Icon

Description automatically generated

Practical Malware Analysis & Triage

Malware Analysis Report

WannaCry Ransomware Malware

Oct 2022 | Vishal Pathak | v1.0

# Table of Contents

[Table of Contents 2](#_Toc85207993)

[Executive Summary 3](#_Toc85207994)

[High-Level Technical Summary 4](#_Toc85207995)

[Malware Composition 5](#_Toc85207996)

[srvupdate.exe 5](#_Toc85207997)

[crt1.crt: 5](#_Toc85207998)

[Basic Static Analysis 6](#_Toc85207999)

[Basic Dynamic Analysis 7](#_Toc85208000)

[Advanced Static Analysis 8](#_Toc85208001)

[Advanced Dynamic Analysis 9](#_Toc85208002)

[Indicators of Compromise 10](#_Toc85208003)

[Network Indicators 10](#_Toc85208004)

[Host-based Indicators 11](#_Toc85208005)

[Rules & Signatures 13](#_Toc85208006)

[Appendices 14](#_Toc85208007)

[A. Yara Rules 14](#_Toc85208008)

[B. Callback URLs 14](#_Toc85208009)

[C. Decompiled Code Snippets 15](#_Toc85208010)

# 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.

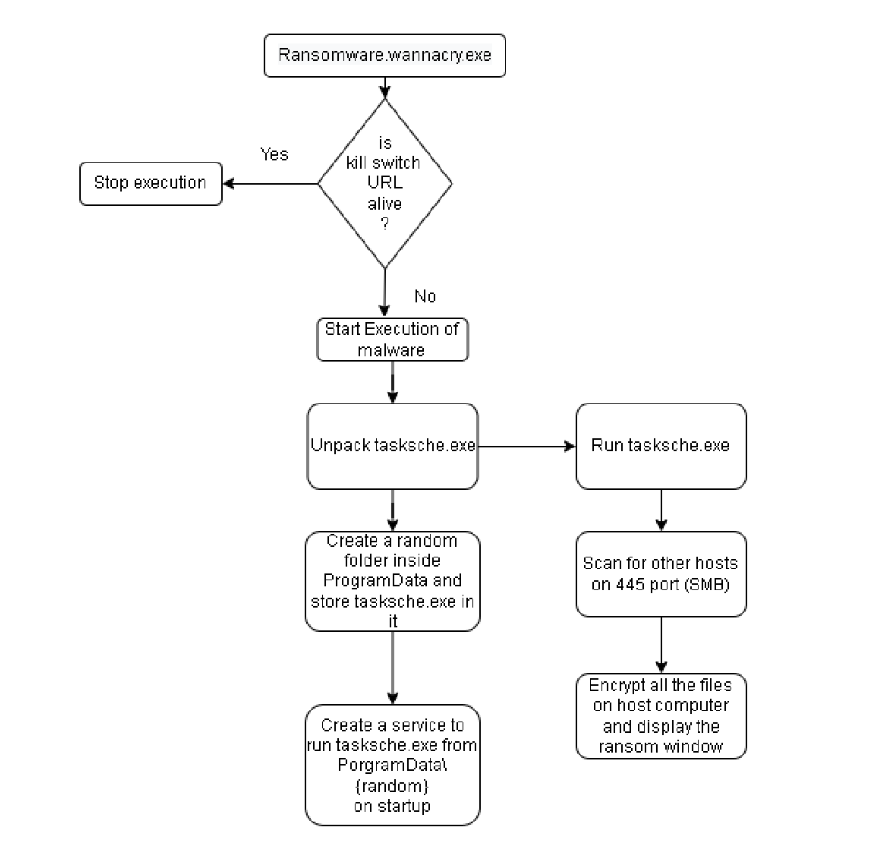


Fig- 1 – Flow of Malware

# Malware Composition

DemoWare consists of the following components:

