ"
00408174   6A 01              push 1
00408176   50                 push eax                                     eax:"MZ"
00408177   884424 6B          mov byte ptr ss:[esp+6B],al
0040817B   FF15 34A14000      call dword ptr ds:[<&InternetOpenA>]
00408181   6A 00              push 0
00408183   68 00000084        push 84000000
00408188   6A 00              push 0
0040818A   8D4C24 14          lea ecx,dword ptr ss:[esp+14]                [esp+14]:"^‹åJÅ\f"
0040818E   8BF0               mov esi,eax                                  eax:"MZ"
00408190   6A 00              push 0
00408192   51                 push ecx
00408193   56                 push esi

esi=0082467F
004313D0 "http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com"

.text:0040814A ransomware.wannacry.exe:$814A #814A
```

```
EAX     00400000     "MZ"
EBX     00000000
ECX     0000000E
EDX     0019FF14
EBP     0019FF70
ESP     0019FE80     <&EntryPoint>
ESI     0082467F
EDI     00409A16     <ransomware.wan
EIP     0040814A     ransomware.wann

EFLAGS    00000304
ZF 0  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 1  IF 1

Default (stdcall)   5   Unlocked
1: [esp+4]  0082467F
2: [esp+8]  00000000
3: [esp+C]  00000000
4: [esp+10] 0019FE70 "`52e"
5: [esp+14] 77605DDE "^‹åJÅ\f"
```

```
0019FE80  00409A16  ransomware.wannacry.EntryPoint
0019FE84  0082467F
0019FE88  00000000
0019FE8C  00000000
0019FE90  0019FE70  "`52e"
0019FE94  77605DDE  return to ntdll.77605DDE from ntdll.77605DF0
0019FE98  0019FF60
0019FE9C  7763AD40  ntdll.7763AD40
0019FEA0  9147CD18
0019FEA4  FFFFFFFE
0019FEA8  0019FEE0
0019FEAC  75850085  return to kernel32.75850085 from ???
```

Paused   INT3 breakpoint at ransomware.wannacry.0040814A (0040814A)!   Time Wasted Debugging: 0:00:01:06

Fig-17 - Set a Break point on the kill switch url

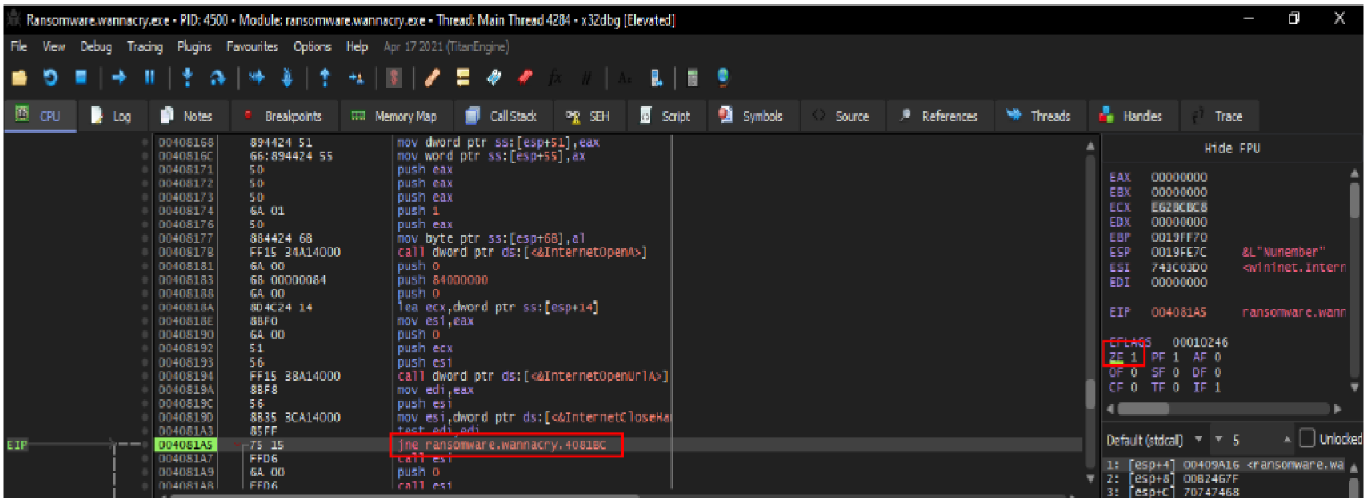


Ransomware.wannacry.exe - PID: 4500 - Module: ransomware.wannacry.exe - Thread: Main Thread 4284 - x32dbg [Elevated]

