Practical Malware Analysis & Triage

Malware Analysis Report

WannaCry Ransomware

Feb 2023 | Sochurthy | v1.0

WannaCry Ransomware
Feb 2023
v1.0

Contents

Executive Summary

SHA256 hash	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c

WannaCry is a ransomware worm that encrypts the files and spreads itself to the network. Microsoft Visual C ++compiled that runs on 32 bits windows operating system. First identified on May of 2017.

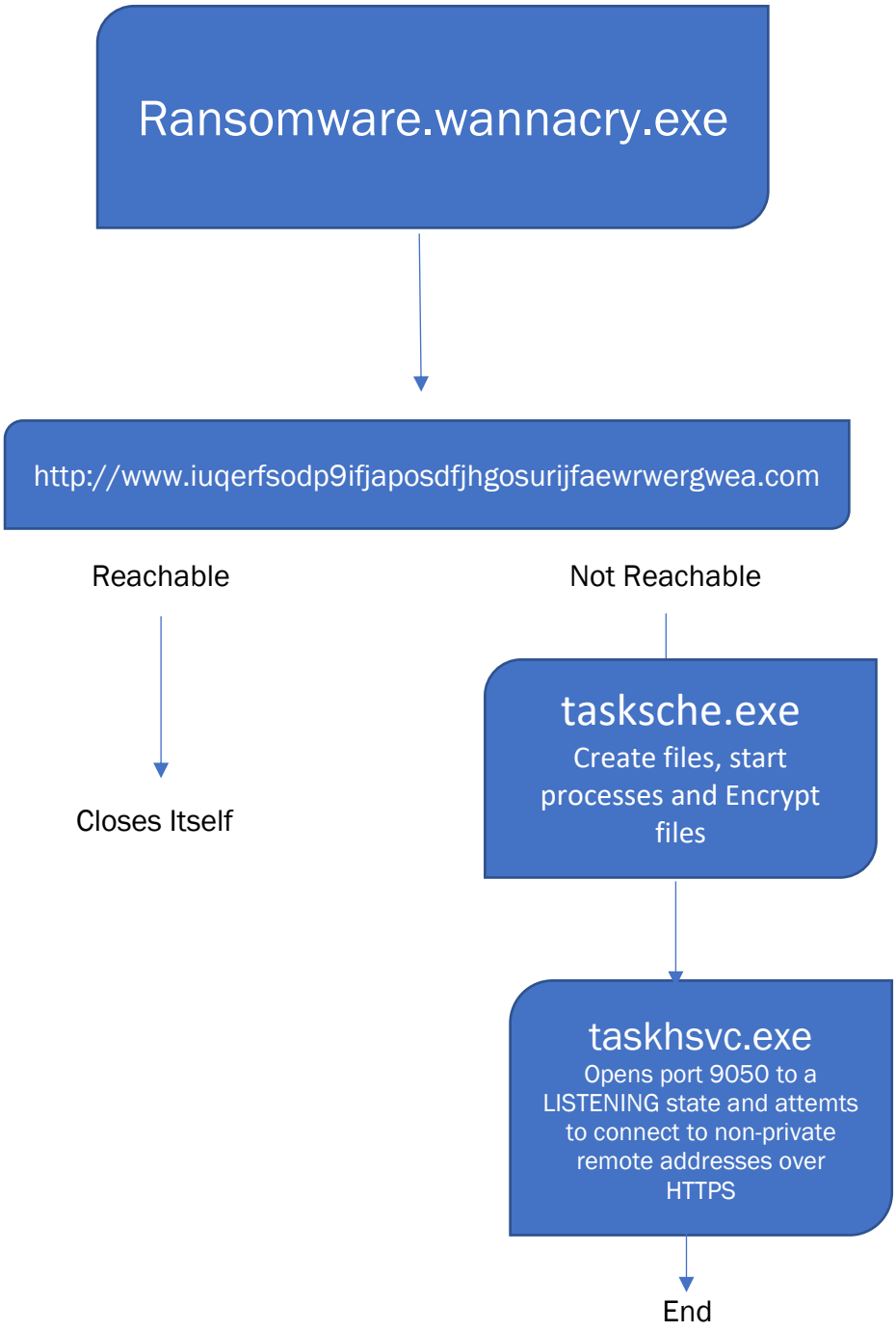
How it works?

It uses an API "InternetOpenUrlA" to test if the url "http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com" is reachable, if so, it spawns the payload "Tasksche.exe" that creates files, encrypt files, "taskhsvc.exe" opens port 9050 to a LISTENING state and attempts to connect to non-private remote addresses over HTTPS. If not, it deletes itself.

Symptoms of infection?

The wallpaper changes on the infected host plus a program shows up indicating that the host has been infected and the files are encrypted with the appearance of @WanaDecryptor@ "executable file" and @Please_Read_Me@ text file on the Desktop

High-Level Technical Summary

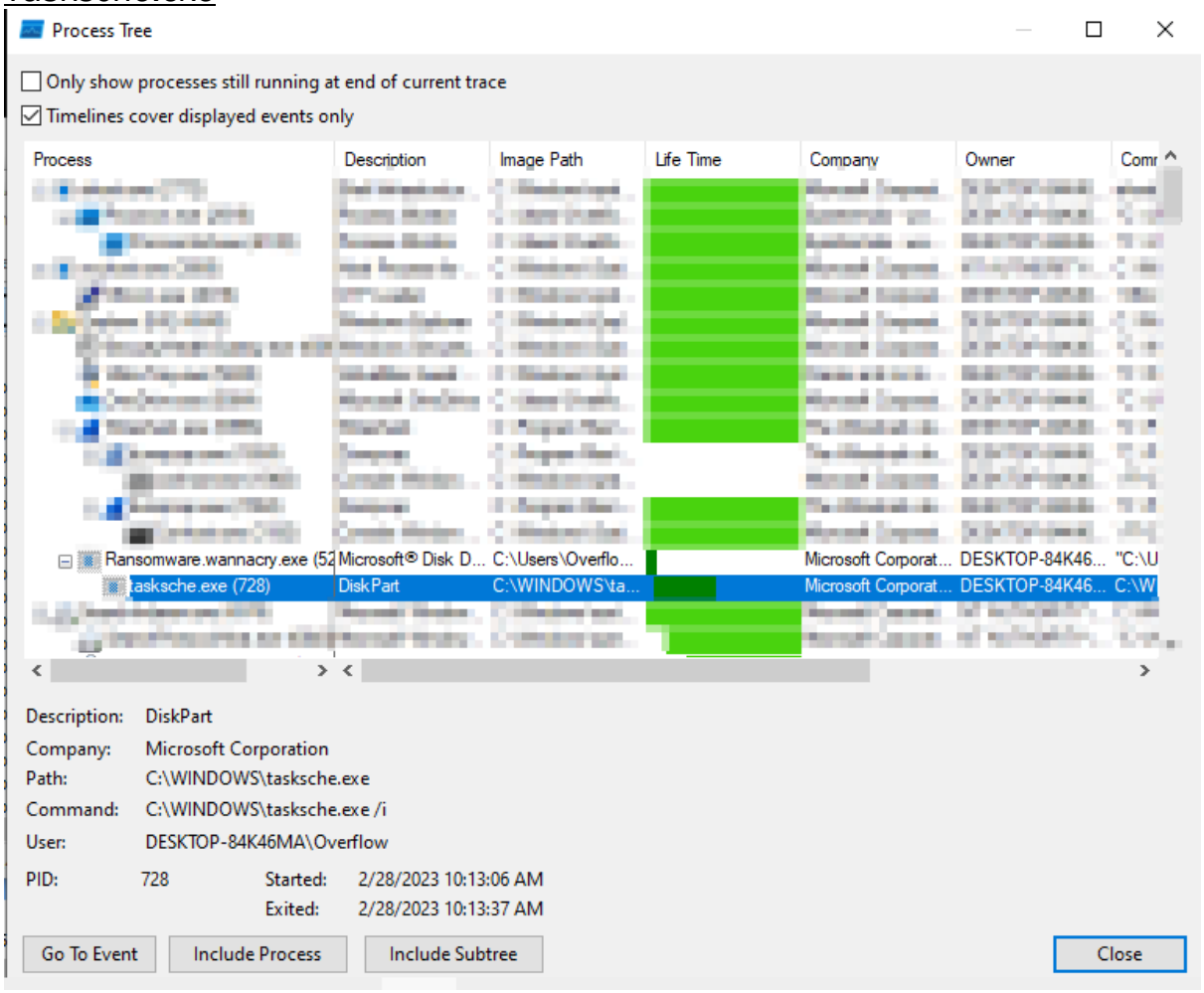


Malware Composition

WannaCry consists of the following components:

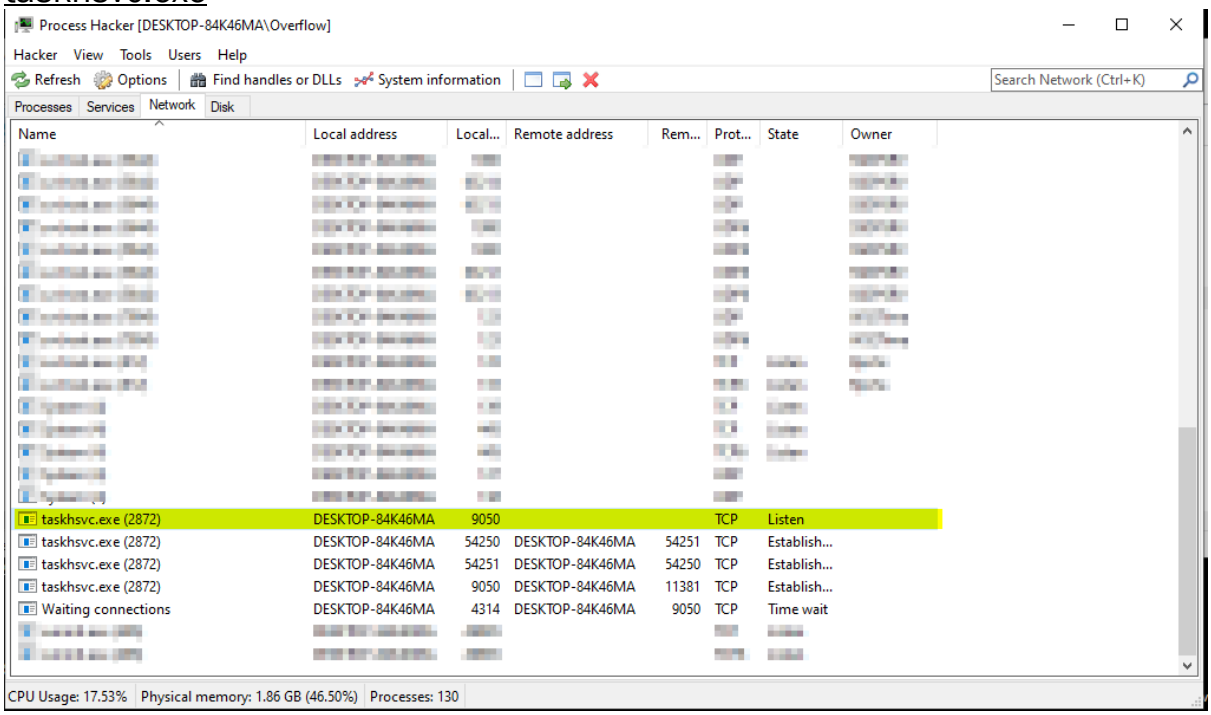
File Name	SHA256 Hash
tasksche.exe	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
taskhsvc.exe	8ac6dc5bb016afc869fcbb713f6a14d3692e866b94f4f1ee83b09a7506a8cb587
tor.exe	e48673680746fbe027e8982f62a83c298d6fb46ad9243de8e79b7e5a24dcd4eb
taskse.exe	2ca2d550e603d74dedda03156023135b38da3630cb014e3d00b1263358c5f00
taskdl.exe	4a468603fdcb7a2eb5770705898cf9ef37aade532a7964642ecd705a74794b79
@WanaDecryptor@.exe	b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25

Tasksche.exe



Create files, start processes and Encrypt files

taskhsvc.exe



Opens port 9050 to a LISTENING state and attempts to connect to non-private remote addresses over HTTPS

