

# Practical Malware Analysis & Triage

## Malware Analysis Report

WannaCry Ransomware  
Course-Final



# Table of Contents

<b>Table of Contents.....</b>	<b>2</b>
<b>Executive Summary.....</b>	<b>3</b>
<b>High-Level Technical Summary.....</b>	<b>4</b>
<b>Malware Composition.....</b>	<b>6</b>
<b>Basic Static Analysis.....</b>	<b>7</b>
<b>Basic Dynamic Analysis.....</b>	<b>10</b>
<b>Advanced Static Analysis.....</b>	<b>13</b>
<b>Advanced Dynamic Analysis.....</b>	<b>14</b>
<b>Indicators of Compromise.....</b>	<b>16</b>
Network Indicators.....	16
Host-based Indicators.....	17
<b>Rules &amp; Signatures.....</b>	<b>18</b>
<b>Appendices.....</b>	<b>19</b>
A. Yara Rules.....	19
B. Callback URLs.....	20
C. Decompiled Code Snippets.....	20



## Executive Summary

SHA256 hash	24d004a104d4d54034dbccfc2a4b19a11f39008a575aa614ea04703480b1022c
-------------	--

WannaCry is ransomware that struck in May 2017, exploiting a Microsoft SMB vulnerability (EternalBlue) to spread rapidly across networks. It encrypted files and demanded Bitcoin ransom for decryption. Industries like healthcare and finance were hit hard.

The binary is a standalone executable that will first check for connectivity to an external URL that is embedded into it. If a connection is established nothing happens, but when the binary is not able to connect to the hard-coded URL it starts its malicious activity.

Dumps a bunch of malicious scripts and then it starts encrypting each and every single user,system file present in the machine. After which we get the ransom demand screen and instructions to carry out to decrypt the files.

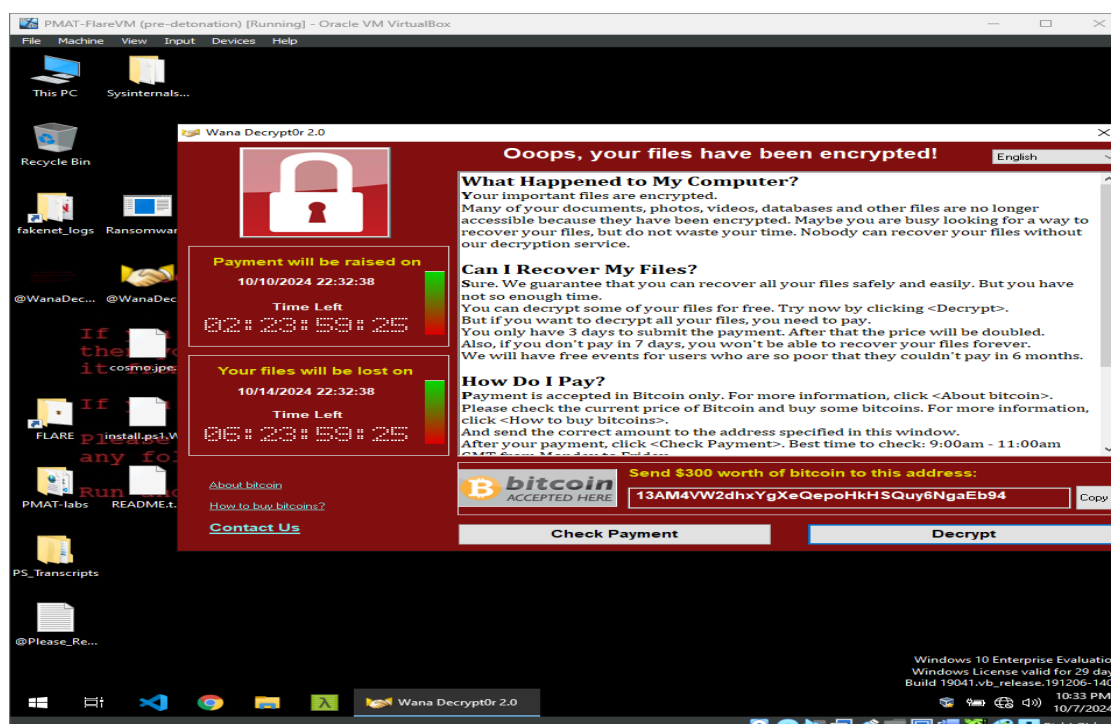


Fig1: WannaCry Ransomware



## High-Level Technical Summary

The WannaCry ransomware is a standalone malware binary that, when executed, will encrypt all system and user files on the machine, lock the system, and demand a ransom payment, without which the decryption key will not be provided.

The roots of WannaCry arise from an SMB vulnerability present on Windows systems called EternalBlue. EternalBlue exploits a buffer overflow vulnerability in the SMBv1 (Server Message Block) protocol (CVE-2017-0144).

In the context of WannaCry, EternalBlue was used to propagate the ransomware across networks. Once a machine was compromised, WannaCry injected its payload, encrypted files, and spread laterally to other unpatched machines by exploiting the same SMB vulnerability, without requiring user interaction.

Initially after detonation the malware gets the system prepared to make a internet connection to an external URL (**URL[defanged]: *hxxp://[www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com***). If the URL is reachable the malware just closes the connection.

In other cases, the malware starts calling out sub-functions inside of it and starts encrypting the system and user files. After encryption there is a pop-up box that demands for ransom payment in Bitcoins. Post which the victim is provided with a decryption key to decrypt their files.