```
00408168   894424 51          mov dword ptr ss:[esp+51],eax
0040816C   66:894424 55       mov word ptr ss:[esp+55],ax
00408171   50                 push eax
00408172   50                 push eax
00408173   50                 push eax
00408174   6A 01              push 1
00408176   50                 push eax
00408177   884424 6B          mov byte ptr ss:[esp+6B],al
0040817B   FF15 34A14000      call dword ptr ds:[<&InternetOpenA>]
00408181   6A 00              push 0
00408183   68 00000084        push 84000000
00408188   6A 00              push 0
0040818A   8D4C24 14          lea ecx,dword ptr ss:[esp+14]
0040818E   8BF0               mov esi,eax
00408190   6A 00              push 0
00408192   51                 push ecx
00408193   56                 push esi
00408194   FF15 38A14000      call dword ptr ds:[<&InternetOpenUrlA>]
0040819A   8BF8               mov edi,eax
0040819C   56                 push esi
0040819D   8B35 3CA14000      mov esi,dword ptr ds:[<&InternetCloseHa
004081A3   85FF               test edi,edi
004081A5   75 15              jne ransomware.wannacry.4081BC
004081A7   FFD6               call esi
004081A9   6A 00              push 0
004081AB   FFD6               call esi
```

```
EAX     00000000
EBX     00000000
ECX     E62BCBC8
EDX     00000000
EBP     0019FF70
ESP     0019FE7C     &L"Nunember"
ESI     743C03D0     <wininet.Intern
EDI     00000000

EIP     004081A3     ransomware.wann

EFLAGS    00010246
ZF 1  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1

Default (stdcall)   5   Unlocked
1: [esp+4]  00409A16 <ransomware.wa
2: [esp+8]  0082467F
3: [esp+C]  70747468
4: [esp+10] 772F2F3A inm32.772F2F3
```

Fig –18 - The kill switch was not found hence EDI value is 0

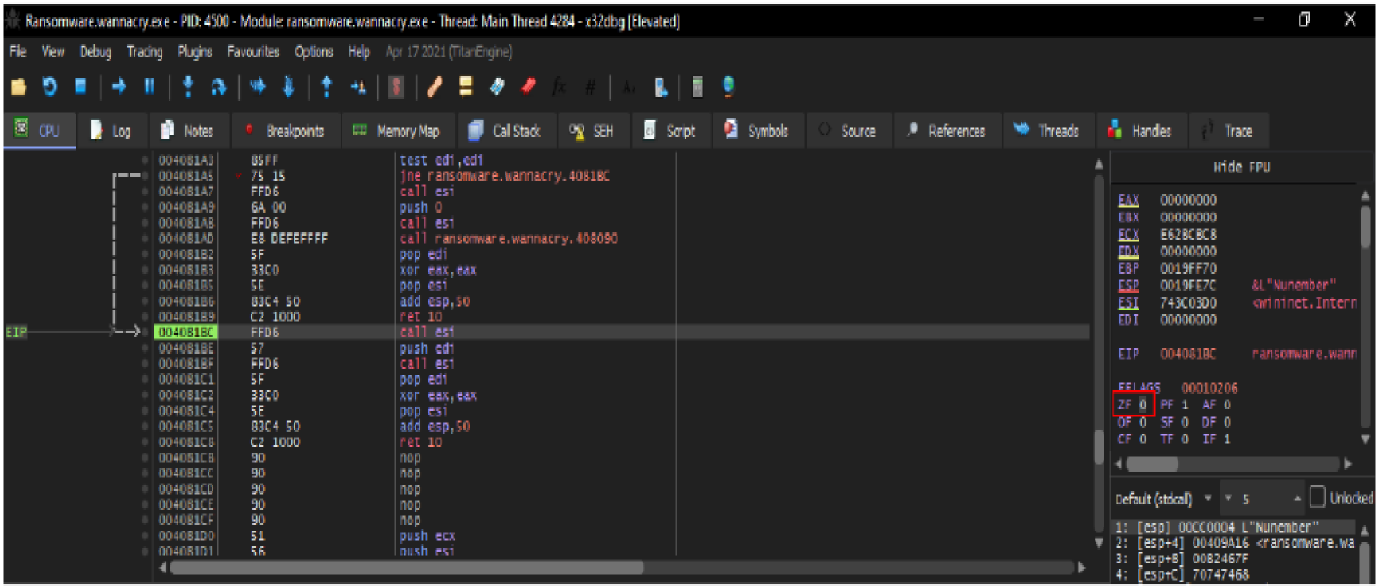

Ransomware.wannacry.exe - PID: 4500 - Module: ransomware.wannacry.exe - Thread: Main Thread 4284 - x32dbg [Elevated]
File View Debug Tracing Plugins Favourites Options Help Apr 17 2021 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace
Hide FPU
Default (stdcall) 5 Unlocked