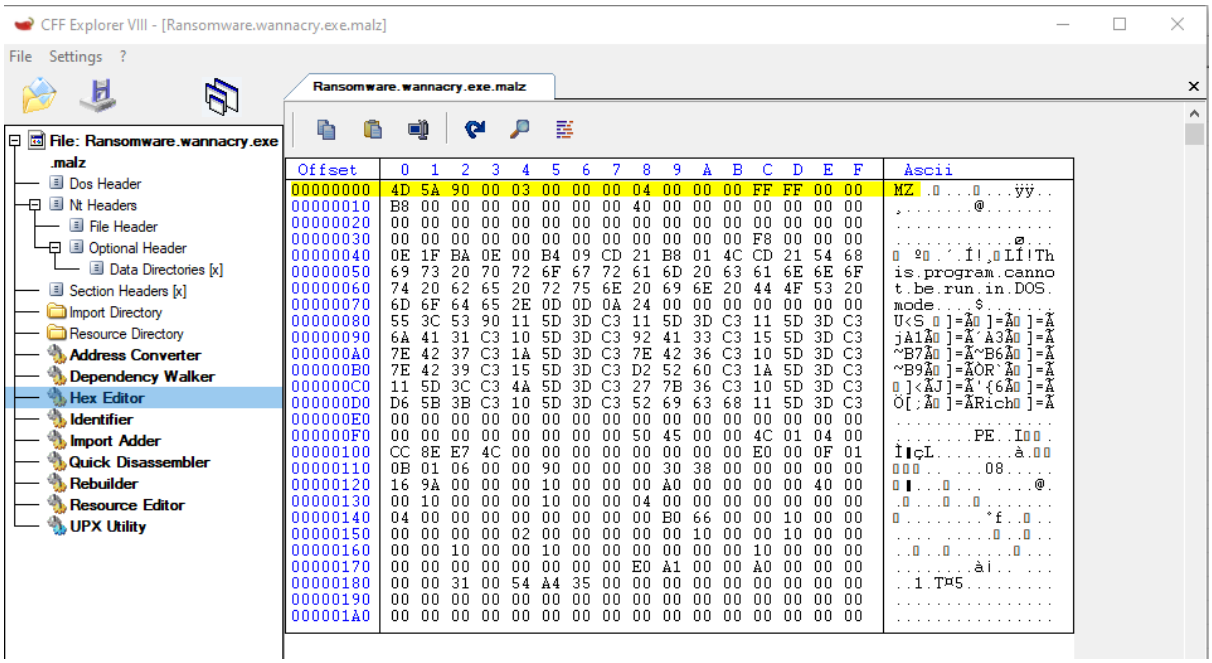
Basic Static Analysis

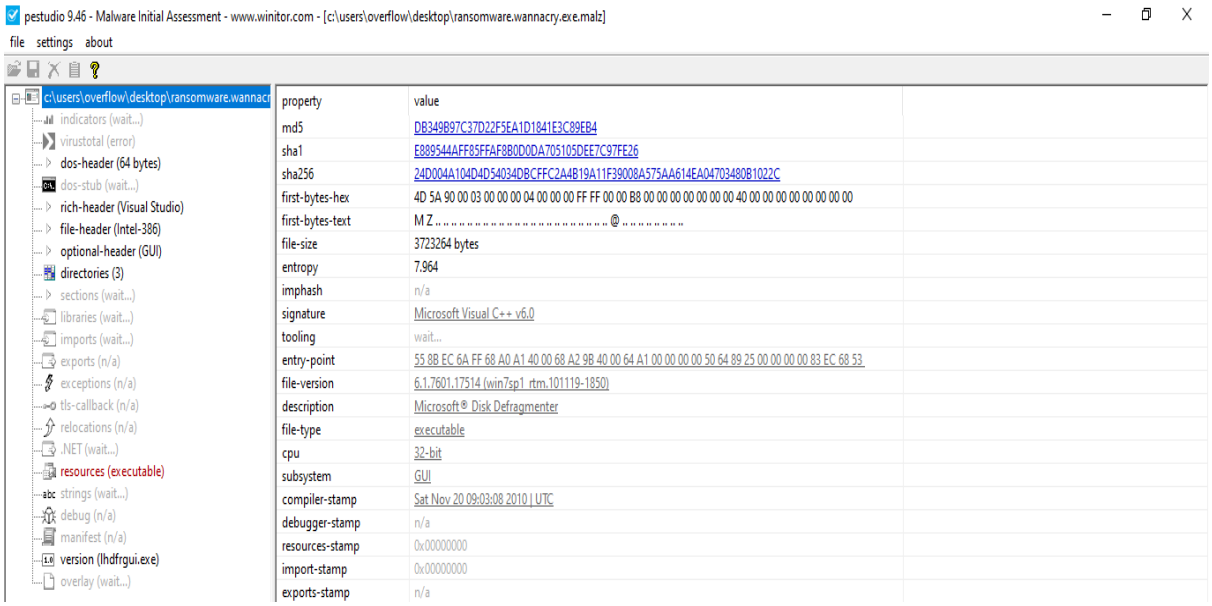
- **Extract strings using Floss**

Example of suspicious strings

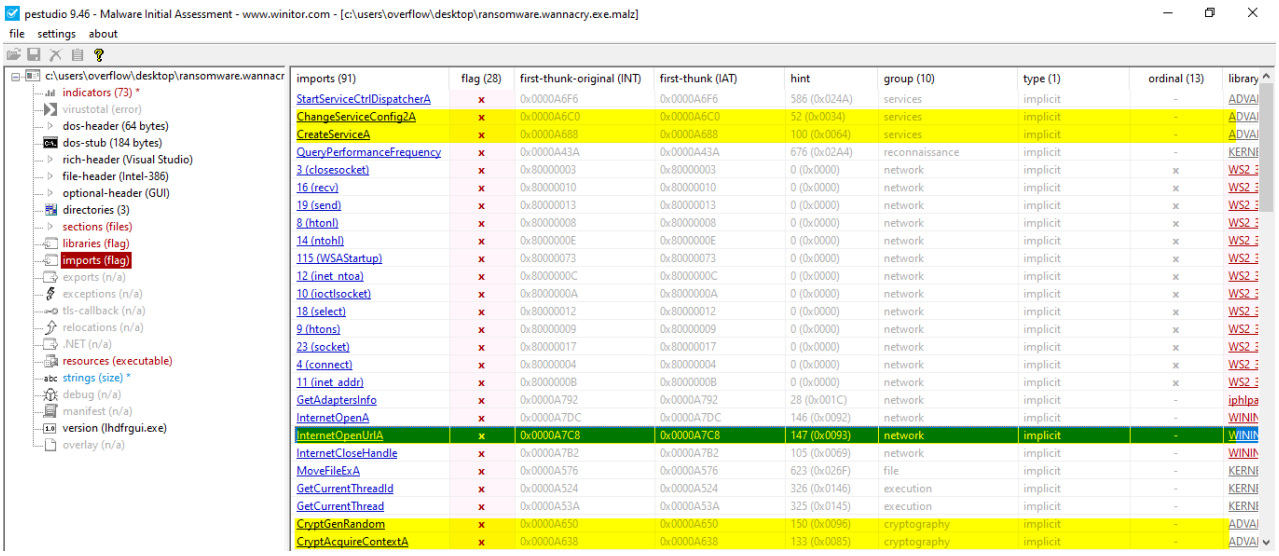
tasksche.exe t.wnry WNcry@2ol7 WanaCrypt0r \\192.168.56.20\IPC$ diskpart.exe lhdfrgui.exe http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com SMB2

- CFF - mz ascii





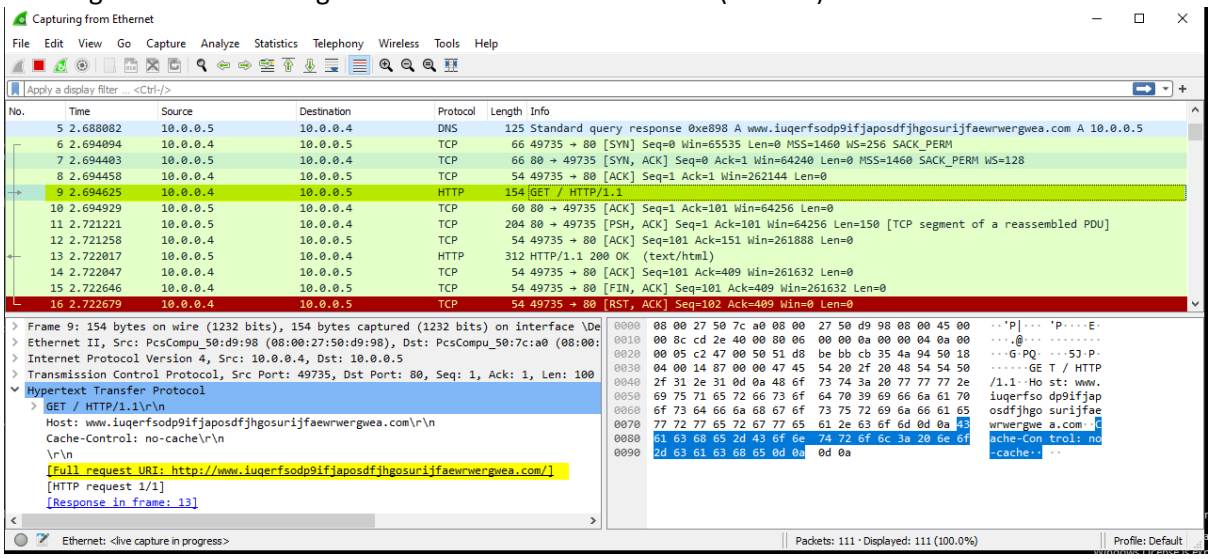
- PESTUDIO:



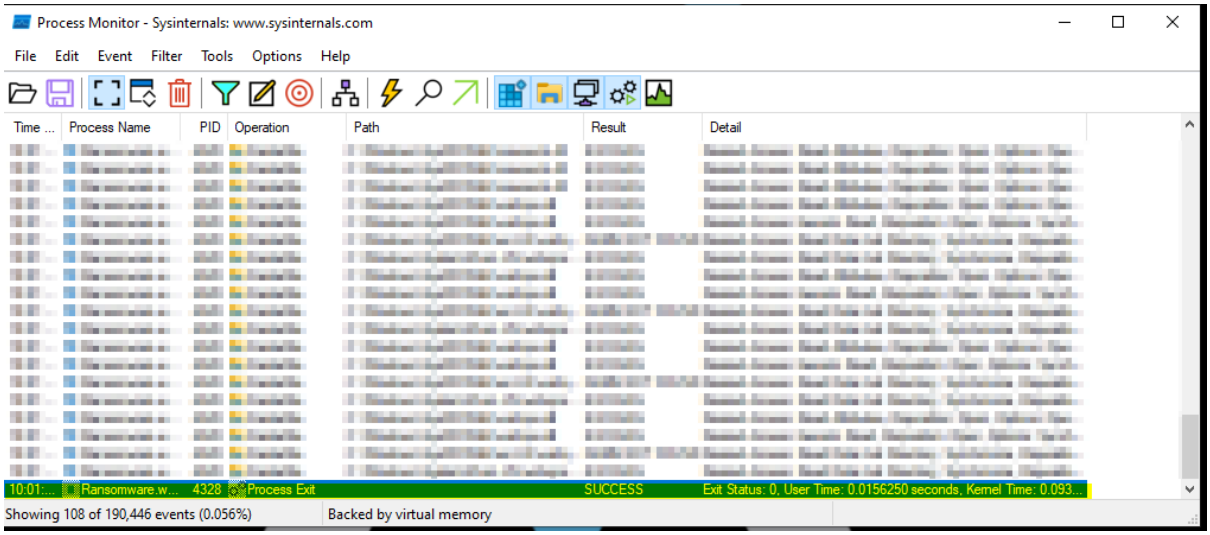
Some red flags imports

Basic Dynamic Analysis

Running the malware using a fake internet to see the result (inetsim)