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

## Wannacry.exe

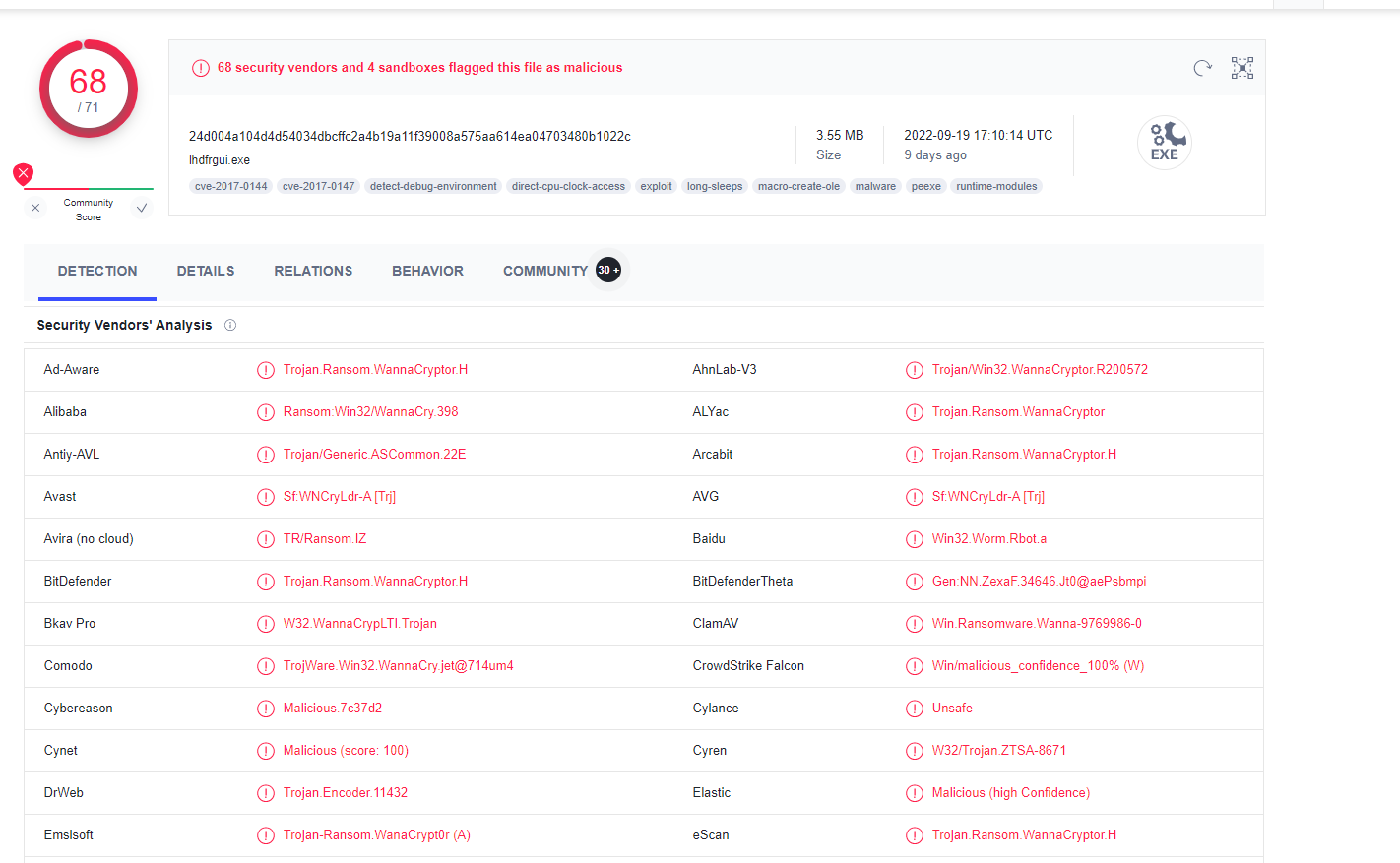
The initial executable that tries to contact the url. If url is alive it doesn’t execute else unpacks the taskche.exe.