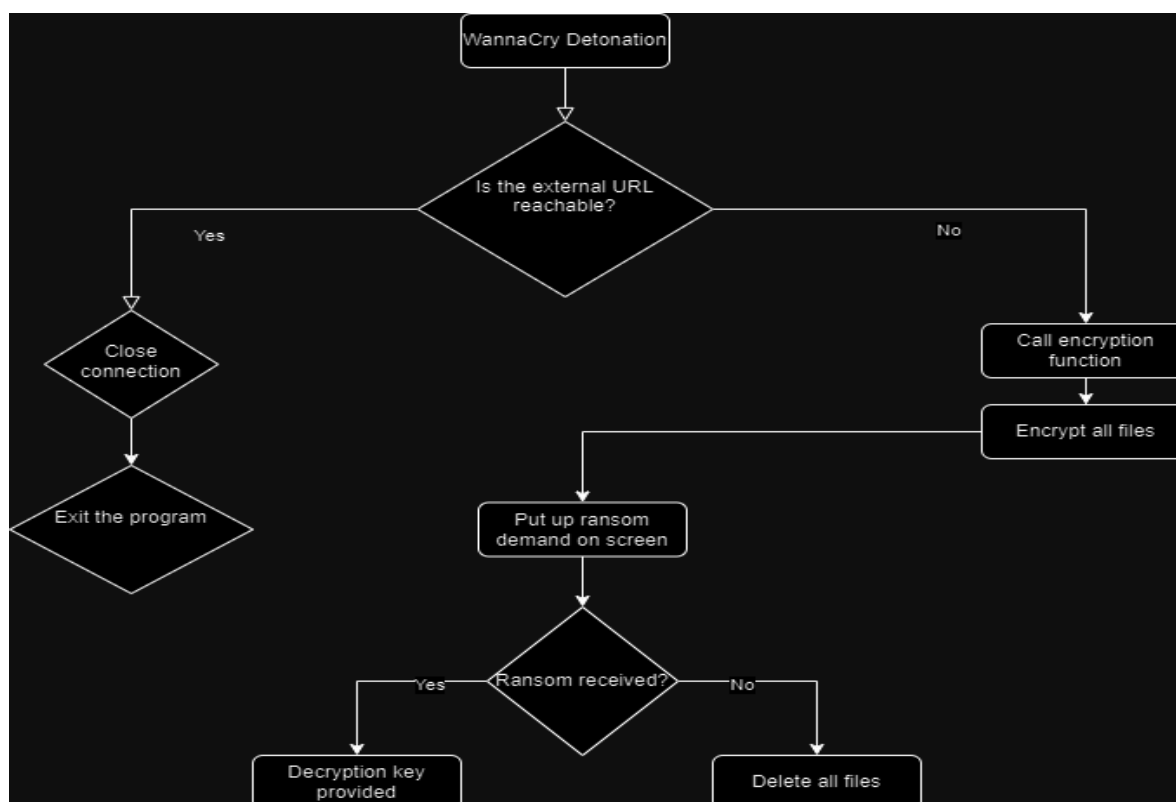


Fig2: Basic Workflow of WannaCry



## Malware Composition

WannaCry consists of the following components:

File Name	SHA256 Hash
<b>Ransomware. wannacry.exe</b>	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c

This malware has a very basic composition. The malware is standalone meaning all of its functionality is packaged into a single binary rather than downloading and executing a second stage.

Though there are some processes that the binary spawns off during its execution. Details of which can be found later in the report.



## Basic Static Analysis

Here are my observations for the binary:

```
flossout.txt
File Edit View
__set_app_type
__controlfp
MSVCP60.dll
GetStartupInfoA
advapi32.dll
WANACRY!
CloseHandle
DeleteFileW
MoveFileExW
MoveFileW
ReadFile
WriteFile
CreateFileW
kernel32.dll
0|x8+^
2/O_..X8w.+
|~}%15
Microsoft Enhanced RSA and AES Cryptographic Provider
CryptGenKey
CryptDecrypt
CryptEncrypt
CryptDestroyKey
CryptImportKey
CryptAcquireContextA
cmd.exe /c "%s"
115p7UMMngo1pMvkpHjicRdfJNXj6LrLn
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
13AM4Vw2dhxYgXeQepoHkHSQuy6NgaEb94
Global\MSWinZonesCacheCounterMutexA
tasksche.exe
TaskStart
icaccls . /grant Everyone:F /T /C /Q
attrib +h
WNcry@2o17
GetNativeSystemInfo
.?AVException@@
incompatible version
buffer error
insufficient memory
data error
stream error
file error
stream end
need dictionary
invalid distance code
invalid literal/length code
invalid bit length repeat
too many length or distance symbols
invalid stored block lengths
```

Fig3: Floss output from the binary

The strings highlighted in the image raise an eyebrow, as the function calls printed out seem to perform some kind of cryptographic function. Adding to this a similar set of strings were found while analyzing the binary in PEvent.