The malware end itself after reaching out the server

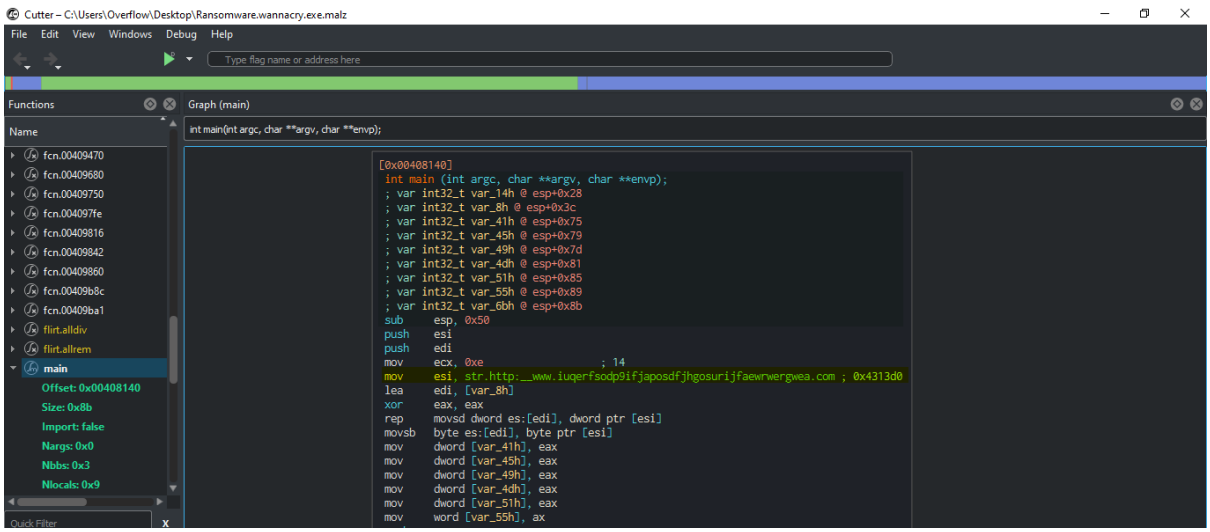


The malware end itself after reaching out the server

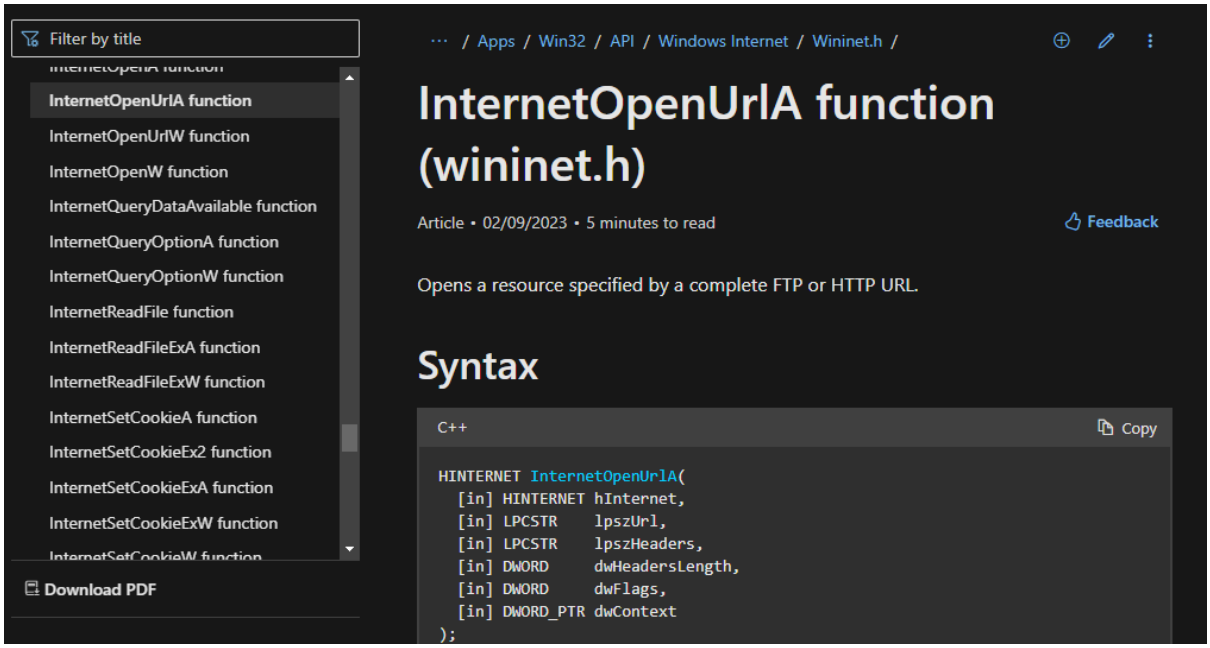
For so, let's try to run the ransomware without using inetsim to see how the malware will behave!

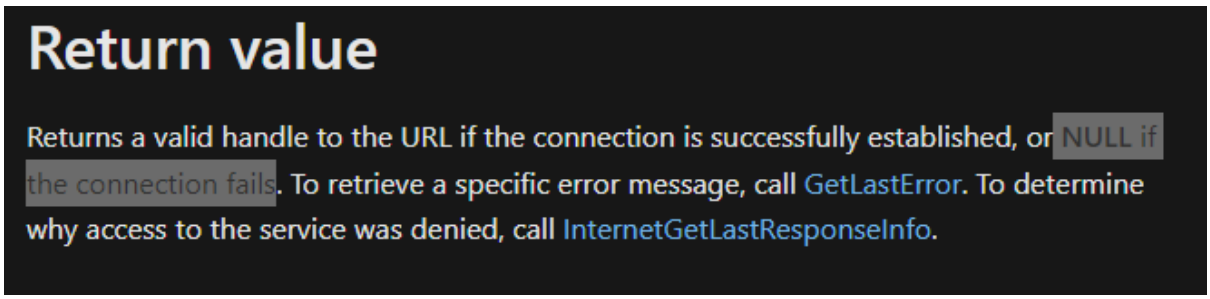
If he can’t reach out to the server, the ransomware runs

Advanced Static Analysis

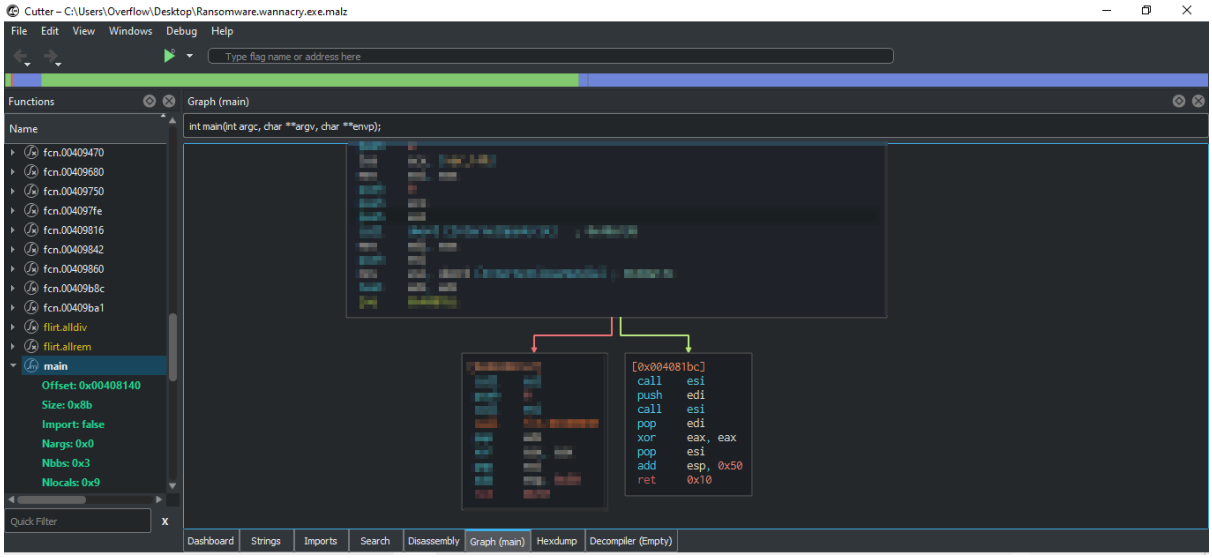


In the main function, we notice the url that the malware tries to reach out, moving it to the esi, and calling the "InternetOpenUrlA" API