```
00408168   894424 51        mov dword ptr ss:[esp+51],eax
0040816C   66:894424 55     mov word ptr ss:[esp+55],ax
00408171   50               push eax
00408172   50               push eax
00408173   50               push eax
00408174   6A 01            push 1
00408176   50               push eax
00408177   884424 68        mov byte ptr ss:[esp+68],al
0040817B   FF15 34A14000    call dword ptr ds:[<&InternetOpenA>]
00408181   6A 00            push 0
00408183   68 00000084      push 84000000
00408188   6A 00            push 0
0040818A   8D4C24 14        lea ecx,dword ptr ss:[esp+14]
0040818E   8BF0             mov esi,eax
00408190   6A 00            push 0
00408192   51               push ecx
00408193   56               push esi
00408194   FF15 38A14000    call dword ptr ds:[<&InternetOpenUrlA>]
0040819A   8BF8             mov edi,eax
0040819C   56               push esi
0040819D   8B35 3CA14000    mov esi,dword ptr ds:[<&InternetCloseHa
004081A3   85FF             test edi,edi
EIP 004081A5   75 15        jne ransomware.wannacry.4081BC
004081A7   FFD6             call esi
004081A9   6A 00            push 0
004081AB   FFD6             call esi
```

```
EAX    00000000
EBX    00000000
ECX    E628CBC8
EDX    00000000
EBP    0019FF70
ESP    0019FE7C    &L"Nunember"
ESI    743C03D0    <wininet.Intern
EDI    00000000

EIP    004081A5    ransomware.wann

EFLAGS    00010246
ZF 1   PF 1   AF 0
OF 0   SF 0   DF 0
CF 0   TF 0   IF 1
```

```
1: [esp+4] 00409A16 <ransomware.wa
2: [esp+8] 0082467F
3: [esp+C] 70747468
```

Fig - 19- The zero is elevated to 1 but we change it to 0


Ransomware.wannacry.exe - PID: 4500 - Module: ransomware.wannacry.exe - Thread: Main Thread 4284 - x32dbg [Elevated]
File View Debug Tracing Plugins Favourites Options Help Apr 17 2021 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace
Hide FPU
Default (stdcall) 5 Unlocked

