VZSECURE

MALWARE ANALYSIS

WANNACRY

JAN 2023 | VZSECURE

Content:

1. Execution Summary

When any user tries to download the file and tries to run in his local machine then in backend the virus executes and encrypt all the files present in the system. It also changes the wallpaper of the machine and pop-up small window for paying ransom to attacker. When we try to access the content of the file, it was completely encrypted format.

So, without wasting time let analyze the virus and show you what happening in the backend of the virus execution.

2. Getting Hashes

Getting the hash is important part of static analysis. With the help of the hash, we can get the hint that what the virus is suppose to do in real case scenario.

We will use floss to get the hash of the executable program. We will need either MD5 or SHA256 hash.

SHA256: 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c

MD5: db349b97c37d22f5ea1d1841e3c89eb4

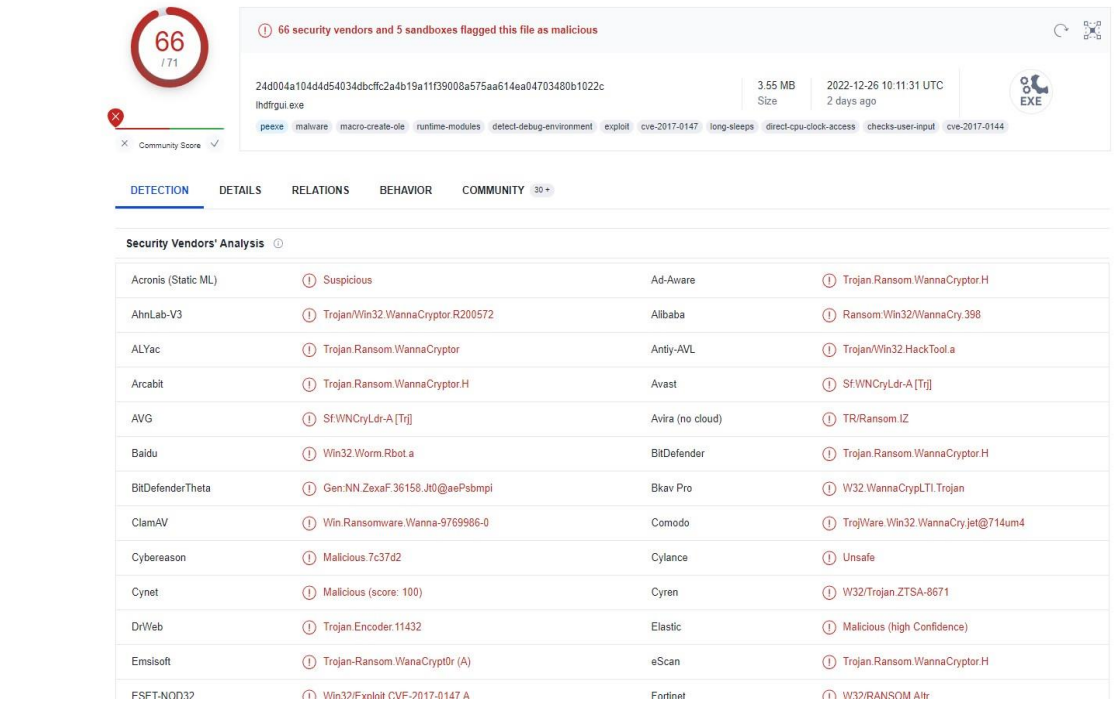
```
C:\Users\hacker\Desktop
λ sha256sum.exe Ransomware.wannacry.exe.malz
24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c *Ransomware.wannacry.exe.malz

C:\Users\hacker\Desktop
λ md5sum.exe Ransomware.wannacry.exe.malz
db349b97c37d22f5ea1d1841e3c89eb4 *Ransomware.wannacry.exe.malz
```

3. Analyzing Hash

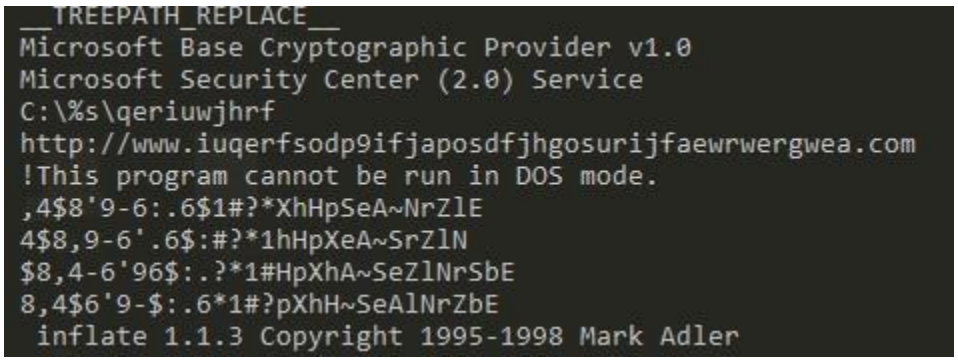
After getting the hash we need to check that hash. So, we will take the help of virus total which will check if the hash matches any virus which was happens in past real case scenario. Then virus total has over 70 antivirus it will analyze the hash through antivirus and give us the result.

We can see that over 66 antiviruses have detected the hash for malicious.