File View Go Help				
Ransomware wannacry.exe.malz				
IMAGE_DOS_HEADER	0000A000	0000A0F6	Hint/Name RVA	024A StartServiceCtrlDispatcherA
MS-DOS Stub Program	0000A004	0000A0D8	Hint/Name RVA	020C RegisterServiceCtrlHandlerA
IMAGE_IMPORT_HEADERS	0000A008	0000A0C0	Hint/Name RVA	0034 ChangeServiceConfig2A
IMAGE_SECTION_HEADER .text	0000A00C	0000A0AC	Hint/Name RVA	0244 SetServiceStatus
IMAGE_SECTION_HEADER .idata	0000A010	0000A09A	Hint/Name RVA	01AD OpenSCManagerA
IMAGE_SECTION_HEADER .data	0000A014	0000A088	Hint/Name RVA	0064 CreateServiceA
IMAGE_SECTION_HEADER .rsrc	0000A018	0000A072	Hint/Name RVA	003E CloseServiceHandle
SECTION .text	0000A01C	0000A062	Hint/Name RVA	0249 StartServiceA
SECTION .idata	0000A020	0000A050	Hint/Name RVA	0096 CryptGenRandom
IMPORT Address Table	0000A024	0000A038	Hint/Name RVA	0085 CryptAcquireContextA
IMPORT Directory Table	0000A028	0000A714	Hint/Name RVA	01AF OpenServiceA
IMPORT Name Table	0000A02C	00000000	End of Imports	ADVAPI32.dll
IMPORT Hints/Names & DLL Names	0000A030	0000A0F6	Hint/Name RVA	0390 WaitForSingleObject
SECTION .data	0000A034	0000A0C0	Hint/Name RVA	022C InterlockedIncrement
SECTION .rsrc	0000A038	0000A024	Hint/Name RVA	0146 GetCurrentThreadId
	0000A03C	0000A03A	Hint/Name RVA	0145 GetCurrentThread
	0000A040	0000A04E	Hint/Name RVA	02B5 ReadFile
	0000A044	0000A05A	Hint/Name RVA	0163 GetFileSize
	0000A048	0000A068	Hint/Name RVA	0053 CreateFileA
	0000A04C	0000A076	Hint/Name RVA	026F MoveFileExA
	0000A050	0000A084	Hint/Name RVA	0355 SizedResource
	0000A054	0000A0E4	Hint/Name RVA	035F TerminateThread
	0000A058	0000A0A6	Hint/Name RVA	0257 LoadResource
	0000A05C	0000A0B6	Hint/Name RVA	00E3 FindResourceA
	0000A060	0000A0C6	Hint/Name RVA	01A0 GetProcAddress
	0000A064	0000A0D8	Hint/Name RVA	0182 GetModuleHandleW
	0000A068	0000A0EC	Hint/Name RVA	00B9 ExitProcess
	0000A06C	0000A0FA	Hint/Name RVA	017D GetModuleFileNameA
	0000A070	0000A010	Hint/Name RVA	025C LocalFree
	0000A074	0000A01C	Hint/Name RVA	0258 LocalAlloc
	0000A078	0000A0D6	Hint/Name RVA	0034 CloseHandle
	0000A07C	0000A0BE	Hint/Name RVA	0228 InterlockedDecrement
	0000A080	0000A0A6	Hint/Name RVA	0098 EnterCriticalSection
	0000A084	0000A08E	Hint/Name RVA	0251 LeaveCriticalSection
	0000A088	0000A072	Hint/Name RVA	0223 InitializeCriticalSection
	0000A08C	0000A064	Hint/Name RVA	01F8 GlobalAlloc
	0000A090	0000A056	Hint/Name RVA	01EF GlobalFree
	0000A094	0000A03A	Hint/Name RVA	0244 QueryPerformanceFrequency
	0000A098	0000A020	Hint/Name RVA	02A3 QueryPerformanceCounter
	0000A09C	0000A010	Hint/Name RVA	01D0 GetTickCount
	0000A0A0	0000A096	Hint/Name RVA	0265 LockResource
	0000A0A4	0000A008	Hint/Name RVA	0356 Sleep
	0000A0A8	0000A07A	Hint/Name RVA	01B7 GetStartupInfoA
	0000A0AC	0000A066	Hint/Name RVA	017F GetModuleHandleA
	0000A0B0	00000000	End of Imports	KERNEL32.dll

Fig4: PView Import Address Table



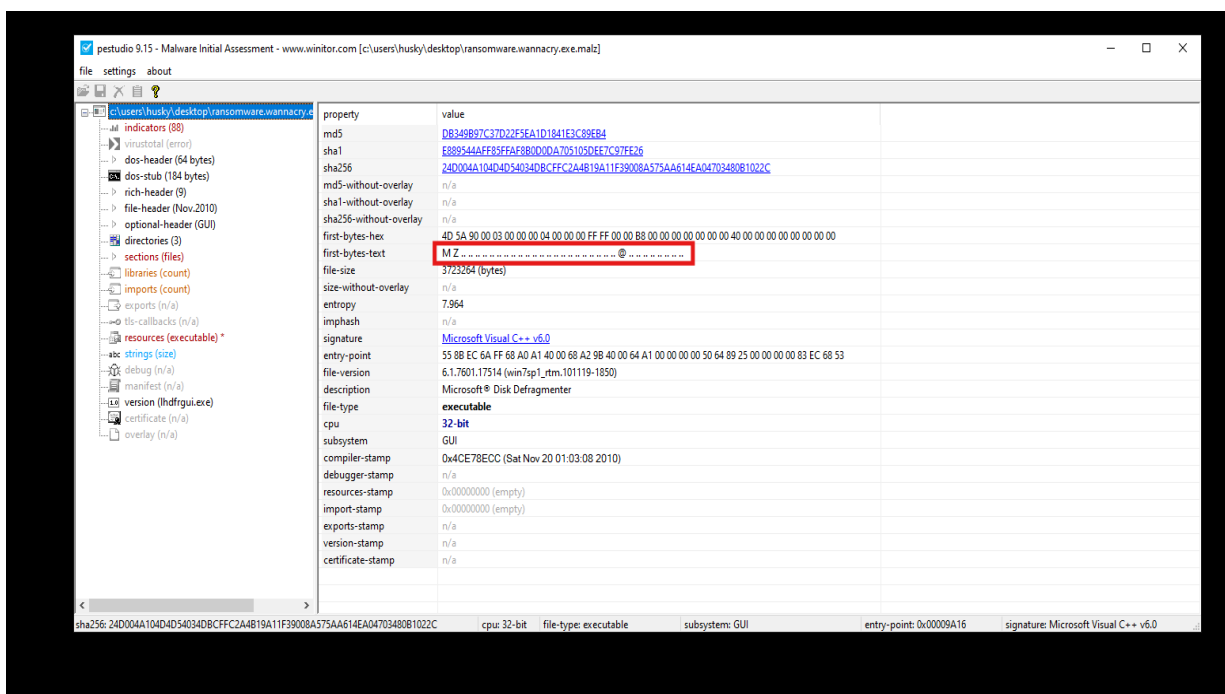


Fig5: PEstudio Output



# Basic Dynamic Analysis

With INETsim:

Wireshark Output:-

No.	Time	Source	Destination	Protocol	Length	Info
21	74.924912791	10.0.0.4	10.0.0.3	TCP	66	49678 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
22	74.924954982	10.0.0.3	10.0.0.4	TCP	66	80 → 49678 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
23	74.925962133	10.0.0.4	10.0.0.3	TCP	60	49678 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
24	74.927424369	10.0.0.4	10.0.0.3	HTTP	154	GET / HTTP/1.1
25	74.927433786	10.0.0.3	10.0.0.4	TCP	54	80 → 49678 [ACK] Seq=1 Ack=101 Win=64256 Len=0
26	74.936263449	10.0.0.3	10.0.0.4	TCP	204	80 → 49678 [PSH, ACK] Seq=1 Ack=101 Win=64256 Len=0
27	74.937038000	10.0.0.4	10.0.0.3	TCP	60	49678 → 80 [ACK] Seq=101 Ack=151 Win=261888 Len=0
28	74.937059827	10.0.0.3	10.0.0.4	HTTP	312	HTTP/1.1 200 OK (text/html)
29	74.937675633	10.0.0.4	10.0.0.3	TCP	60	49678 → 80 [ACK] Seq=101 Ack=409 Win=261632 Len=0
30	74.937992255	10.0.0.4	10.0.0.3	TCP	60	49678 → 80 [FIN, ACK] Seq=101 Ack=409 Win=261632 Len=0
31	74.937992318	10.0.0.4	10.0.0.3	TCP	60	49678 → 80 [RST, ACK] Seq=102 Ack=409 Win=0 Len=0
32	76.188605555	10.0.0.4	10.0.0.3	DNS	81	Standard query 0x19bc PTR 3.0.0.10.in-addr.arpa
33	76.194472075	10.0.0.3	10.0.0.4	DNS	110	Standard query response 0x19bc PTR 3.0.0.10.in-addr.arpa
34	80.180136333	PcsCompu_ce:a9:dd	PcsCompu_55:06:07	ARP	42	Who has 10.0.0.4? Tell 10.0.0.3
35	80.180998938	PcsCompu_55:06:07	PcsCompu_ce:a9:dd	ARP	60	10.0.0.4 is at 08:00:27:55:06:07

Internet Protocol Version 4, Src: 10.0.0.3, Dst: 10.0.0.4  
Transmission Control Protocol, Src Port: 80, Dst Port: 49678, Seq: 151, Ack: 101, Len: 258  
[2 Reassembled TCP Segments (408 bytes): #26(150), #28(258)]  
Hypertext Transfer Protocol  
HTTP/1.1 200 OK  
Content-Type: text/html  
Content-Length: 258  
Connection: Close  
Date: Tue, 08 Oct 2024 05:06:11 GMT  
Server: INetSim HTTP Server  
[HTTP response 1/1]  
[Time since request: 0.009626458 seconds]  
[Request in frame: 24]  
[Request URI: http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrgwea.com/]  
File data: 258 bytes  
Line-based text data: text/html (10 lines)

Fig6: Wireshark Output-Connection to external domain



Process Monitor - Sysinternals: www.sysinternals.com

Time ...	Process Name	PID	Operation	Path	Result	Detail
11:04:...	Ransomware.w...	5628	TCP Connect	DESKTOP-M87PSAK:1167 -> www.inet...	SUCCESS	Length: 0, mss: 14...
11:04:...	Ransomware.w...	5628	TCP Send	DESKTOP-M87PSAK:1167 -> www.inet...	SUCCESS	Length: 100, starti...
11:04:...	Ransomware.w...	5628	TCP Receive	DESKTOP-M87PSAK:1167 -> www.inet...	SUCCESS	Length: 150, seqn...
11:04:...	Ransomware.w...	5628	TCP Receive	DESKTOP-M87PSAK:1167 -> www.inet...	SUCCESS	Length: 258, seqn...
11:04:...	Ransomware.w...	5628	TCP Disconnect	DESKTOP-M87PSAK:1167 -> www.inet...	SUCCESS	Length: 0, seqnum...