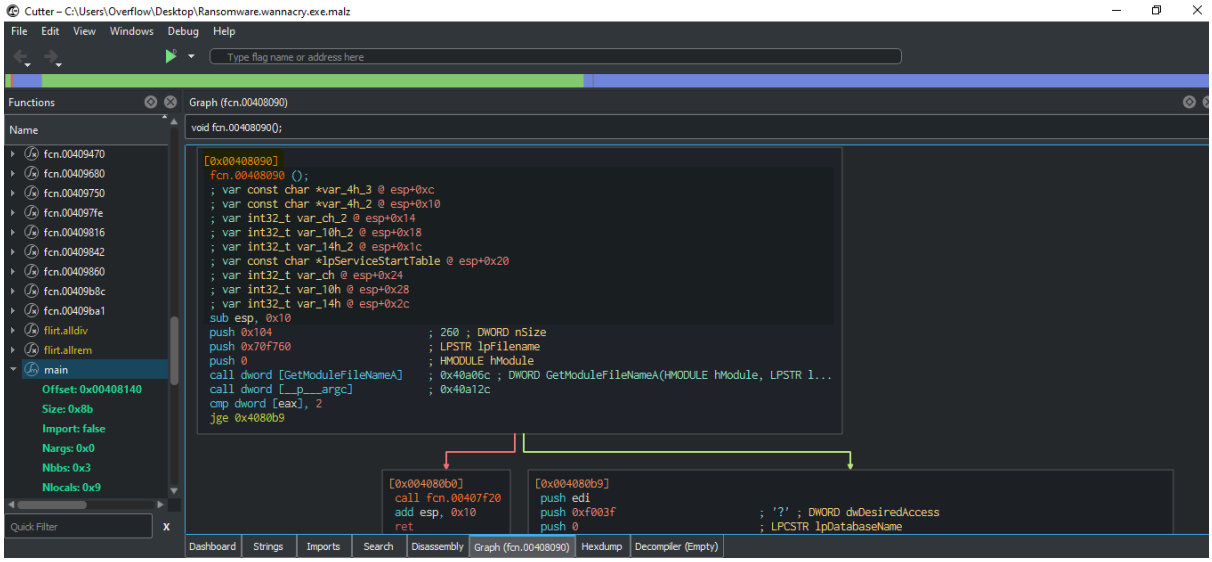




If it reaches out the url, to malware closes itself => value 1



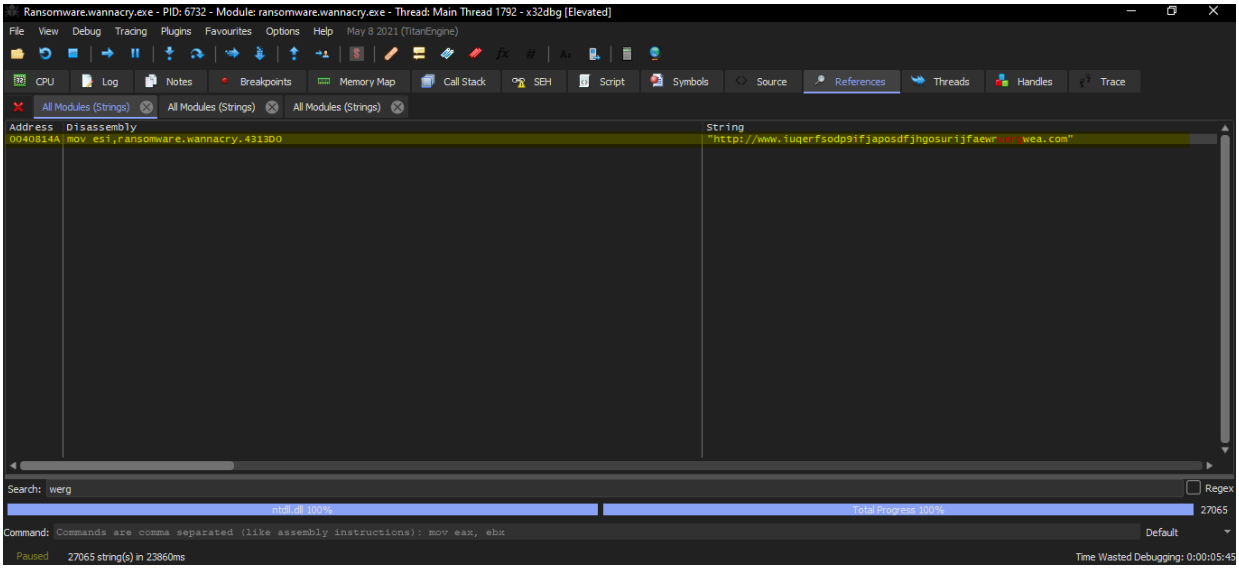
If not, the malware calls fcn.00408090 (payload)

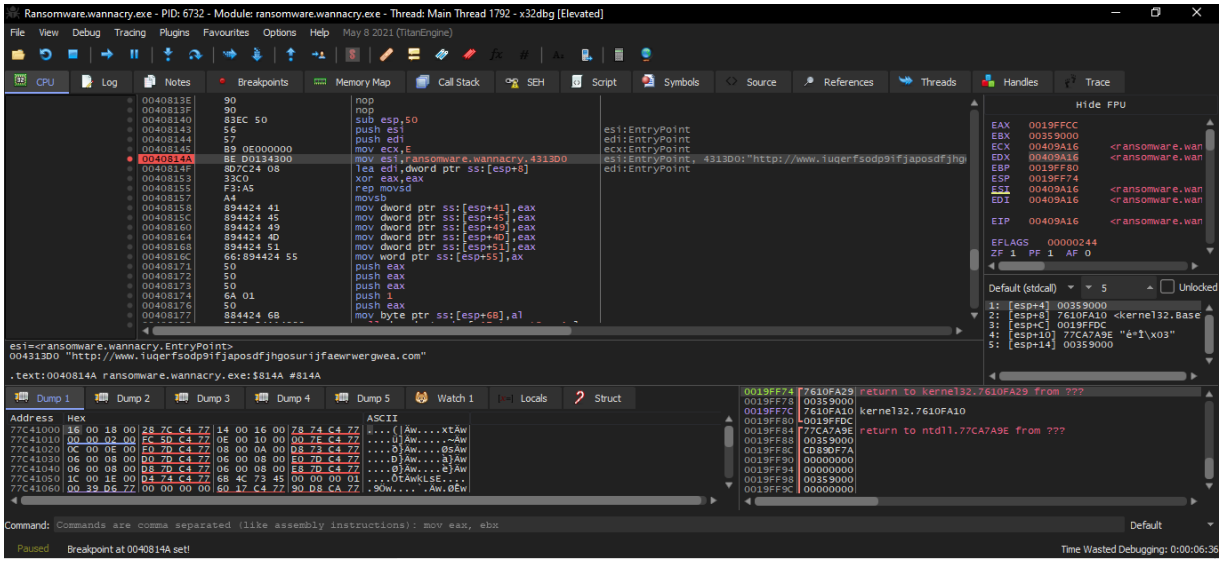


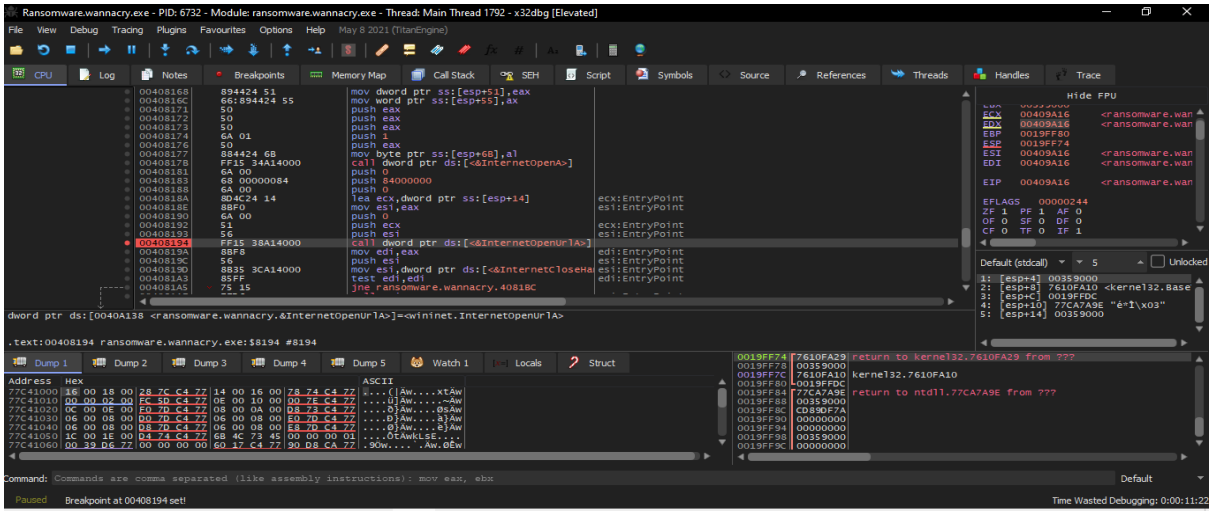
Advanced Dynamic Analysis

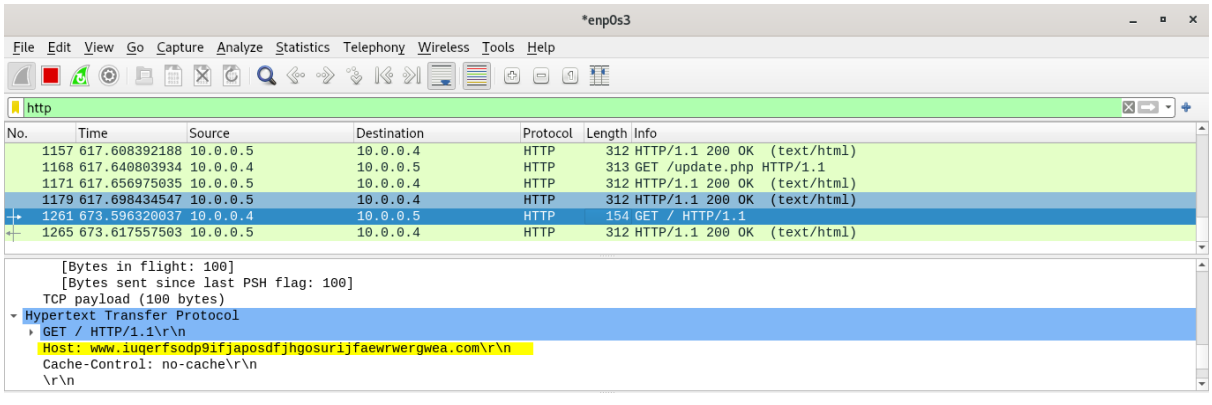
Using x32db, let's search for the API "InternetOpenUrlA" and the Url http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com and setting them as breakpoints to see how the malware will behave, also we'll try to change the zero flag value to see if the malware will call fcn.00408090 (payload) even if it reaches out the Url, for so, we'll use the fake internet "inetsim".