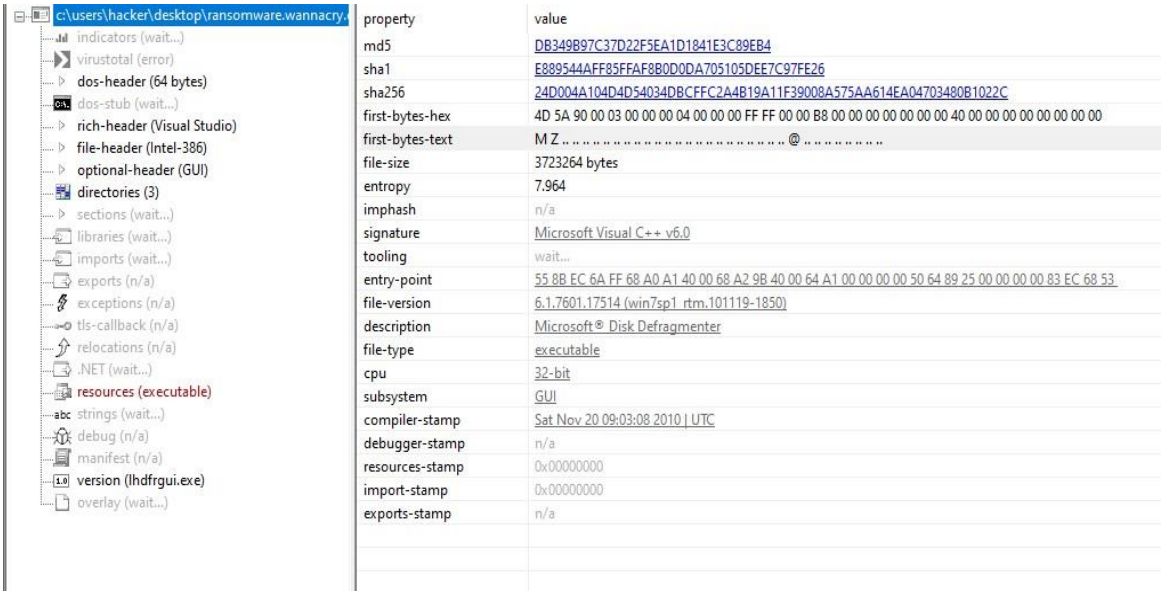
4. Static Analysis

Here the Static analysis begins, we will now analyze the malware without running the malware. So, we will use some kind of tool for analysis which will be discuss below.
Now let analyze the malware with the help of strings, tries to find if we are able to get useful string.



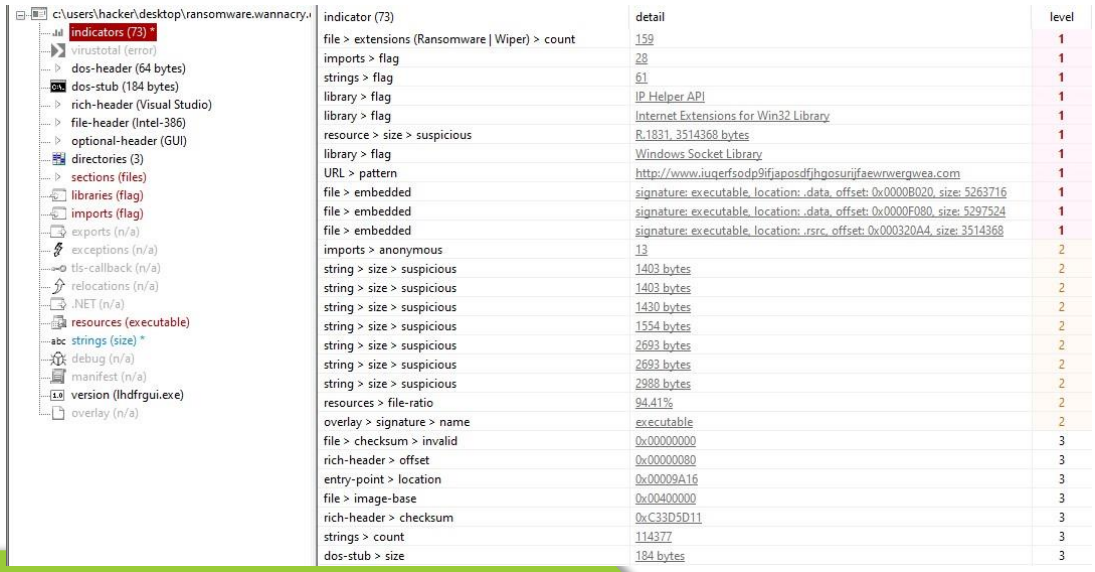
We have got some useful strings which is shown above image. We came to know that there is some file creation on [C://?/qeriuwjhrf], There is using of sting format which means it will get path from string format and create the file.
There is one unknown domain which we can see, the malware should use domain to fetch something from internet.