Fig7: Procmon Output for network connectivity

Process Monitor - Sysinternals: www.sysinternals.com

Process Tree

Only show processes still running at end of current trace  
Timelines cover displayed events only

Process	Description	Image Path	Life Time	Company	Owner
svchost.exe (2356)	Host Process for ...	C:\Windows\syst...		Microsoft Corporat...	NT AUTHORITY\...
sihost.exe (3600)	Shell Infrastructur...	C:\Windows\syst...		Microsoft Corporat...	DESKTOP-M87P...
Procmon.exe (4524)	Process Monitor	C:\Users\husky\A...		Sysinternals - ww...	DESKTOP-M87P...
Procmon64.exe (2724)	Process Monitor	C:\Users\husky\A...		Sysinternals - ww...	DESKTOP-M87P...
svchost.exe (932)	Host Process for ...	C:\Windows\Syst...		Microsoft Corporat...	NT AUTHORITY\...
ctfmon.exe (1252)	CTF Loader	C:\Windows\syst...		Microsoft Corporat...	DESKTOP-M87P...
Explorer.EXE (2804)	Windows Explorer	C:\Windows\Expl...		Microsoft Corporat...	DESKTOP-M87P...
VirtualBox.exe (388)	VirtualBox Guest...	C:\Windows\Syst...		Oracle and/or its...	DESKTOP-M87P...
Ransomware.wannacry.exe (5628)	Microsoft® Disk D...	C:\Users\husky\N...		Microsoft Corporat...	DESKTOP-M87P...
System (4)	System				NT AUTHORITY\...
MemCompression (1848)	MemCompression				NT AUTHORITY\...
Registry (92)	Registry				NT AUTHORITY\...
smss.exe (328)	Windows Session ...	C:\Windows\Syst...		Microsoft Corporat...	NT AUTHORITY\...
csrss.exe (440)	Client Server Runt...	C:\Windows\syst...		Microsoft Corporat...	NT AUTHORITY\...
wininit.exe (516)	Windows Start-Up...	C:\Windows\syst...		Microsoft Corporat...	NT AUTHORITY\...
services.exe (648)	Services and Cont...	C:\Windows\syst...		Microsoft Corporat...	NT AUTHORITY\...
svchost.exe (1748)	Host Process for ...	C:\Windows\syst...		Microsoft Corporat...	NT AUTHORITY\...

Description: Microsoft® Disk Defragmenter  
Company: Microsoft Corporation  
Path: C:\Users\husky\Desktop\Ransomware.wannacry.exe  
Command: "C:\Users\husky\Desktop\Ransomware.wannacry.exe"  
User: DESKTOP-M87PSAK\husky  
PID: 5628 Started: 9/30/2024 11:04:15 PM  
Exited: 9/30/2024 11:04:16 PM

Go To Event Include Process Include Subtree Close

Fig8: Procmon Process Tree Output



The Procmon Process tree also gives out details about some other subtasks that are spawned and run by WannaCry. Details of which can be found in the Indicators of compromise section.