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



String./Floss Output

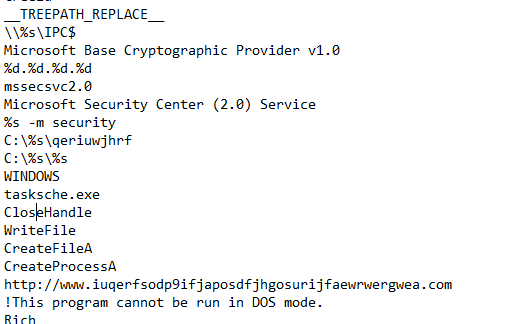


Fig –2 – Kill Switch Url and random paths

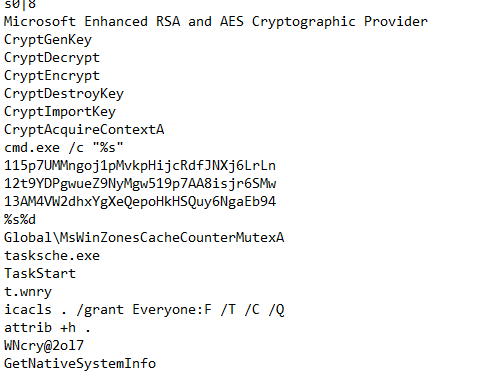


Fig –3 – Some imports, ical used for modifying acess control on file ,attrib +h to hide file attribute

PE View Analysis

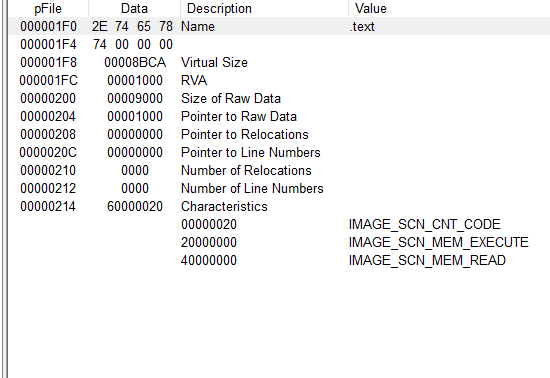


Fig – 4- (Unpacked Size)