Let's take the help of one tool which is "PEVIEW" which is present in flareVM. After importing the program in tool se get lots of information. We will get same information as we get in floss and getting hash. But we also see what API call is present within the binary.



c:\users\hacker\desktop\ransomware.wannacry.
- indicators (wait...)
- virustotal (error)
- dos-header (64 bytes)
- dos-stub (wait...)
- rich-header (Visual Studio)
- file-header (Intel-386)
- optional-header (GUI)
- directories (3)
- sections (wait...)
- libraries (wait...)
- imports (wait...)
- exports (n/a)
- exceptions (n/a)
- tls-callback (n/a)
- relocations (n/a)
- .NET (wait...)
- resources (executable)
- strings (wait...)
- debug (n/a)
- manifest (n/a)
- version (lhdfrgui.exe)
- overlay (wait...)

property	value
md5	DB349B97C37D22F5EA1D1841E3C89EB4
sha1	E889544AFF85FFAF8B0D0DA705105DEE7C97FE26
sha256	24D004A104D4D54034DBCFFC2A4B19A11F39008A575AA614EA04703480B1022C
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
first-bytes-text	M Z . . . . . @ . . . . .
file-size	3723264 bytes
entropy	7.964
imphash	n/a
signature	Microsoft Visual C++ v6.0
tooling	wait...
entry-point	55 8B EC 6A FF 68 A0 A1 40 00 68 A2 9B 40 00 64 A1 00 00 00 00 50 64 89 25 00 00 00 00 83 EC 68 53
file-version	6.1.7601.17514 (win7sp1_rtm.101119-1850)
description	Microsoft® Disk Defragmenter
file-type	executable
cpu	32-bit
subsystem	GUI
compiler-stamp	Sat Nov 20 09:03:08 2010 | UTC
debugger-stamp	n/a
resources-stamp	0x00000000
import-stamp	0x00000000
exports-stamp	n/a



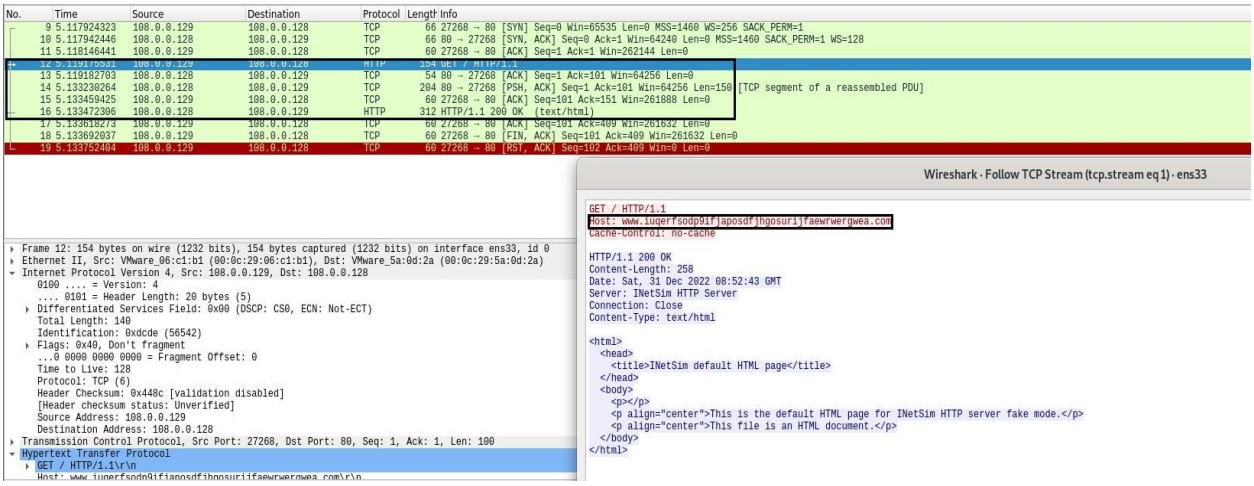
c:\users\hacker\desktop\ransomware.wannacry.
- indicators (73) *
- virustotal (error)
- dos-header (64 bytes)
- dos-stub (184 bytes)
- rich-header (Visual Studio)
- file-header (Intel-386)
- optional-header (GUI)
- directories (3)
- sections (files)
- libraries (flag)
- imports (flag)
- exports (n/a)
- exceptions (n/a)
- tls-callback (n/a)
- relocations (n/a)
- .NET (n/a)
- resources (executable)
- strings (size) *
- debug (n/a)
- manifest (n/a)
- version (lhdfrgui.exe)
- overlay (n/a)

indicator (73)	detail	level
file > extensions (Ransomware | Wiper) > count	159	1
imports > flag	28	1
strings > flag	61	1
library > flag	IP Helper API	1
library > flag	Internet Extensions for Win32 Library	1
resource > size > suspicious	R,1831, 3514368 bytes	1
library > flag	Windows Socket Library	1
URL > pattern	http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com	1
file > embedded	signature: executable, location: .data, offset: 0x0000B020, size: 5263716	1
file > embedded	signature: executable, location: .data, offset: 0x0000F080, size: 5297524	1
file > embedded	signature: executable, location: .rsrc, offset: 0x000320A4, size: 3514368	1
imports > anonymous	13	2
string > size > suspicious	1403 bytes	2
string > size > suspicious	1403 bytes	2
string > size > suspicious	1430 bytes	2
string > size > suspicious	1554 bytes	2
string > size > suspicious	2693 bytes	2
string > size > suspicious	2693 bytes	2
string > size > suspicious	2988 bytes	2
resources > file-ratio	94.41%	2
overlay > signature > name	executable	2
file > checksum > invalid	0x00000000	3
rich-header > offset	0x00000080	3
entry-point > location	0x00009A16	3
file > image-base	0x00400000	3
rich-header > checksum	0xC33D5D11	3
strings > count	114377	3
dos-stub > size	184 bytes	3