# Advanced Static Analysis

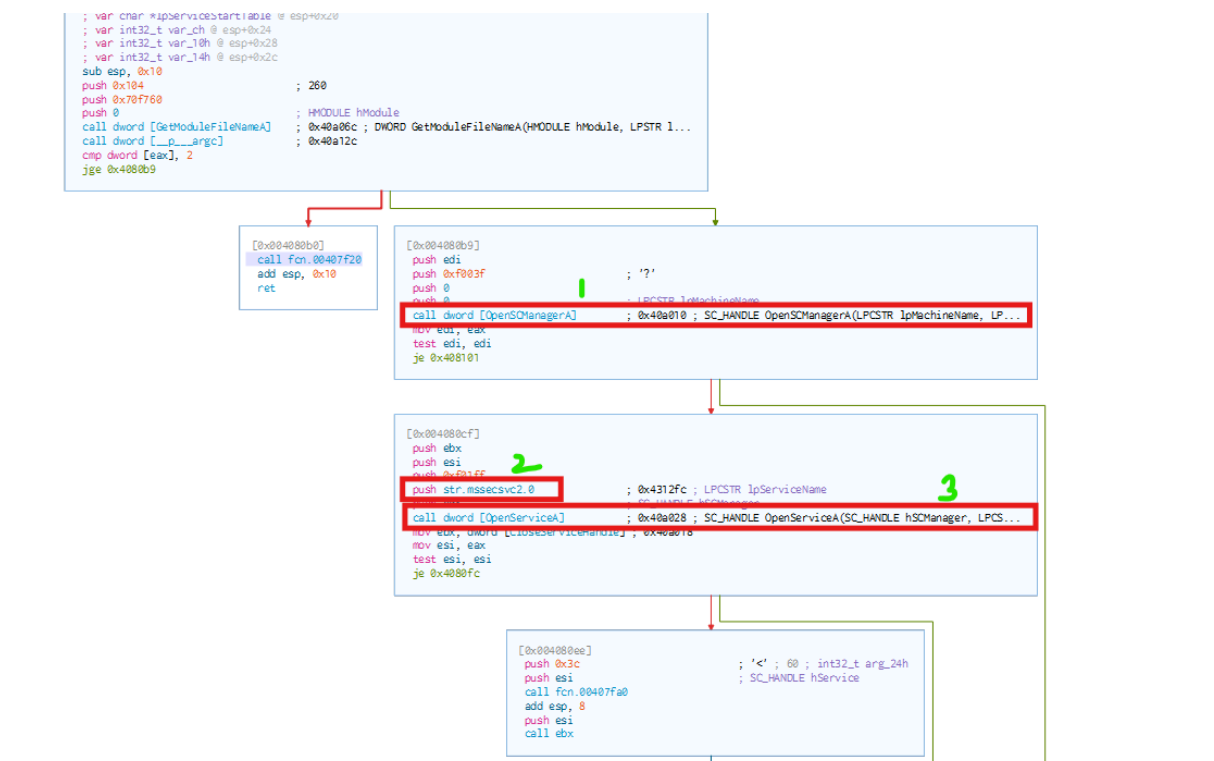


Fig9: Cutter Output



# Advanced Dynamic Analysis

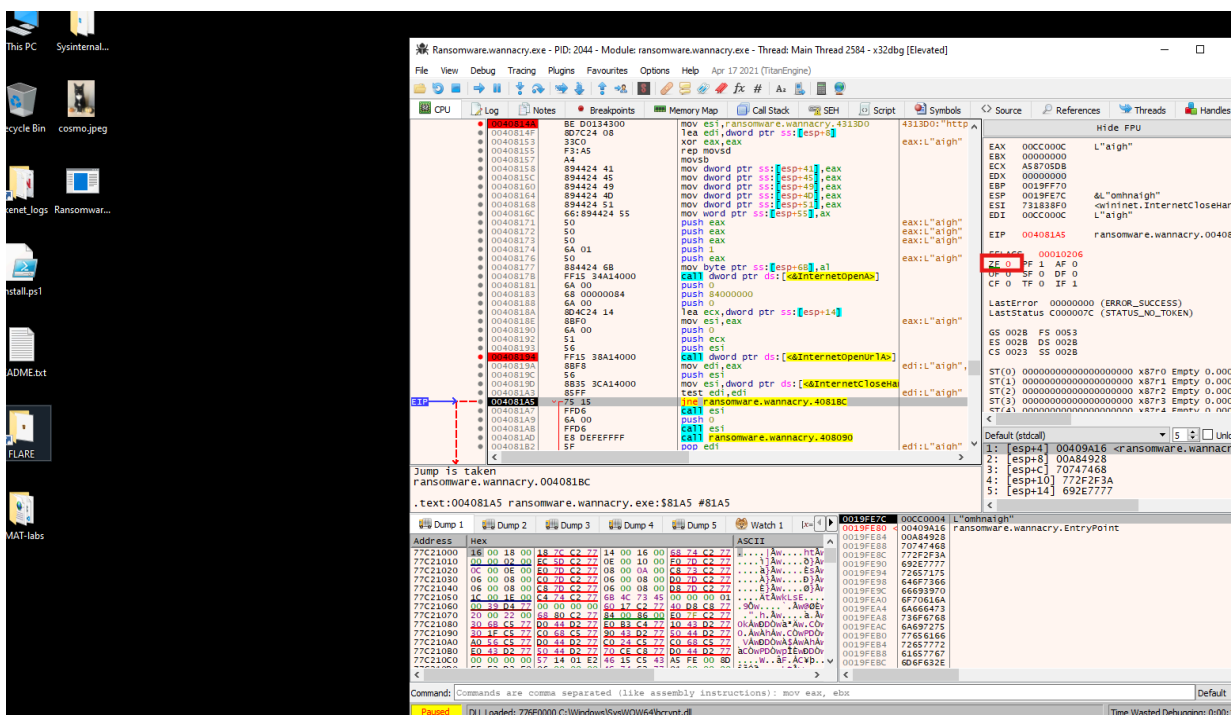
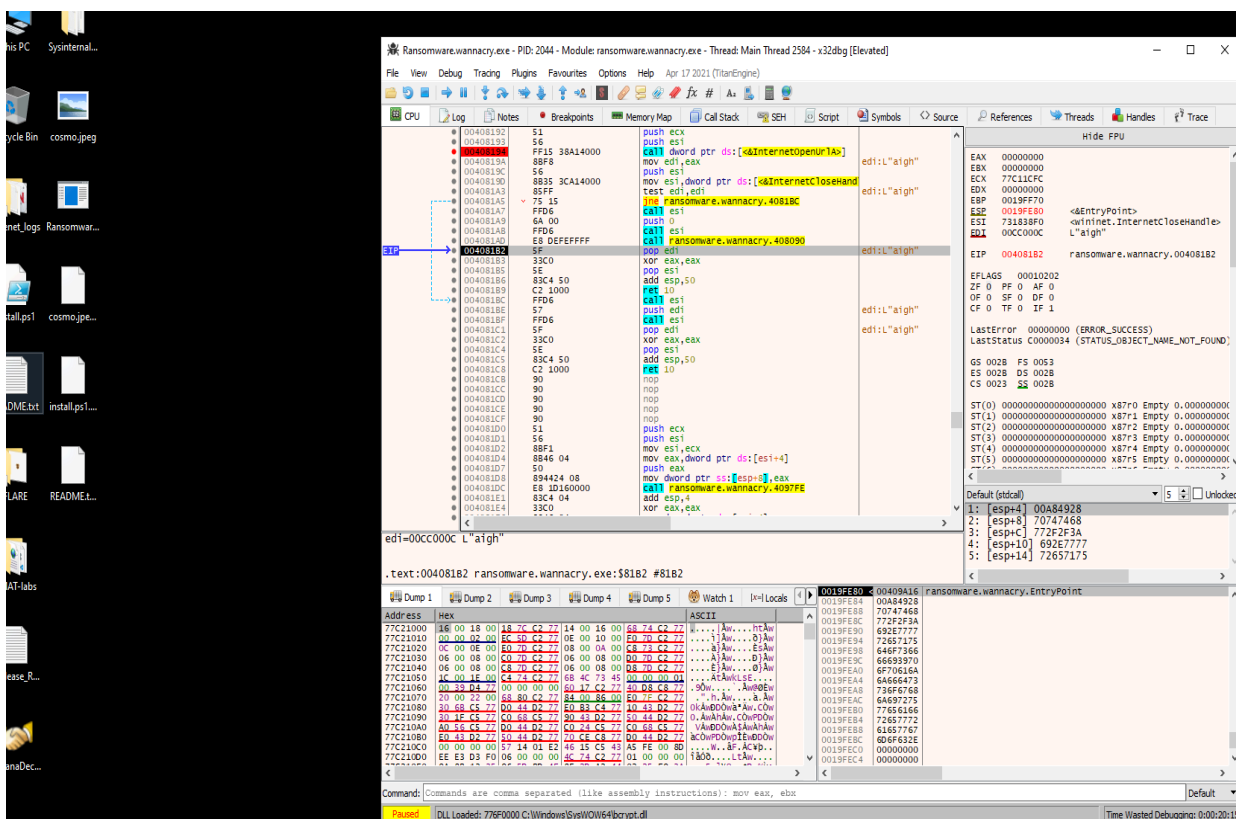