Import Address Tables

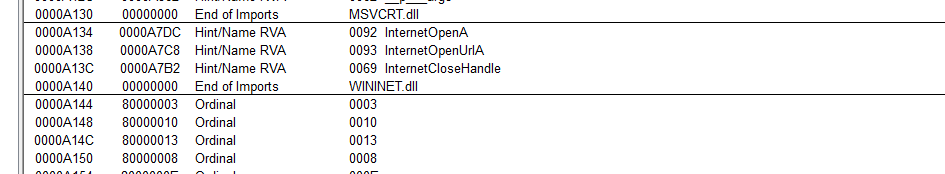


Fig –5 – Internet Connection Address/Imports

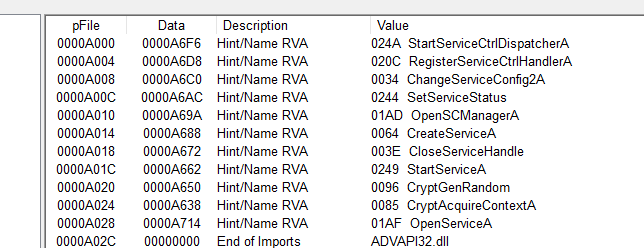


Fig – 6- Encrptying Import Address/Imports

# Basic Dynamic Analysis

Analysis with InetSim – ON

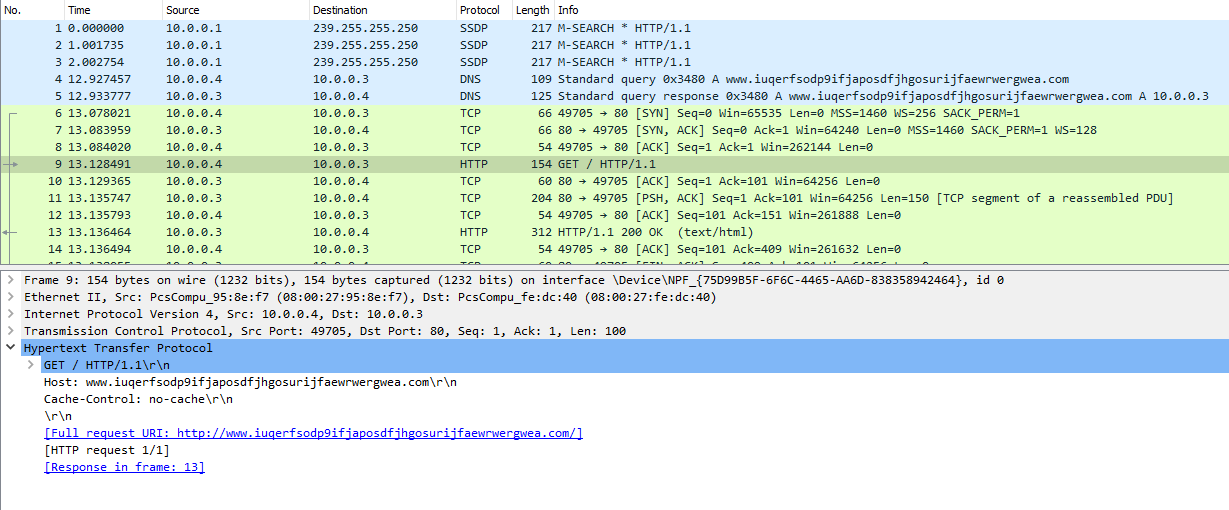


Fig - 7- Network Traffic when malware is executed

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

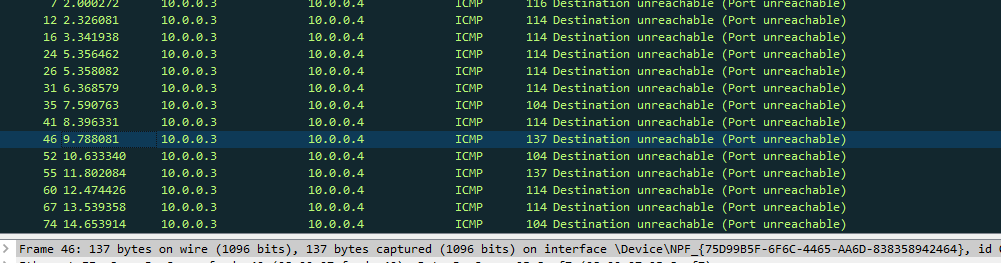


Fig – 8 – Network Traffic when malware execute. The request are unreachable since inetsim is off.



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

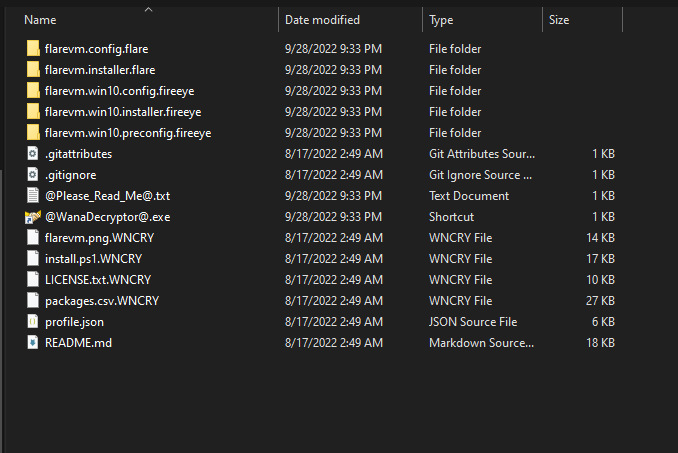


Fig – 10 – Encrypted file with extension .WNCRY and New files added.