Setting the breakpoint "url'

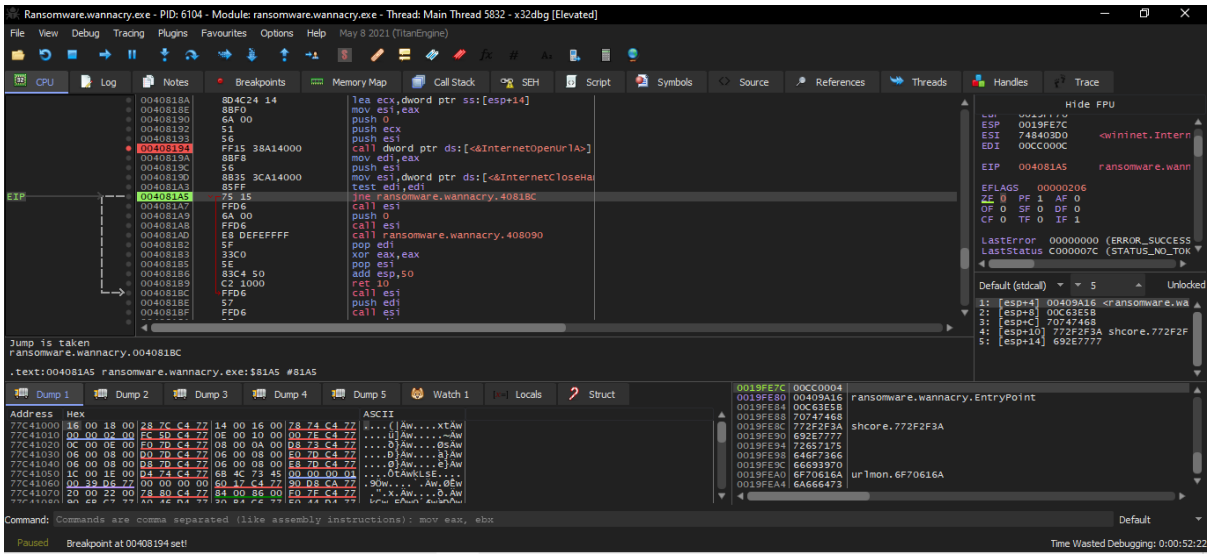




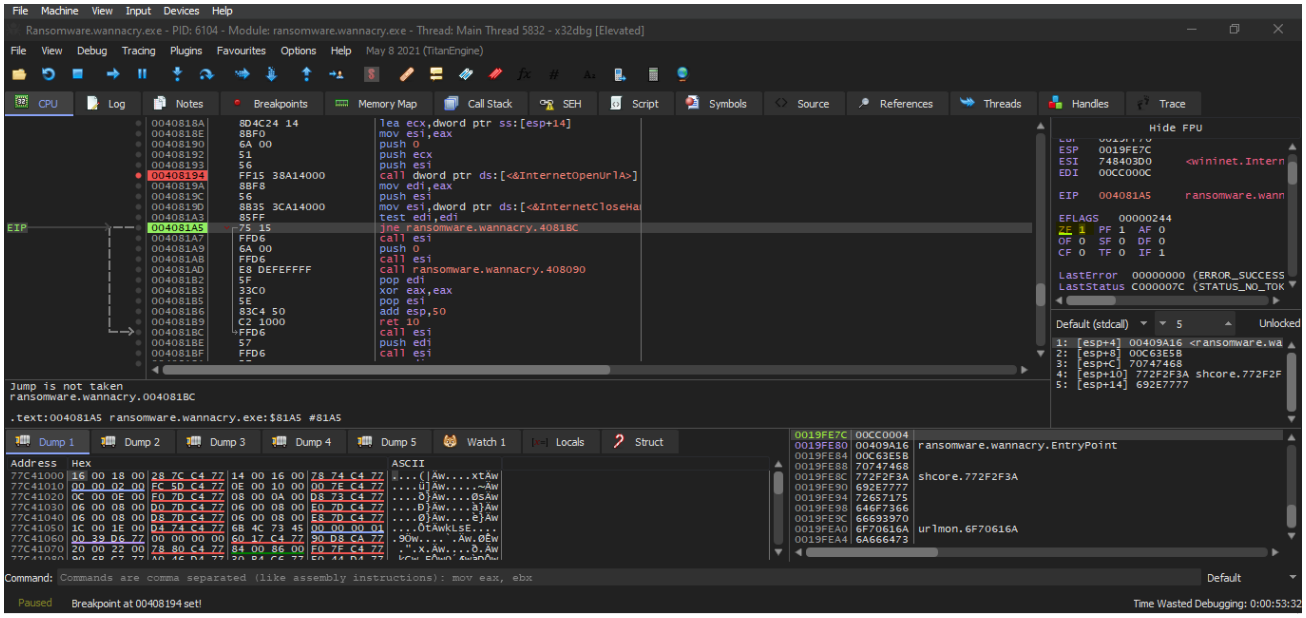


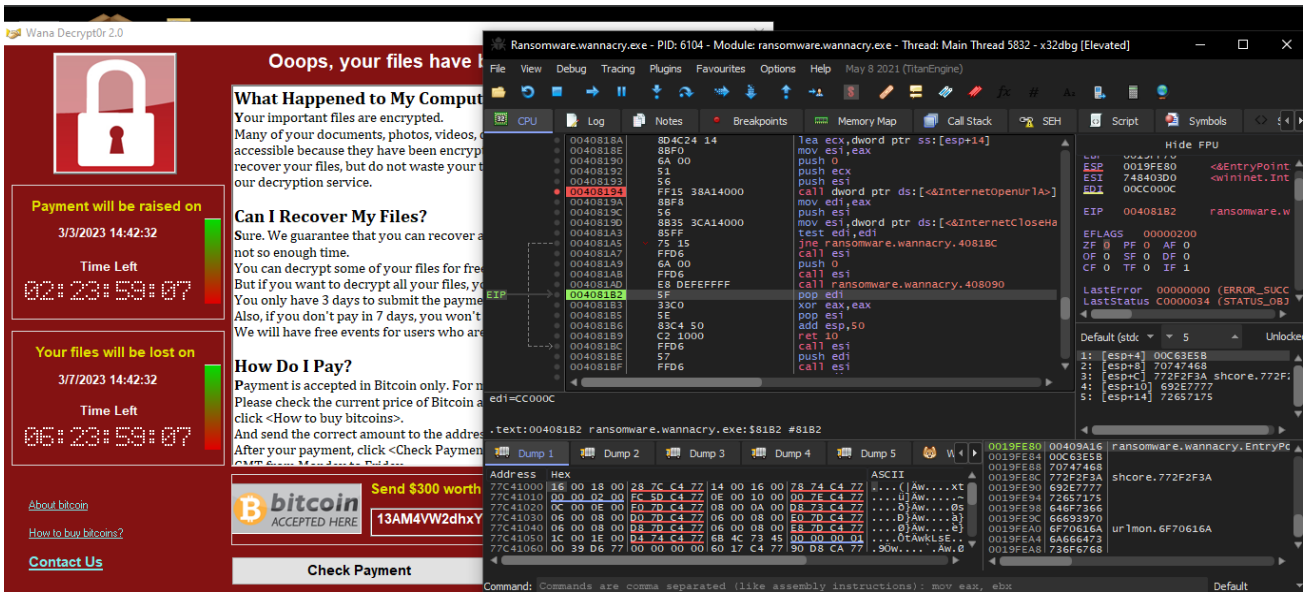


Connection successfully established



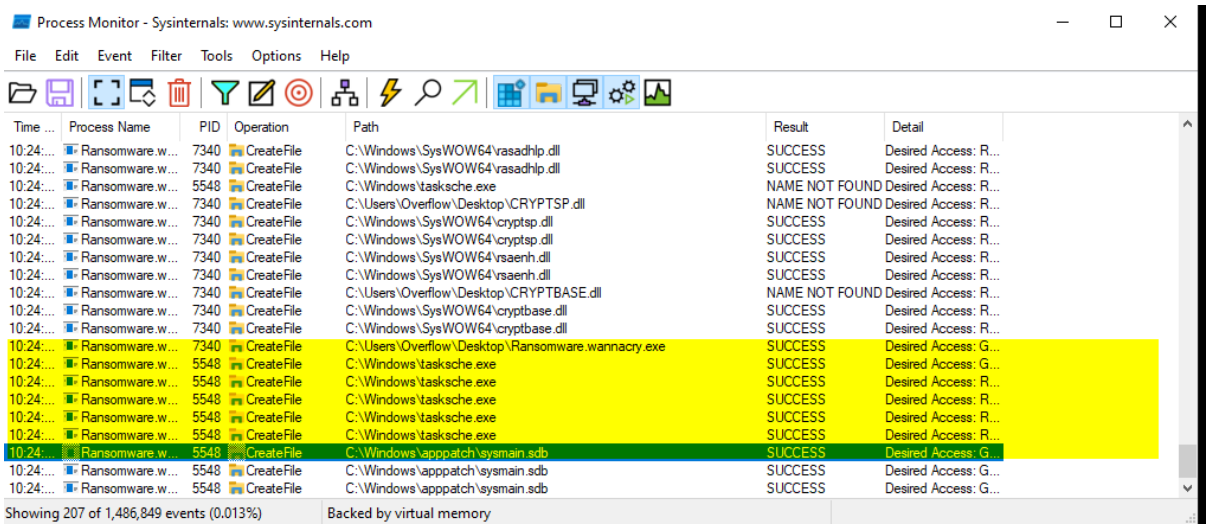