Fig10: Executing binary without patching



### Fig11: Executing after patching binary

DemoWare Crypto-Dropper Malware  
Oct 2021  
v1.0



# Indicators of Compromise

## Network Indicators

TCPView - Sysinternals: www.sysinternals.com

File Edit View Process Connection Options Help

4 TCP v4 6 TCP v6 4 UDP v4 6 UDP v6 Search

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	Sent Packets
svchost.exe	880	TCP	Listen	0.0.0.0	135	0.0.0.0	0	8/12/2024 11:03:31 AM	RpcEptMapper	
System	4	TCP	Listen	10.0.0.4	139	0.0.0.0	0	10/8/2024 12:55:12 AM	System	
System	4	TCP	Listen	169.254.243.48	139	0.0.0.0	0	8/12/2024 11:03:27 AM	System	
MicrosoftEdgeUpdate.exe	1228	TCP	Syn Sent	10.0.0.4	3932	10.0.0.3	443	10/8/2024 12:57:10 AM	MicrosoftEdgeUpdate.exe	
svchost.exe	3088	TCP	Syn Sent	10.0.0.4	4287	10.0.0.3	443	10/8/2024 12:57:24 AM	svchost.exe	
Ransomware.wannacr...	1592	TCP	Syn Sent	169.254.243.48	4653	169.254.215.3	445	10/8/2024 12:57:37 AM	mssecsvcs2.0	
Ransomware.wannacr...	1592	TCP	Syn Sent	169.254.243.48	4654	169.254.216.3	445	10/8/2024 12:57:37 AM	mssecsvcs2.0	
Ransomware.wannacr...	1592	TCP	Syn Sent	169.254.243.48	4657	169.254.217.3	445	10/8/2024 12:57:38 AM	mssecsvcs2.0	
Ransomware.wannacr...	1592	TCP	Syn Sent	169.254.243.48	4658	169.254.218.3	445	10/8/2024 12:57:38 AM	mssecsvcs2.0	
Ransomware.wannacr...	1592	TCP	Syn Sent	169.254.243.48	4664	169.254.219.3	445	10/8/2024 12:57:38 AM	mssecsvcs2.0	
Ransomware.wannacr...	1592	TCP	Syn Sent	169.254.243.48	4666	169.254.220.3	445	10/8/2024 12:57:38 AM	mssecsvcs2.0	
Ransomware.wannacr...	1592	TCP	Syn Sent	169.254.243.48	4668	169.254.221.3	445	10/8/2024 12:57:38 AM	mssecsvcs2.0	
Ransomware.wannacr...	1592	TCP	Syn Sent	169.254.243.48	4674	169.254.222.3	445	10/8/2024 12:57:38 AM	mssecsvcs2.0	
Ransomware.wannacr...	1592	TCP	Syn Sent	169.254.243.48	4675	169.254.223.3	445	10/8/2024 12:57:38 AM	mssecsvcs2.0	
svchost.exe	2012	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	8/11/2024 10:33:29 PM	CDPSvc	
lsass.exe	660	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	8/12/2024 11:03:31 AM	lsass.exe	
wininit.exe	516	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	8/12/2024 11:03:31 AM	wininit.exe	
svchost.exe	1184	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	8/12/2024 11:03:32 AM	EventLog	
svchost.exe	1148	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	8/12/2024 11:03:32 AM	Schedule	
spoolsv.exe	2544	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	8/11/2024 10:33:37 PM	Spooler	
services.exe	648	TCP	Listen	0.0.0.0	49669	0.0.0.0	0	8/11/2024 10:33:40 PM	services.exe	
svchost.exe	2780	TCP	Listen	0.0.0.0	49670	0.0.0.0	0	8/11/2024 10:33:40 PM	PolicyAgent	
System	4	TCP	Listen	0.0.0.0	445	0.0.0.0	0	8/11/2024 10:33:39 PM	System	
System	4	TCP	Listen	0.0.0.0	5357	0.0.0.0	0	8/11/2024 10:33:37 PM	System	
svchost.exe	880	TCPv6	Listen	::	135	::	0	8/12/2024 11:03:31 AM	RpcEptMapper	
System	4	TCPv6	Listen	::	445	::	0	8/11/2024 10:33:39 PM	System	
System	4	TCPv6	Listen	::	5357	::	0	8/11/2024 10:33:37 PM	System	

Endpoints: 78 Established: Listening: 23 Time Wait: Close Wait: Update: 2 sec States: (All)