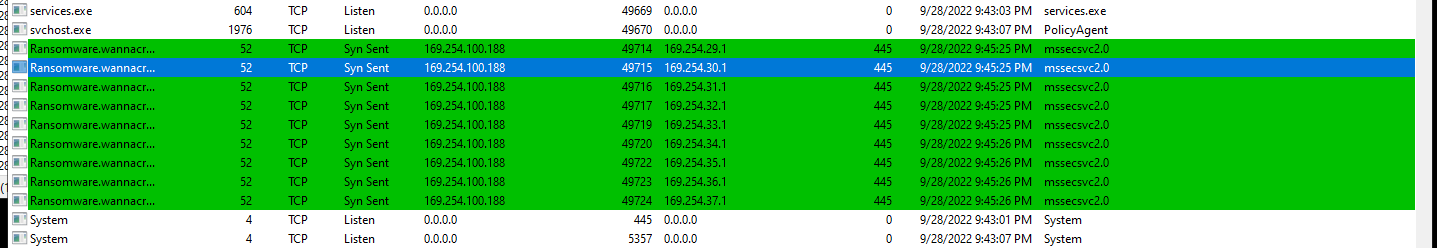


Fig –11 – Taskche.exe tries to locate and infect computer using port 445(SMB)

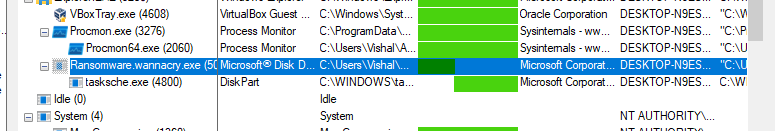


Fig – 12 – Procmon Process tree for wannacry.

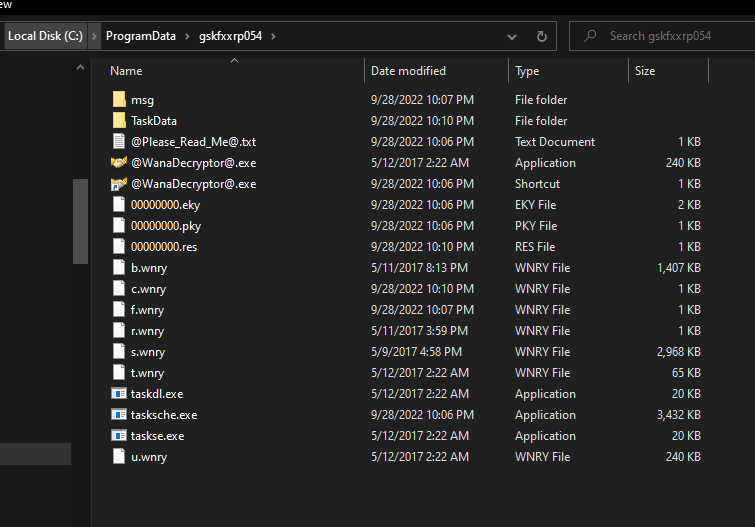


Fig – 13 – New Folder Created with random name in C:/ProgramData/{random name}

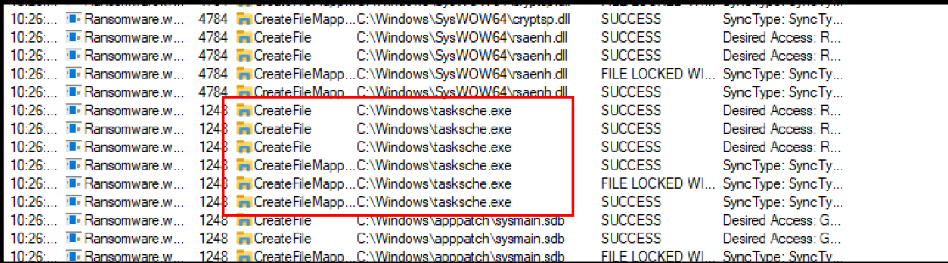


Fig – 14 – Creation of taskche.exe file

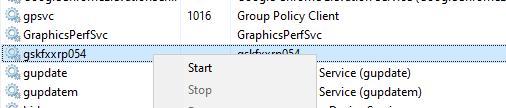


Fig – 15- Task Manager. A service named as the random folder created by malware.