5. Dynamic Analysis

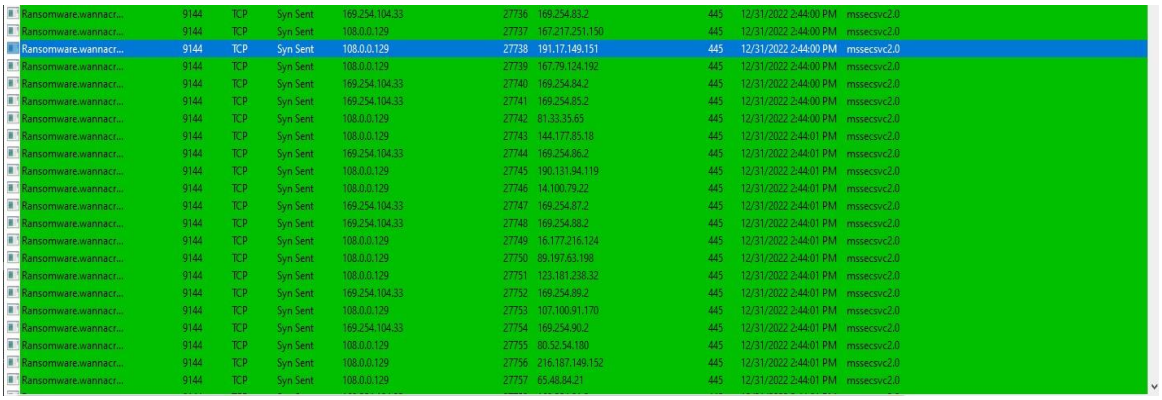
In this section we will cover about the dynamic analysis on binary and see what is actually happening behind the execution of the binary. We will run the malware in created Sandbox environment so that it will not pivot over the local network and analyze the malware working.

We will take help “Wireshark” and “Process-Monitor” tool which is pre-installed in FlareVM.



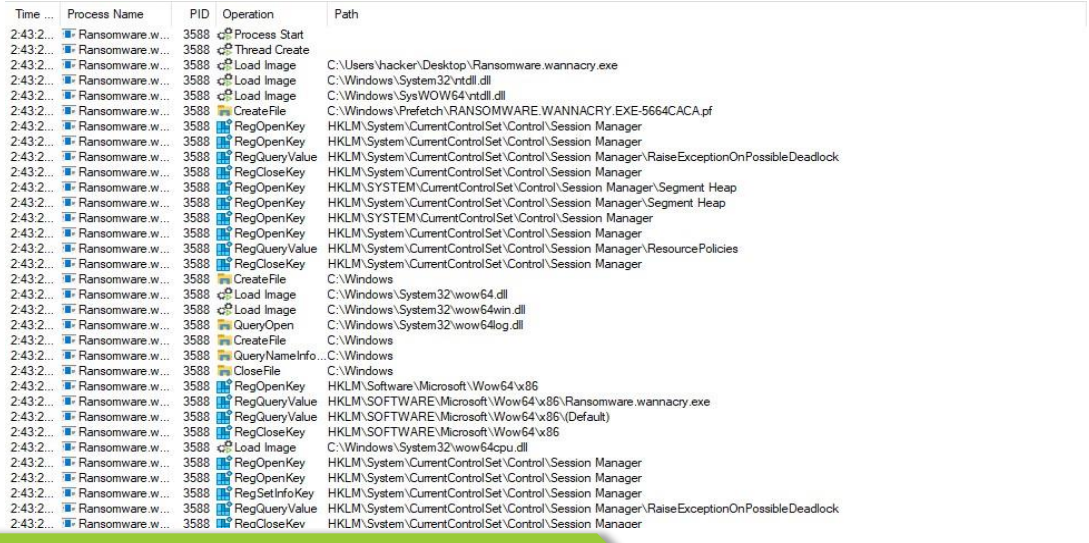
We can see that virus is reaching to the present domain but the virus is not harmed our system while it reaches to internet. Let’s check one more time without internet.

When execute the program without the internet connection it starts working in background and encrypt the system. First, I saw that in “TCPVIEW” it gives random remote IP address which tries to communicate, it means that this is not a real IP.