Fig12: TCPview Output displaying network indicators





## Host-based Indicators

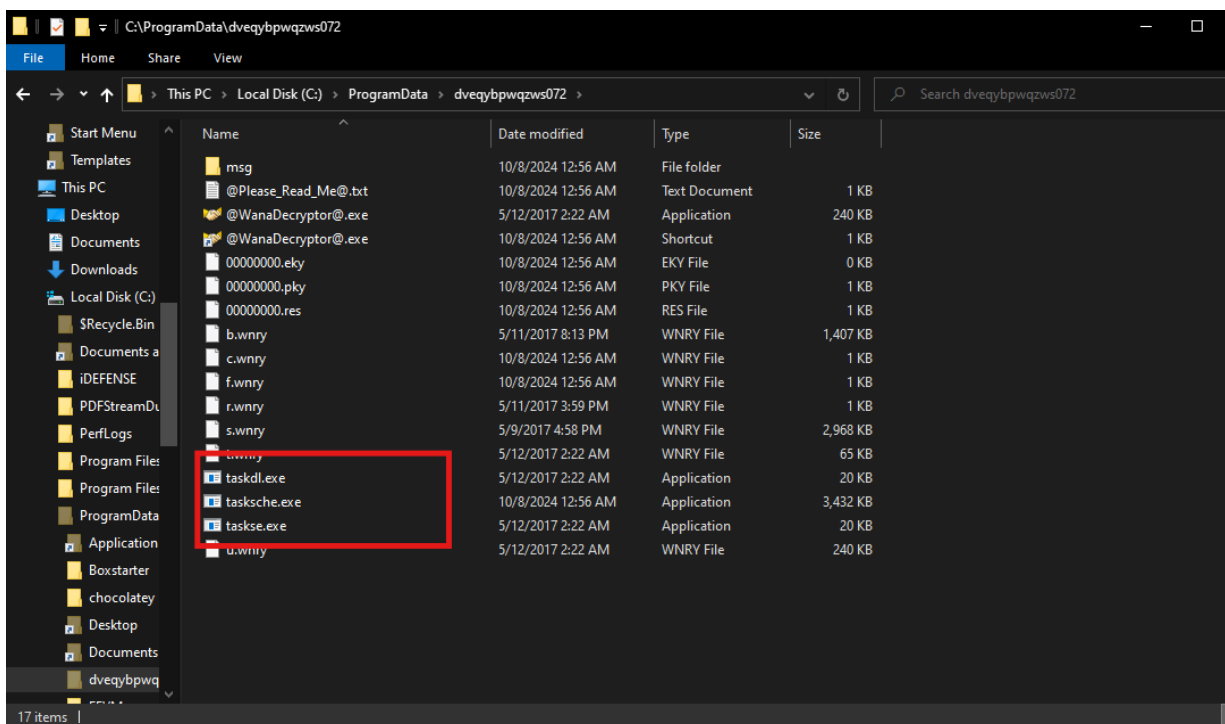


Fig13: Creation of hidden directory with malicious processes.

### Note:-

The highlighted executables are the malicious processes that the sample spawns off and executes.



## Rules & Signatures

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

- Since this is a windows based binary the PE magic header can be found at the start of the file which can be marked.
- Also the external URL that the malware initially tries to connect with is another such string to look out for.
- We can also look out for the hidden directory that is created once the malware starts its proper functioning.
- Including the processes dropped into that folder.



# Appendices

## A. Yara Rules

```
rule WannaCry_catcher {  
    meta:  
        author = "Niyanth Guruprasad"  
        Created on = "08-10-2024"  
        Last updated on = "08-10-2024"  
        Description = "Detection Rule for WannaCry Ransomware,PMAT"  
  
    strings:  
        $PE_magic_header_byte = "MZ"  
        $External_URL =  
"http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com" ascii  
        $hidden_directory = "C:\\ProgramData\\%s"  
        $spawned_executables1 = "tasksche.exe"  
        $spawned_executables2 = "taskse.exe"  
        $spawned_executables3 = "taskdl.exe"  
        $common_file_extension = ".wnry"  
  
    condition:  
        $PE_magic_header_byte at 0 and $common_file_extension and $External_URL  
and $hidden_directory and ($spawned_executables1 or $spawned_executables2 or  
$spawned_executables3)  
}
```



## B. Callback URLs

Domain	Port
hxxp[:]//www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com	80

## C. Decompiled Code Snippets

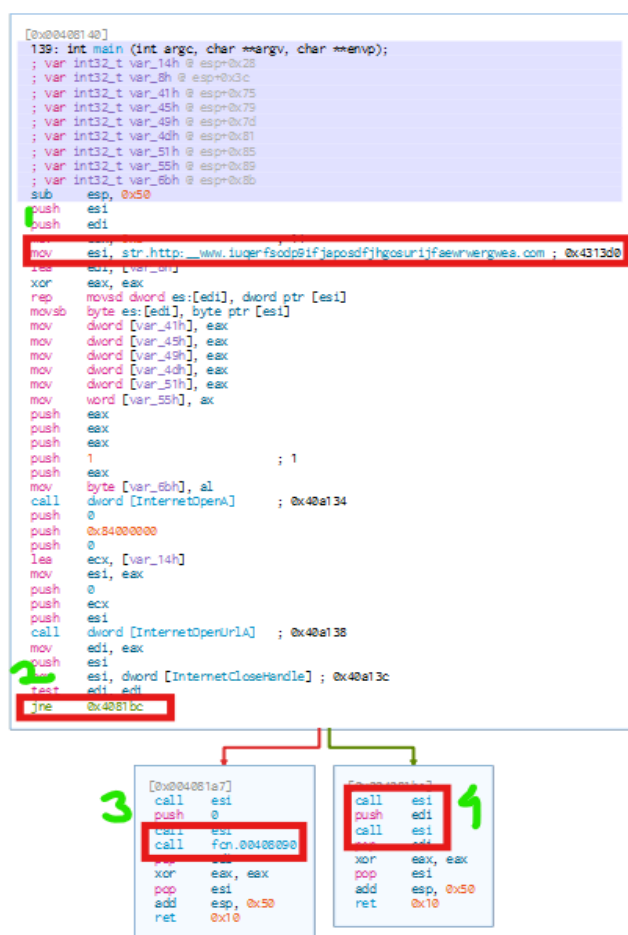


Fig14: Cutter Output of main function