# Advanced Static Analysis

Cutter



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

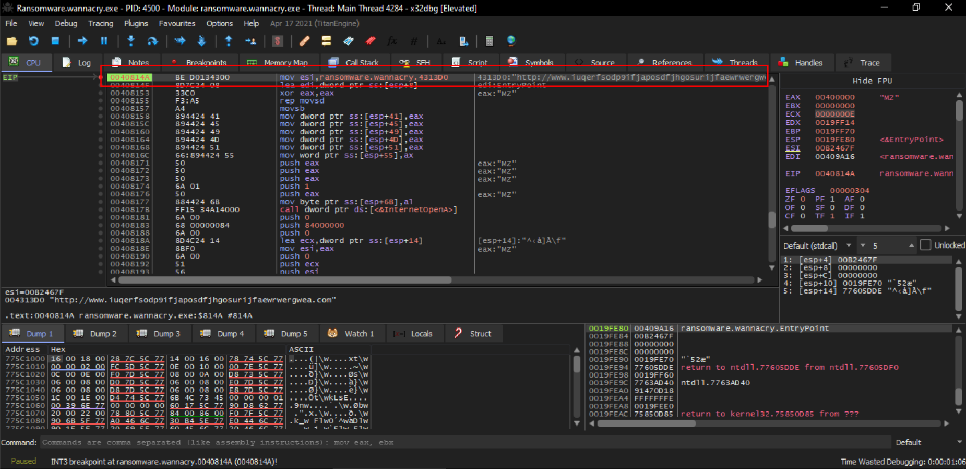


Fig-17 - Set a Break point on the kill switch url

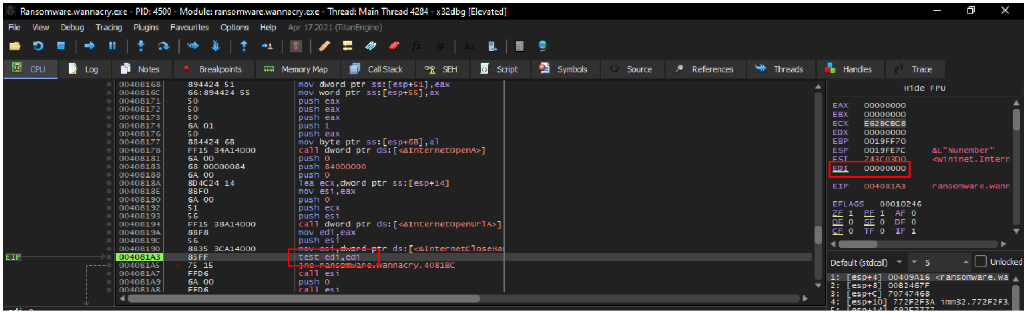


Fig –18 - The kill switch was not found hence EDI value is 0

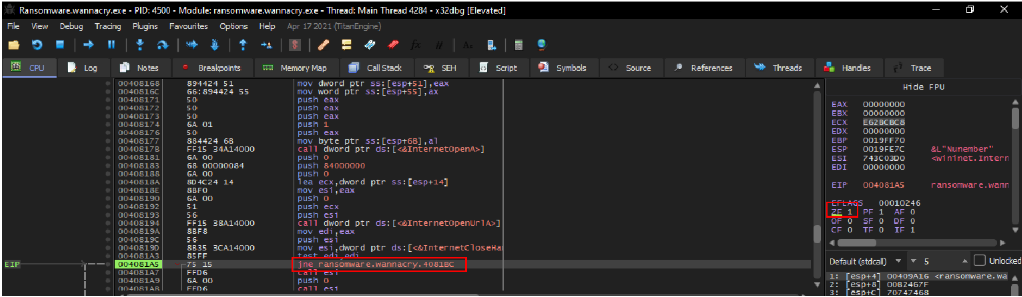


Fig - 19- The zero is elevated to 1 but we change it to 0

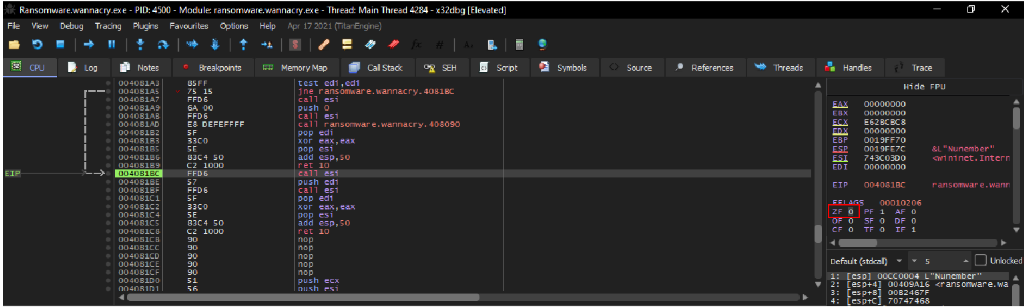


Fig -20 -Changing the zero flag to 0 make the malware jump call and it is not executed