Let's change the zf value to 1
PS => zf => 1 => the value is 0 means we haven't reached out the Url

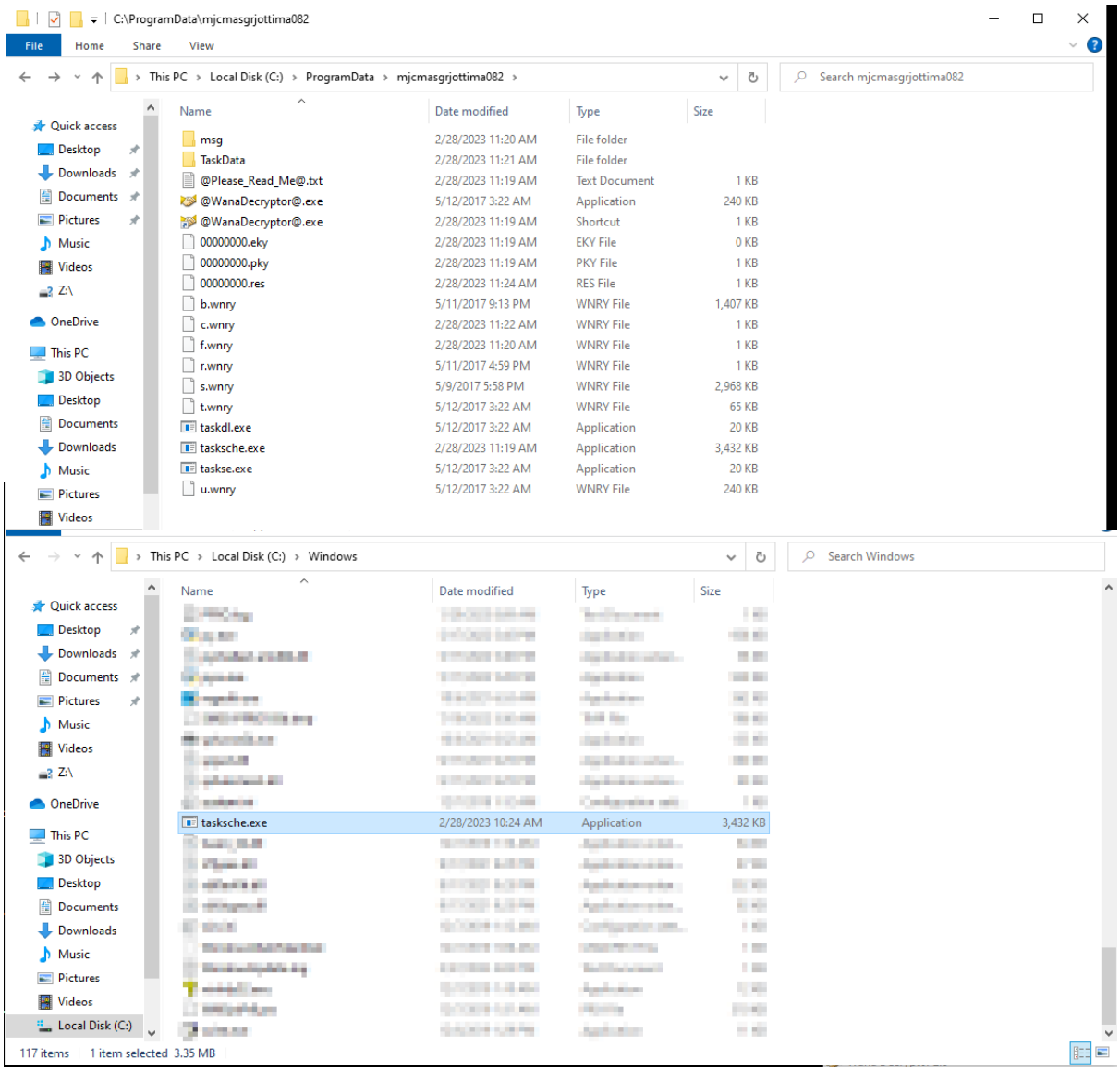


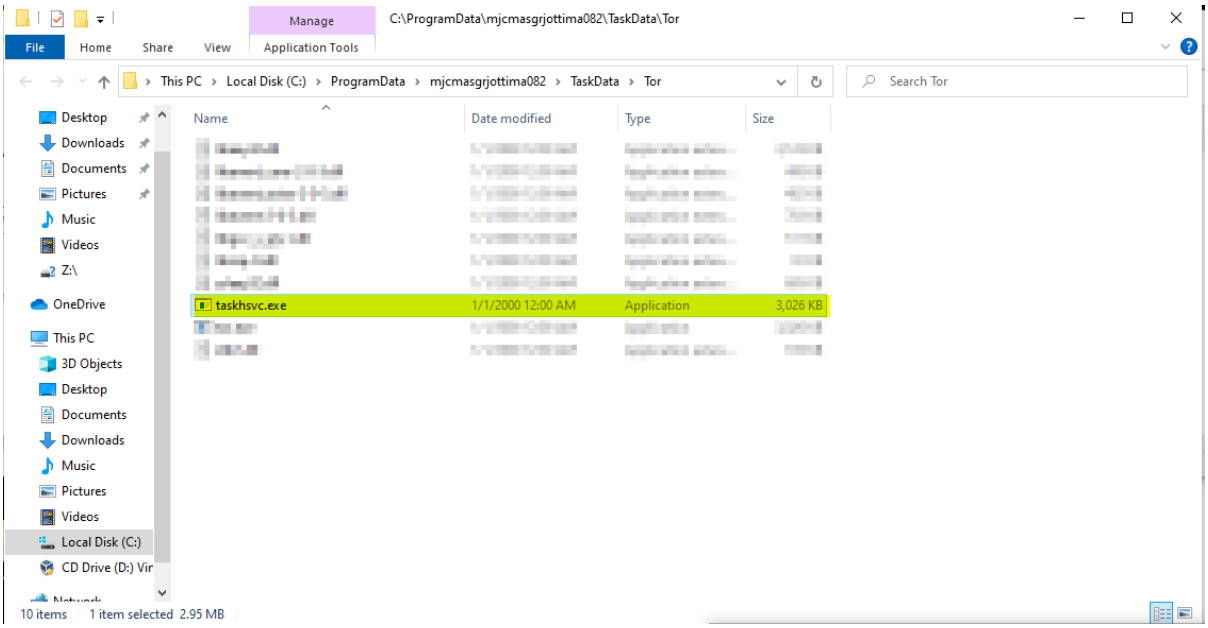


Indicators of Compromise

1- file creation :