```
004081A3   85FF             test edi,edi
004081A5   75 15            jne ransomware.wannacry.4081BC
004081A7   FFD6             call esi
004081A9   6A 00            push 0
004081AB   FFD6             call esi
004081AD   E8 DEFEFFFF      call ransomware.wannacry.408090
004081B2   5F               pop edi
004081B3   33C0             xor eax,eax
004081B5   5E               pop esi
004081B6   83C4 50          add esp,50
004081B9   C2 1000          ret 10
EIP 004081BC   FFD6         call esi
004081BE   57               push edi
004081BF   FFD6             call esi
004081C1   5F               pop edi
004081C2   33C0             xor eax,eax
004081C4   5E               pop esi
004081C5   83C4 50          add esp,50
004081C8   C2 1000          ret 10
004081CB   90               nop
004081CC   90               nop
004081CD   90               nop
004081CE   90               nop
004081CF   90               nop
004081D0   51               push ecx
004081D1   56               push esi
```

```
EAX    00000000
EBX    00000000
ECX    E628CBC8
EDX    00000000
EBP    0019FF70
ESP    0019FE7C    &L"Nunember"
ESI    743C03D0    <wininet.Intern
EDI    00000000

EIP    004081BC    ransomware.wann

EFLAGS    00010206
ZF 0   PF 1   AF 0
OF 0   SF 0   DF 0
CF 0   TF 0   IF 1
```

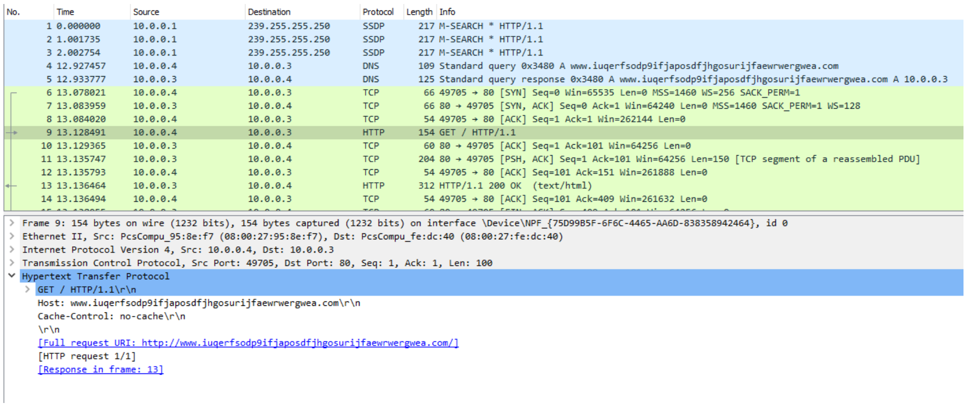
```
1: [esp] 00CC0004 L"Nunember"
2: [esp+4] 00409A16 <ransomware.wa
3: [esp+8] 0082467F
4: [esp+C] 70747468
```

Fig -20 -Changing the zero flag to 0 make the malware jump call and it is not executed

Indicators of Compromise

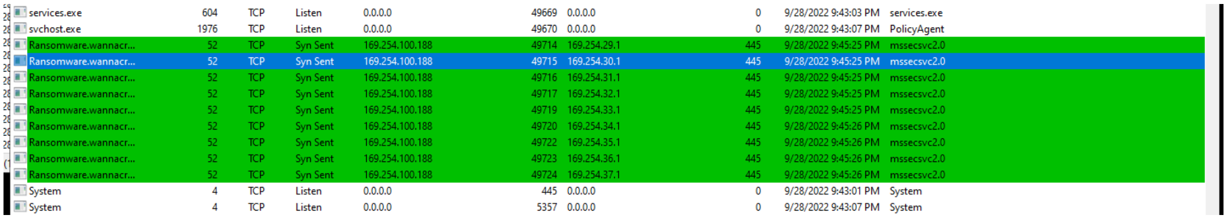
The full list of IOCs can be found in the Appendices.

Network Indicators