# Indicators of Compromise

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

## Network Indicators

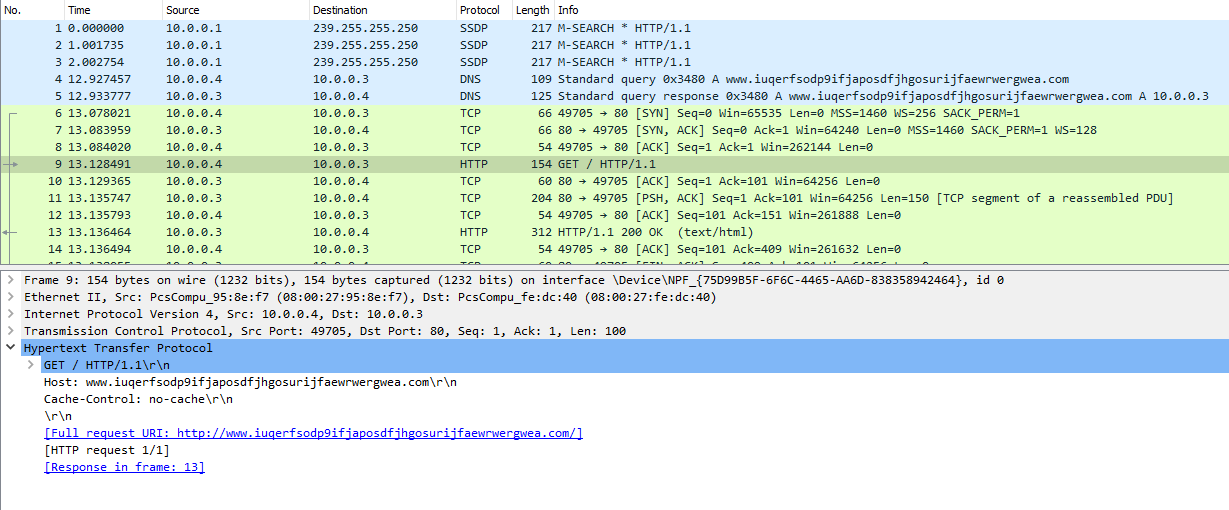


Fig -21 - Initial Connection to kill switch Url

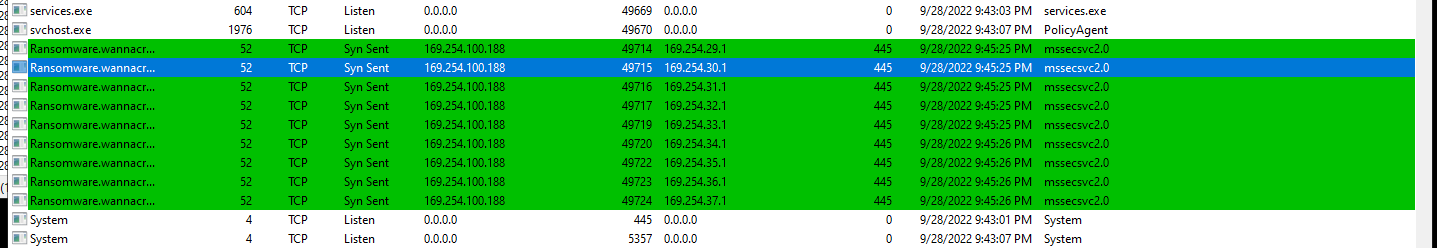


Fig - 22- Locating other machine and exploiting SMB on port 445