Ransomware.wannacr...	9144	TCP	Syn Sent	169.254.104.33	27736	169.254.83.2	445	12/31/2022 2:44:00 PM	mssecsvc2.0
Ransomware.wannacr...	9144	TCP	Syn Sent	108.0.0.129	27737	167.217.251.150	445	12/31/2022 2:44:00 PM	mssecsvc2.0
Ransomware.wannacr...	9144	TCP	Syn Sent	108.0.0.129	27738	191.17.149.151	445	12/31/2022 2:44:00 PM	mssecsvc2.0
Ransomware.wannacr...	9144	TCP	Syn Sent	108.0.0.129	27739	167.79.124.192	445	12/31/2022 2:44:00 PM	mssecsvc2.0
Ransomware.wannacr...	9144	TCP	Syn Sent	169.254.104.33	27740	169.254.84.2	445	12/31/2022 2:44:00 PM	mssecsvc2.0
Ransomware.wannacr...	9144	TCP	Syn Sent	169.254.104.33	27741	169.254.85.2	445	12/31/2022 2:44:00 PM	mssecsvc2.0
Ransomware.wannacr...	9144	TCP	Syn Sent	108.0.0.129	27742	81.33.35.65	445	12/31/2022 2:44:00 PM	mssecsvc2.0
Ransomware.wannacr...	9144	TCP	Syn Sent	108.0.0.129	27743	144.177.85.18	445	12/31/2022 2:44:01 PM	mssecsvc2.0
Ransomware.wannacr...	9144	TCP	Syn Sent	169.254.104.33	27744	169.254.86.2	445	12/31/2022 2:44:01 PM	mssecsvc2.0
Ransomware.wannacr...	9144	TCP	Syn Sent	108.0.0.129	27745	190.131.94.119	445	12/31/2022 2:44:01 PM	mssecsvc2.0
Ransomware.wannacr...	9144	TCP	Syn Sent	108.0.0.129	27746	14.100.79.22	445	12/31/2022 2:44:01 PM	mssecsvc2.0
Ransomware.wannacr...	9144	TCP	Syn Sent	169.254.104.33	27747	169.254.87.2	445	12/31/2022 2:44:01 PM	mssecsvc2.0
Ransomware.wannacr...	9144	TCP	Syn Sent	169.254.104.33	27748	169.254.88.2	445	12/31/2022 2:44:01 PM	mssecsvc2.0
Ransomware.wannacr...	9144	TCP	Syn Sent	108.0.0.129	27749	16.177.216.124	445	12/31/2022 2:44:01 PM	mssecsvc2.0
Ransomware.wannacr...	9144	TCP	Syn Sent	108.0.0.129	27750	89.197.63.198	445	12/31/2022 2:44:01 PM	mssecsvc2.0
Ransomware.wannacr...	9144	TCP	Syn Sent	108.0.0.129	27751	123.181.238.32	445	12/31/2022 2:44:01 PM	mssecsvc2.0
Ransomware.wannacr...	9144	TCP	Syn Sent	169.254.104.33	27752	169.254.89.2	445	12/31/2022 2:44:01 PM	mssecsvc2.0
Ransomware.wannacr...	9144	TCP	Syn Sent	108.0.0.129	27753	107.100.91.170	445	12/31/2022 2:44:01 PM	mssecsvc2.0
Ransomware.wannacr...	9144	TCP	Syn Sent	169.254.104.33	27754	169.254.90.2	445	12/31/2022 2:44:01 PM	mssecsvc2.0
Ransomware.wannacr...	9144	TCP	Syn Sent	108.0.0.129	27755	80.52.54.180	445	12/31/2022 2:44:01 PM	mssecsvc2.0
Ransomware.wannacr...	9144	TCP	Syn Sent	108.0.0.129	27756	216.187.149.152	445	12/31/2022 2:44:01 PM	mssecsvc2.0
Ransomware.wannacr...	9144	TCP	Syn Sent	108.0.0.129	27757	65.48.84.21	445	12/31/2022 2:44:01 PM	mssecsvc2.0

In “Procmon” we are able to see that there is lot of files and registry operation are carried on in background on execution.



Time ...	Process Name	PID	Operation	Path
2:43:2...	Ransomware.w...	3588	Process Start	
2:43:2...	Ransomware.w...	3588	Thread Create	
2:43:2...	Ransomware.w...	3588	Load Image	C:\Users\hacker\Desktop\Ransomware.wannacry.exe
2:43:2...	Ransomware.w...	3588	Load Image	C:\Windows\System32\ntdll.dll
2:43:2...	Ransomware.w...	3588	Load Image	C:\Windows\SysWOW64\ntdll.dll
2:43:2...	Ransomware.w...	3588	CreateFile	C:\Windows\Prefetch\RANSOMWARE.WANNACRY.EXE-5664CACA.pf
2:43:2...	Ransomware.w...	3588	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager
2:43:2...	Ransomware.w...	3588	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager
2:43:2...	Ransomware.w...	3588	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\RaiseExceptionOnPossibleDeadlock
2:43:2...	Ransomware.w...	3588	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager
2:43:2...	Ransomware.w...	3588	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Segment Heap
2:43:2...	Ransomware.w...	3588	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\Segment Heap
2:43:2...	Ransomware.w...	3588	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager
2:43:2...	Ransomware.w...	3588	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager
2:43:2...	Ransomware.w...	3588	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies
2:43:2...	Ransomware.w...	3588	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager
2:43:2...	Ransomware.w...	3588	CreateFile	C:\Windows
2:43:2...	Ransomware.w...	3588	Load Image	C:\Windows\System32\wow64.dll
2:43:2...	Ransomware.w...	3588	Load Image	C:\Windows\System32\wow64win.dll
2:43:2...	Ransomware.w...	3588	QueryOpen	C:\Windows\System32\wow64log.dll
2:43:2...	Ransomware.w...	3588	CreateFile	C:\Windows
2:43:2...	Ransomware.w...	3588	QueryNameInfo...	C:\Windows
2:43:2...	Ransomware.w...	3588	CloseFile	C:\Windows
2:43:2...	Ransomware.w...	3588	RegOpenKey	HKLM\Software\Microsoft\Wow64\x86
2:43:2...	Ransomware.w...	3588	RegQueryValue	HKLM\SOFTWARE\Microsoft\Wow64\x86\Ransomware.wannacry.exe
2:43:2...	Ransomware.w...	3588	RegQueryValue	HKLM\SOFTWARE\Microsoft\Wow64\x86\(Default)
2:43:2...	Ransomware.w...	3588	RegCloseKey	HKLM\SOFTWARE\Microsoft\Wow64\x86
2:43:2...	Ransomware.w...	3588	Load Image	C:\Windows\System32\wow64cpu.dll
2:43:2...	Ransomware.w...	3588	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager
2:43:2...	Ransomware.w...	3588	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager
2:43:2...	Ransomware.w...	3588	RegSetInfoKey	HKLM\System\CurrentControlSet\Control\Session Manager
2:43:2...	Ransomware.w...	3588	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\RaiseExceptionOnPossibleDeadlock
2:43:2...	Ransomware.w...	3588	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager

6. Overview of Basic Analysis

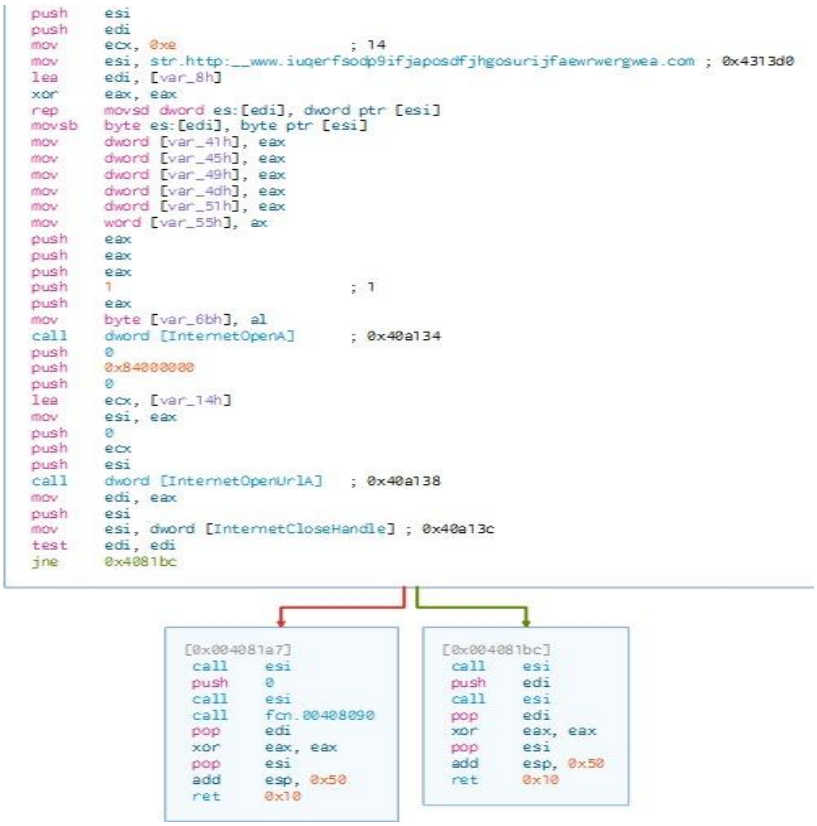
1. **Internet connection Enable**:
   a. When we execute the program while internet connection is enabled it tries to reach the domain.
   b. The malware didn't work, our all files were safe.
2. **Internet connection Disable**:
   a. When we execute the program, we able to see random IP which is trying to communicate with remote server.
   b. It creates file and registry operation.
   c. It encrypts all the content of the file and small pop-up is reflected in screen.

7. Advance Static Analysis

In this section we will analyze the code compares to basic static analysis but this time will analyze the assembly language of the binary. We need to know about machine level instruction to analyze the malware.

We will take help of cutter tool and know what it supposed to do.