```
No.   Time        Source     Destination      Protocol Length Info
    1 0.000000    10.0.0.1   239.255.255.250  SSDP     217 M-SEARCH * HTTP/1.1
    2 1.001735    10.0.0.1   239.255.255.250  SSDP     217 M-SEARCH * HTTP/1.1
    3 2.002754    10.0.0.1   239.255.255.250  SSDP     217 M-SEARCH * HTTP/1.1
    4 12.927457   10.0.0.4   10.0.0.3         DNS      109 Standard query 0x3480 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
    5 12.933777   10.0.0.3   10.0.0.4         DNS      125 Standard query response 0x3480 A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com A 10.0.0.3
    6 13.078021   10.0.0.4   10.0.0.3         TCP       66 49705 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
    7 13.083959   10.0.0.3   10.0.0.4         TCP       66 80 → 49705 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
    8 13.084020   10.0.0.4   10.0.0.3         TCP       54 49705 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
    9 13.128491   10.0.0.4   10.0.0.3         HTTP     154 GET / HTTP/1.1
   10 13.129365   10.0.0.3   10.0.0.4         TCP       60 80 → 49705 [ACK] Seq=1 Ack=101 Win=64256 Len=0
   11 13.135747   10.0.0.3   10.0.0.4         TCP      204 80 → 49705 [PSH, ACK] Seq=1 Ack=101 Win=64256 Len=150 [TCP segment of a reassembled PDU]
   12 13.135793   10.0.0.4   10.0.0.3         TCP       54 49705 → 80 [ACK] Seq=101 Ack=151 Win=261888 Len=0
   13 13.136464   10.0.0.3   10.0.0.4         HTTP     312 HTTP/1.1 200 OK  (text/html)
   14 13.136494   10.0.0.4   10.0.0.3         TCP       54 49705 → 80 [ACK] Seq=101 Ack=409 Win=261632 Len=0