## Host-based Indicators

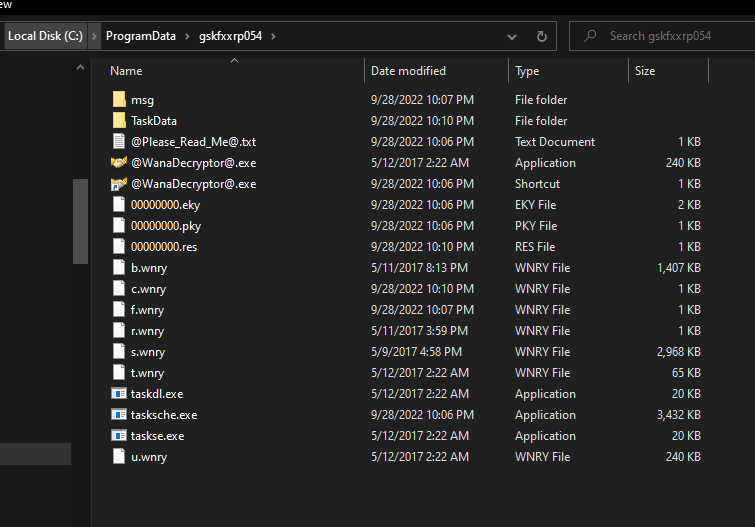


Fig-23 - New Folder Created with random name



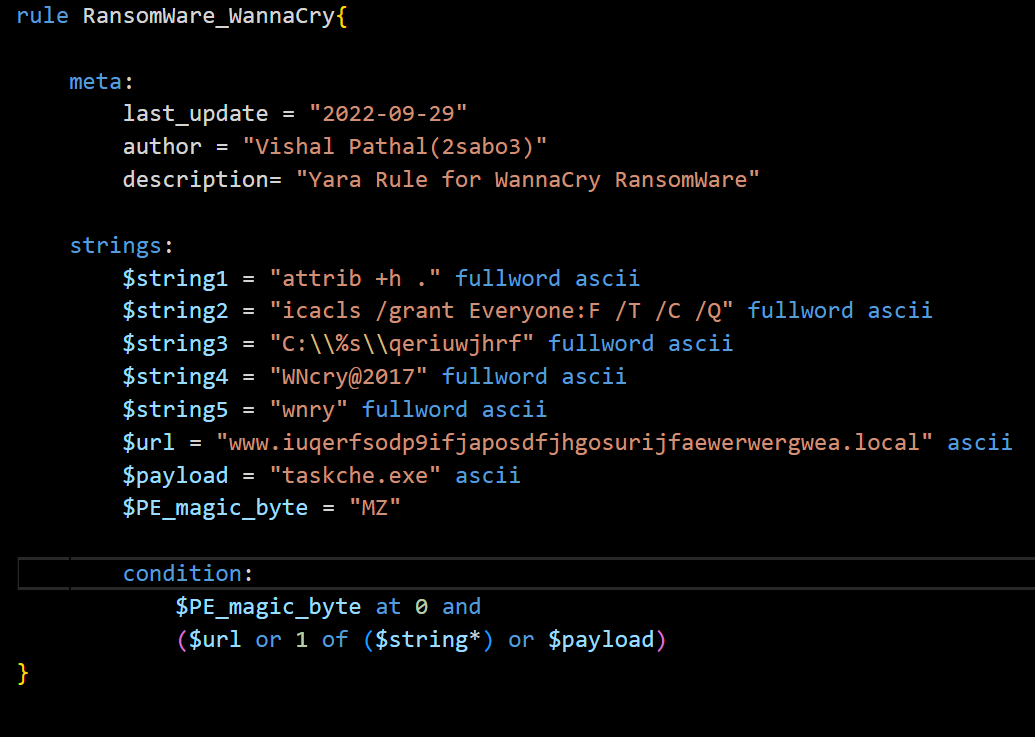
Fig- 24- Payment Screen, wannadecrpytor and desktop background changed.

# Rules & Signatures

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

# Appendices

## Yara Rules



## Decompiled Code Snippets