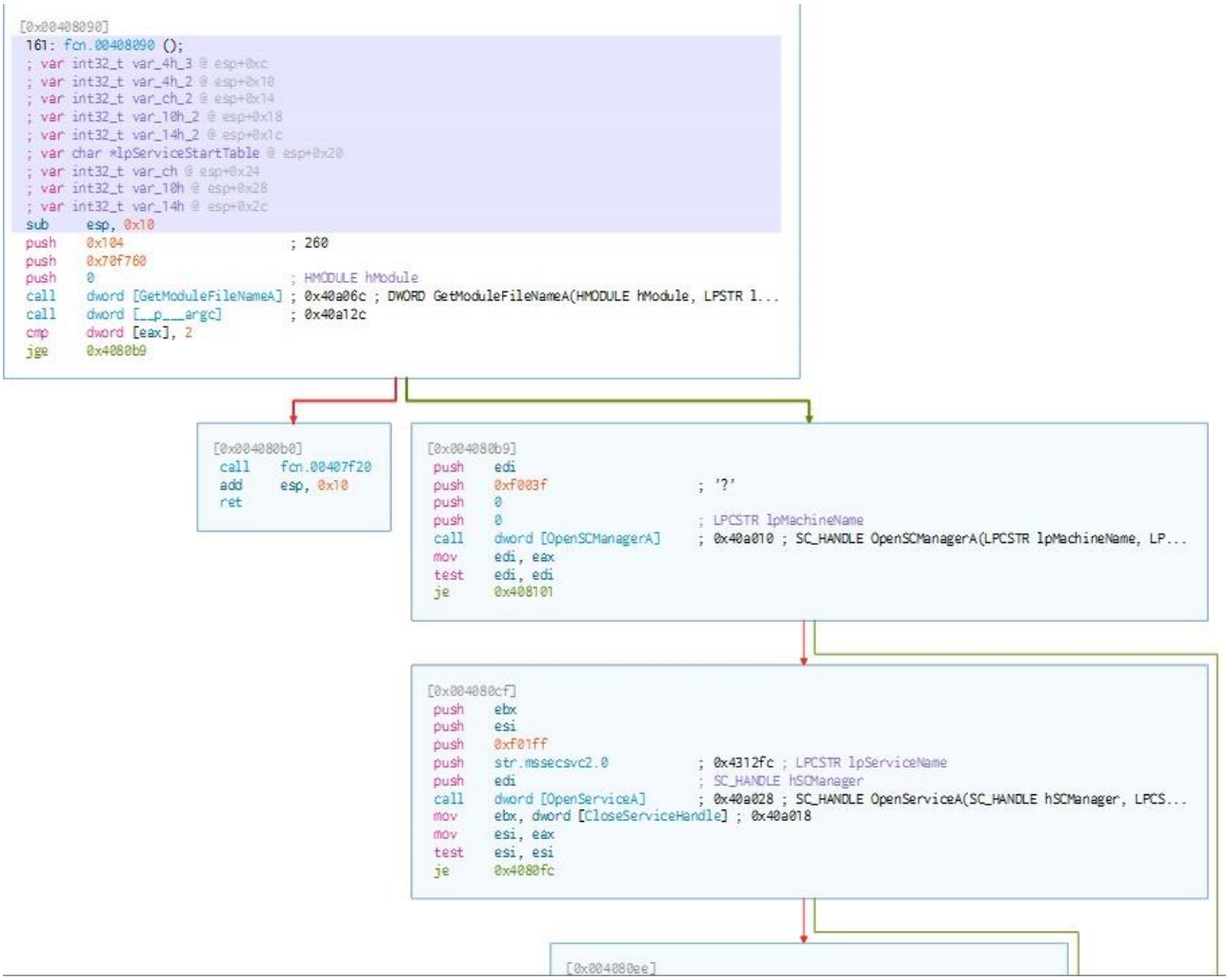
In Image we can see that the API call is make when we execute the program. The domain address is stored in the ESI and afterward the ESI instruction is passed in the “InternetOpenUrlA” API call.



We can see that as the binary connects to internet it will immediately close the connection via “InternetCloseHandle” API call and does not harm the machine.

We can see “jne (jump if not equal to zero)” instruction which perform some condition. It checks the binary is able to communicate over the internet. If yes then it will return true (1) and exit binary or else it will return False (0) and continue.

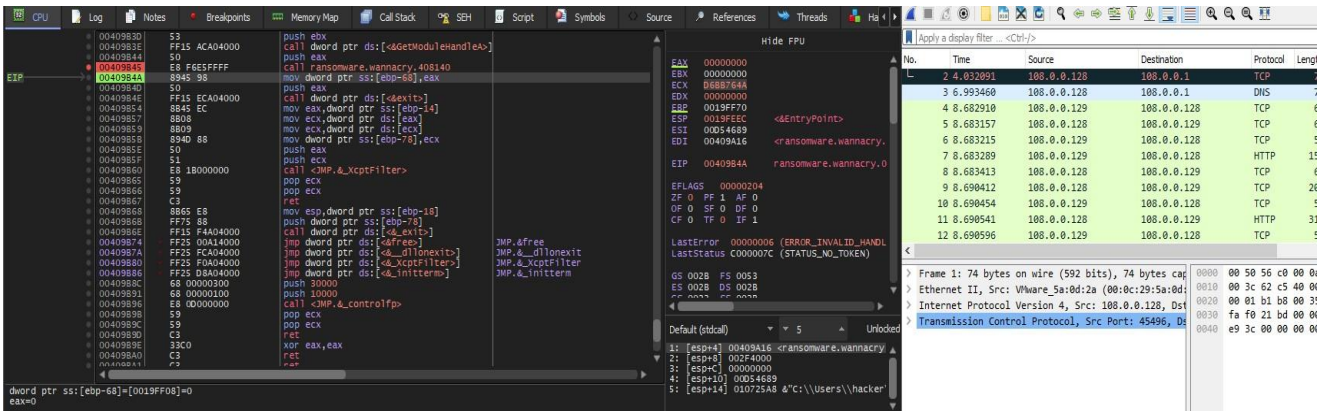
What if there is not internet connection? So, that time while condition checking it will return False as it not reaches to domain. There is function call within the condition, which take to address (0x00408090). Here program executes and encrypt all files present in the system.