> Frame 9: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) on interface \Device\NPF_{75D99B5F-6F6C-4465-AA6D-838358942464}, id 0
> Ethernet II, Src: PcsCompu_95:8e:f7 (08:00:27:95:8e:f7), Dst: PcsCompu_fe:dc:40 (08:00:27:fe:dc:40)
> Internet Protocol Version 4, Src: 10.0.0.4, Dst: 10.0.0.3
> Transmission Control Protocol, Src Port: 49705, Dst Port: 80, Seq: 1, Ack: 1, Len: 100
v 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: 13]
```

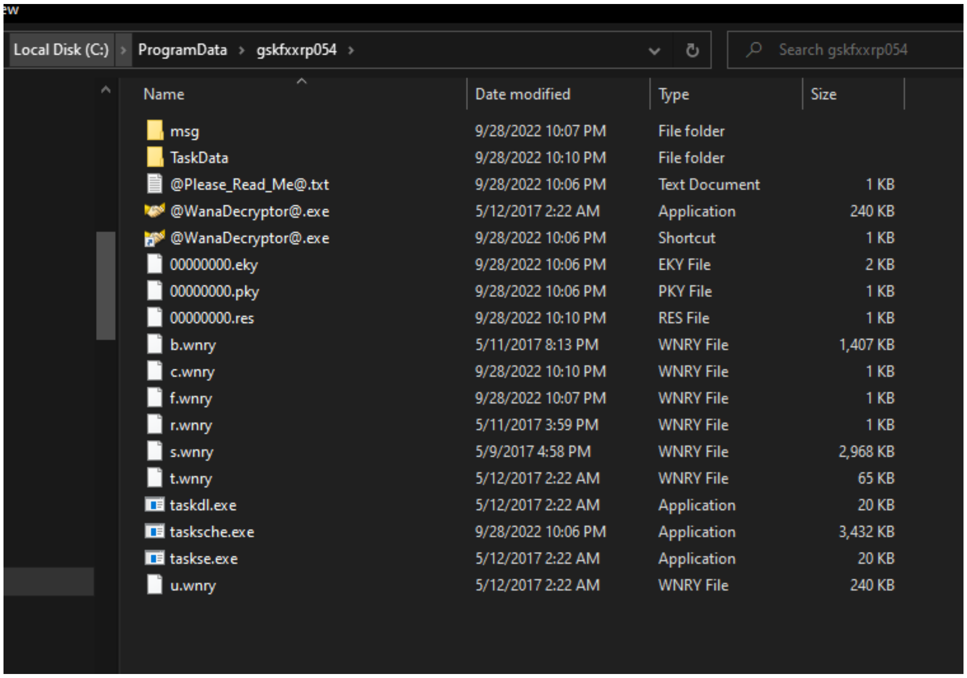
Fig -21 - Initial Connection to kill switch Url



services.exe	604	TCP	Listen	0.0.0.0	49669	0.0.0.0	0	9/28/2022 9:43:03 PM	services.exe
svchost.exe	1976	TCP	Listen	0.0.0.0	49670	0.0.0.0	0	9/28/2022 9:43:07 PM	PolicyAgent
Ransomware.wannacr...	52	TCP	Syn Sent	169.254.100.188	49714	169.254.29.1	445	9/28/2022 9:45:25 PM	mssecsvc2.0
Ransomware.wannacr...	52	TCP	Syn Sent	169.254.100.188	49715	169.254.30.1	445	9/28/2022 9:45:25 PM	mssecsvc2.0
Ransomware.wannacr...	52	TCP	Syn Sent	169.254.100.188	49716	169.254.31.1	445	9/28/2022 9:45:25 PM	mssecsvc2.0
Ransomware.wannacr...	52	TCP	Syn Sent	169.254.100.188	49717	169.254.32.1	445	9/28/2022 9:45:25 PM	mssecsvc2.0
Ransomware.wannacr...	52	TCP	Syn Sent	169.254.100.188	49719	169.254.33.1	445	9/28/2022 9:45:25 PM	mssecsvc2.0
Ransomware.wannacr...	52	TCP	Syn Sent	169.254.100.188	49720	169.254.34.1	445	9/28/2022 9:45:26 PM	mssecsvc2.0
Ransomware.wannacr...	52	TCP	Syn Sent	169.254.100.188	49722	169.254.35.1	445	9/28/2022 9:45:26 PM	mssecsvc2.0
Ransomware.wannacr...	52	TCP	Syn Sent	169.254.100.188	49723	169.254.36.1	445	9/28/2022 9:45:26 PM	mssecsvc2.0
Ransomware.wannacr...	52	TCP	Syn Sent	169.254.100.188	49724	169.254.37.1	445	9/28/2022 9:45:26 PM	mssecsvc2.0
System	4	TCP	Listen	0.0.0.0	445	0.0.0.0	0	9/28/2022 9:43:01 PM	System
System	4	TCP	Listen	0.0.0.0	5357	0.0.0.0	0	9/28/2022 9:43:07 PM	System

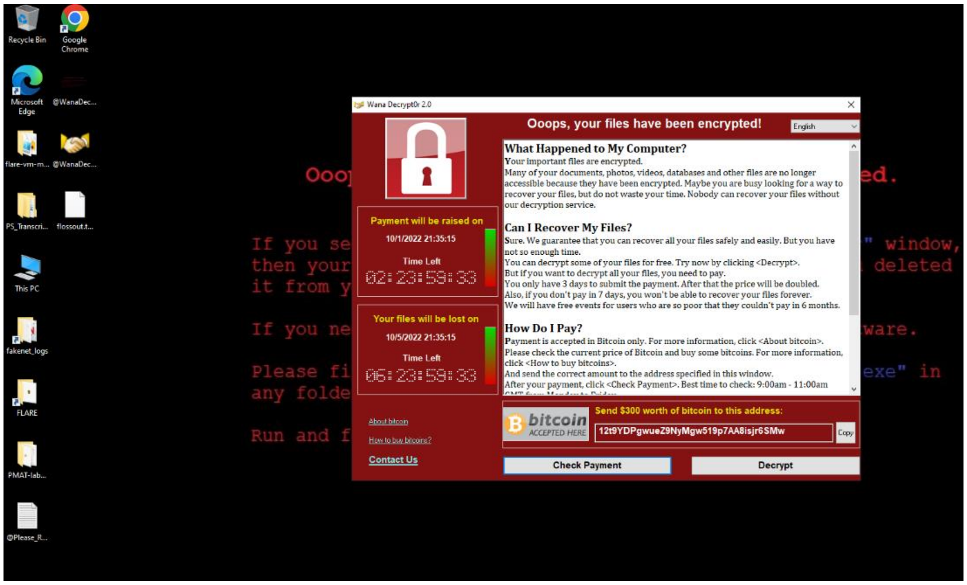
Fig - 22- Locating other machine and exploiting SMB on port 445

Host-based Indicators



Name	Date modified	Type	Size
msg	9/28/2022 10:07 PM	File folder	
TaskData	9/28/2022 10:10 PM	File folder	
@Please_Read_Me@.txt	9/28/2022 10:06 PM	Text Document	1 KB
@WanaDecryptor@.exe	5/12/2017 2:22 AM	Application	240 KB
@WanaDecryptor@.exe	9/28/2022 10:06 PM	Shortcut	1 KB
00000000.eky	9/28/2022 10:06 PM	EKY File	2 KB
00000000.pky	9/28/2022 10:06 PM	PKY File	1 KB
00000000.res	9/28/2022 10:10 PM	RES File	1 KB
b.wnry	5/11/2017 8:13 PM	WNRY File	1,407 KB
c.wnry	9/28/2022 10:10 PM	WNRY File	1 KB
f.wnry	9/28/2022 10:07 PM	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	9/28/2022 10:06 PM	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

Fig-23 - New Folder Created with random name



Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