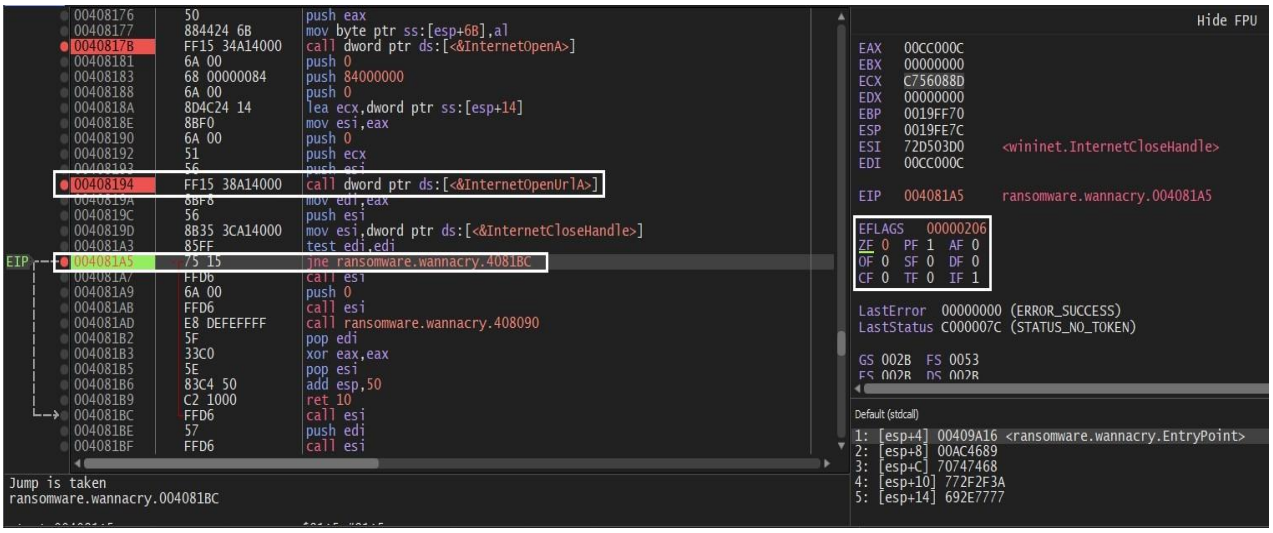
8. Advance Dynamic Analysis

In this section the analysis will be same as Static but this time we will run the binary in debugger and control the binary. As we understand the static analysis, we are able to control the flow of binary.

For these we will take help of any debugger and control the flow of program

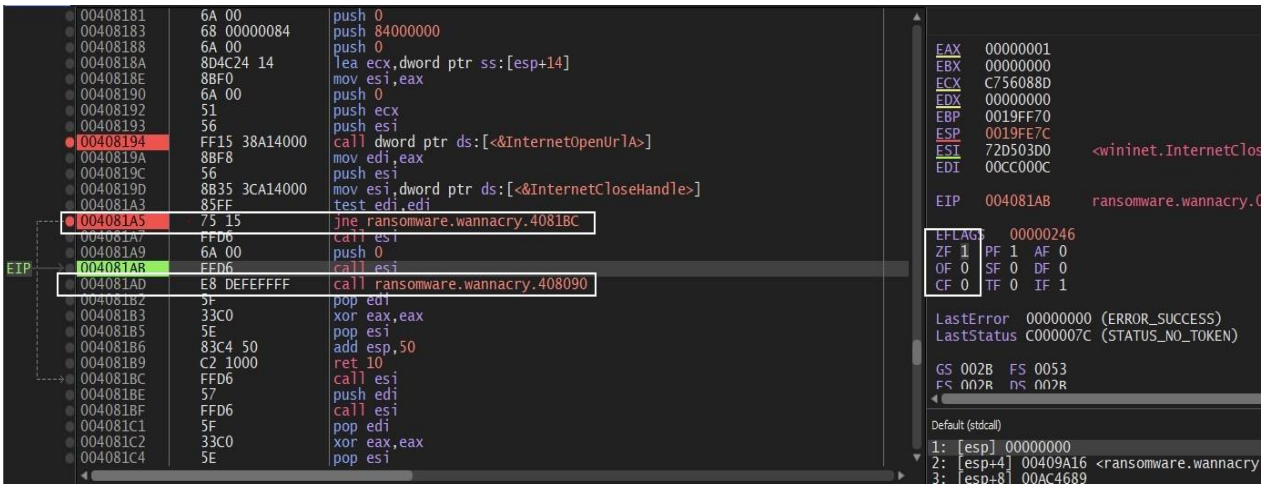


I have setup the breakpoint where the internet communication is to be done. When we move one step forward of that instruction, we are able to get HTTP response in Wireshark. Let take a look at the breakpoint call.



When it hit the second breakpoint in above image it will tries to communicate over internet and goes further jump instruction. The jump instruction checks the condition we can see in right section of image the “ZF (Zero Flag)” its value will be 1 if the condition value is 0 or else it will be 0. As in image it is 0 so “JNE” will goes to arrow pointed toward another call.

What If we try to control the jump instruction? As we have full control of binary which is running in debugger. Let’s try it.



In above image I have set the Zero Flag to 1 in which the condition will have value 0 and it will execute further. The binary will execute the function call and start causing harm to machine and we are able to see pop-up window of WannaCry Malware.

Hope so you get deep understanding for working of the malware.

9. Yara Rules

Yara rules classify and identify malware samples by creating descriptions of malware families based on textual or binary patterns. We can use Yara rules to define text or binary patterns that will match a file or component of a file to quickly find malicious files.

```
rule WannaCry_Malware {
    meta:
        lastest_update = "01-01-2023"
        author = "VZsecure"
        description = "Analyze the wannacry malware, save your system from such attacks."
    strings:
        $Domain_call = "http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.comYOUARETHEMANNOWDOG" ascii
        $Command_exec = "cmd.exe" ascii
        $magic_byte = "MZ"
        $File_Create = "tasksche.exe" ascii

    condition:
        $magic_byte at 0 and
        $Domain_call or
        $Command_exec or
        $File_Create
}
```

Thank You!