10/1/2022 21:35:15
Time Left
02:23:59:33

Your files will be lost on
10/5/2022 21:35:15
Time Left
06:23:59:33

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

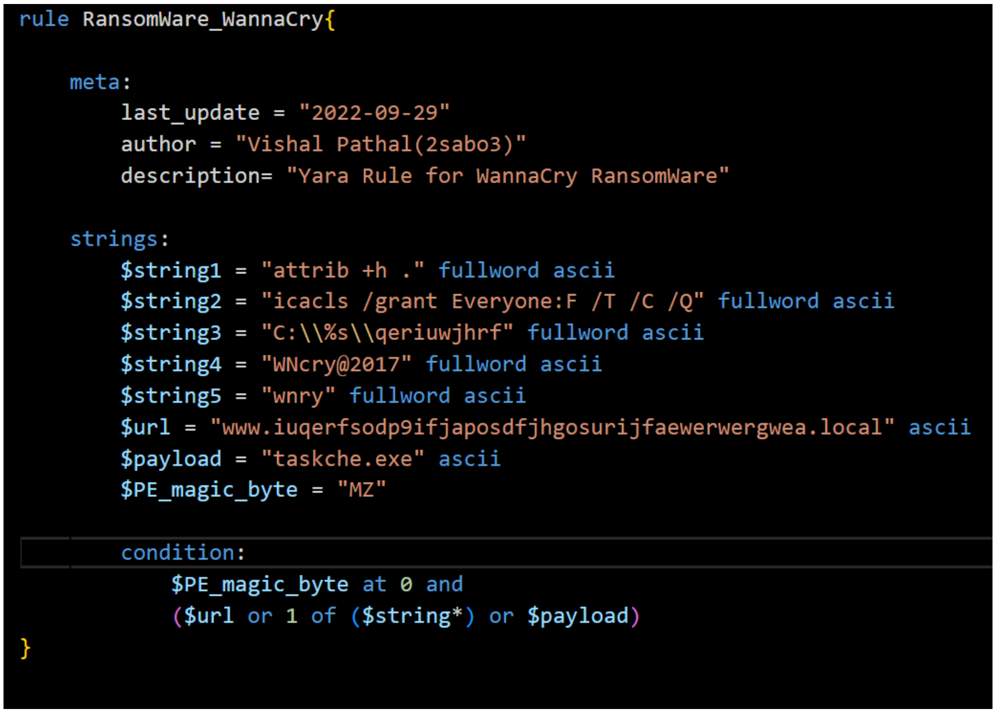
Fig- 24- Payment Screen, wannadecrpytor and desktop background changed.

Rules & Signatures

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

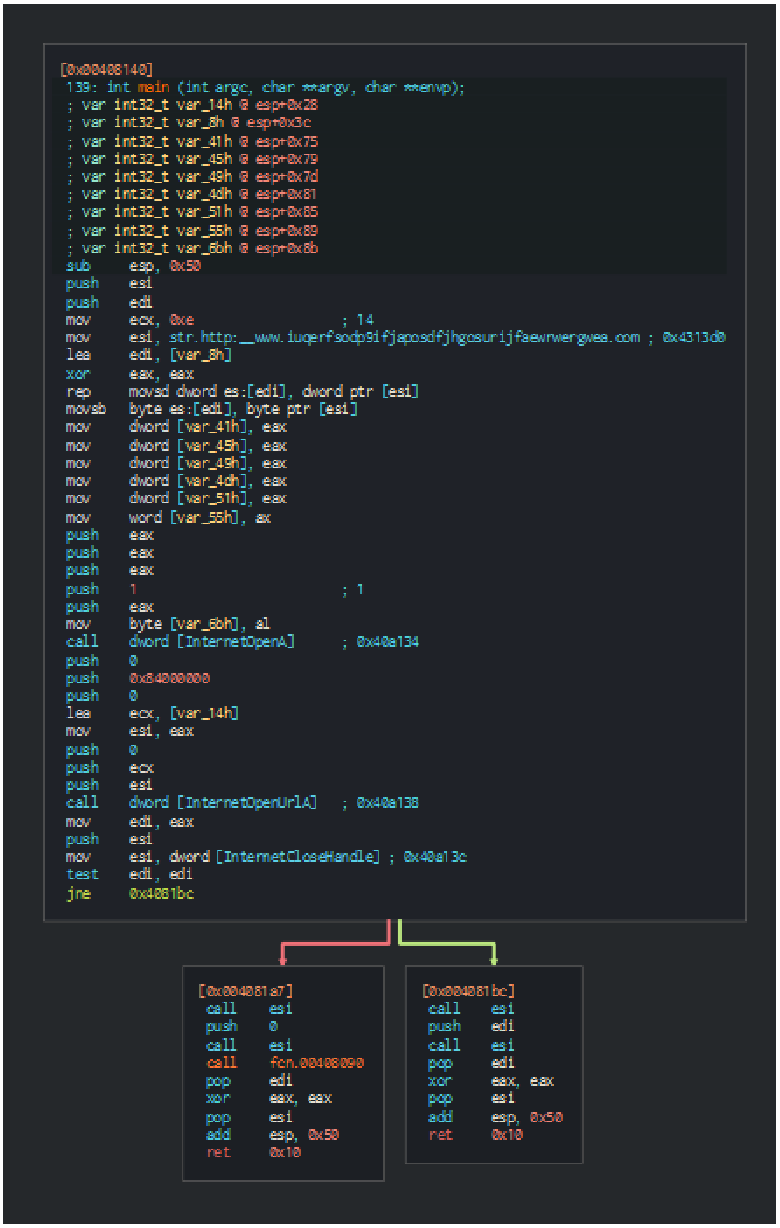
Appendices

A. Yara Rules



```
rule RansomWare_WannaCry{

    meta:
        last_update = "2022-09-29"
        author = "Vishal Pathal(2sabo3)"
        description= "Yara Rule for WannaCry RansomWare"

    strings:
        $string1 = "attrib +h ." fullword ascii
        $string2 = "icacls /grant Everyone:F /T /C /Q" fullword ascii
        $string3 = "C:\\%s\\qeriuwjhrf" fullword ascii
        $string4 = "WNcry@2017" fullword ascii
        $string5 = "wnry" fullword ascii
        $url = "www.iuqerfsodp9ifjaposdfjhgosurijfaewerwergwea.local" ascii
        $payload = "taskche.exe" ascii
        $PE_magic_byte = "MZ"

        condition:
            $PE_magic_byte at 0 and
            ($url or 1 of ($string*) or $payload)
}
```

B. Decompiled Code Snippets



```
[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     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
```

```
[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
```