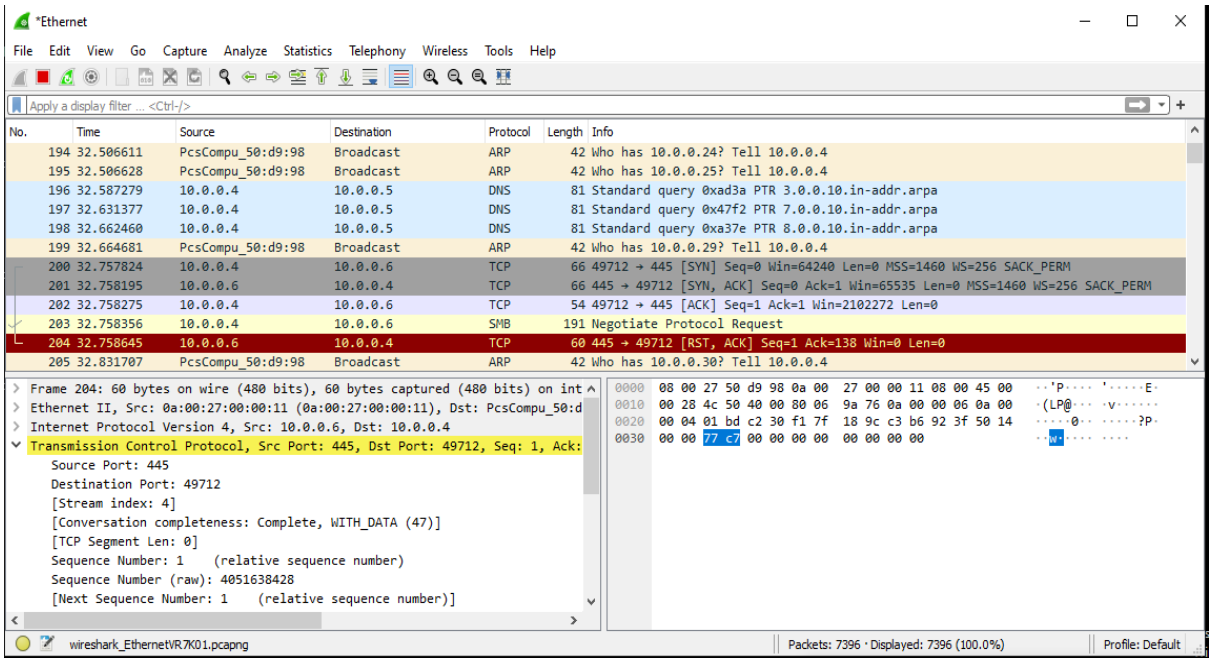



C:\ProgramData\mjcmasgrjottima082
File
Home
Share
View
This PC › Local Disk (C:) › ProgramData › mjcmasgrjottima082 ›
Search mjcmasgrjottima082
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
Z:\
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Name
Date modified
Type
Size
msg 2/28/2023 11:20 AM File folder
TaskData 2/28/2023 11:21 AM File folder
@Please_Read_Me@.txt 2/28/2023 11:19 AM Text Document 1 KB
@WanaDecryptor@.exe 5/12/2017 3:22 AM Application 240 KB
@WanaDecryptor@.exe 2/28/2023 11:19 AM Shortcut 1 KB
00000000.eky 2/28/2023 11:19 AM EKY File 0 KB
00000000.pky 2/28/2023 11:19 AM PKY File 1 KB
00000000.res 2/28/2023 11:24 AM RES File 1 KB
b.wnry 5/11/2017 9:13 PM WNRY File 1,407 KB
c.wnry 2/28/2023 11:22 AM WNRY File 1 KB
f.wnry 2/28/2023 11:20 AM WNRY File 1 KB
r.wnry 5/11/2017 4:59 PM WNRY File 1 KB
s.wnry 5/9/2017 5:58 PM WNRY File 2,968 KB
t.wnry 5/12/2017 3:22 AM WNRY File 65 KB
taskdl.exe 5/12/2017 3:22 AM Application 20 KB
tasksche.exe 2/28/2023 11:19 AM Application 3,432 KB
taskse.exe 5/12/2017 3:22 AM Application 20 KB
u.wnry 5/12/2017 3:22 AM WNRY File 240 KB
This PC › Local Disk (C:) › Windows
Search Windows
tasksche.exe 2/28/2023 10:24 AM Application 3,432 KB
Local Disk (C:)
117 items
1 item selected 3.35 MB

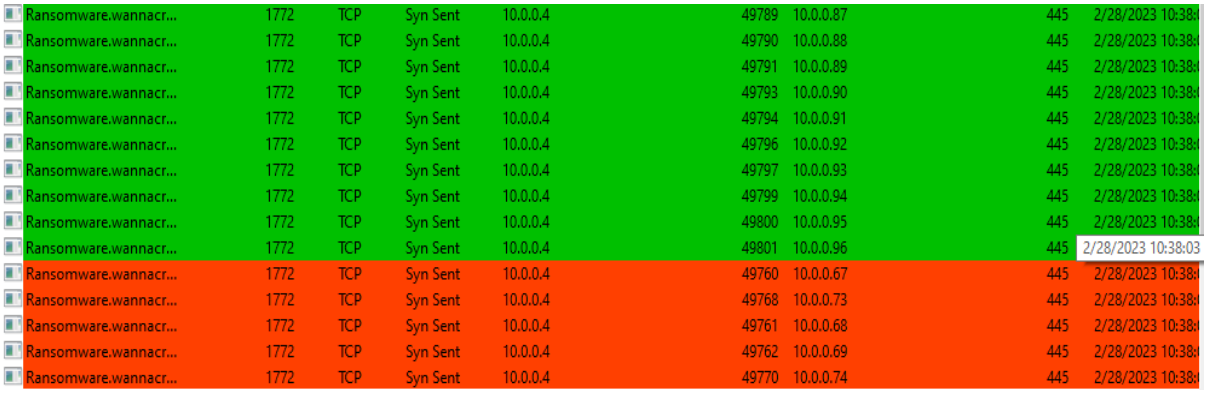


WannaCry Ransomware
Feb 2023
v1.0

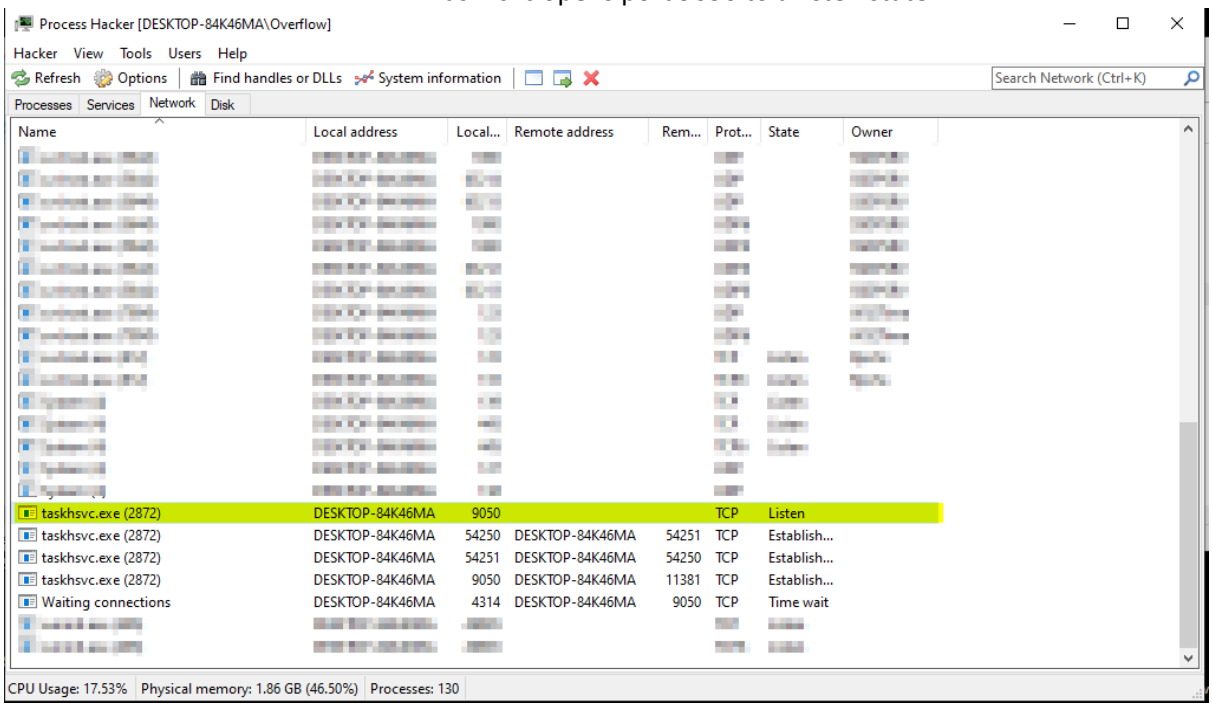
2- Network



The malware tries to spread itself over the network, the attack uses SMB and TCP port 445 to propagate



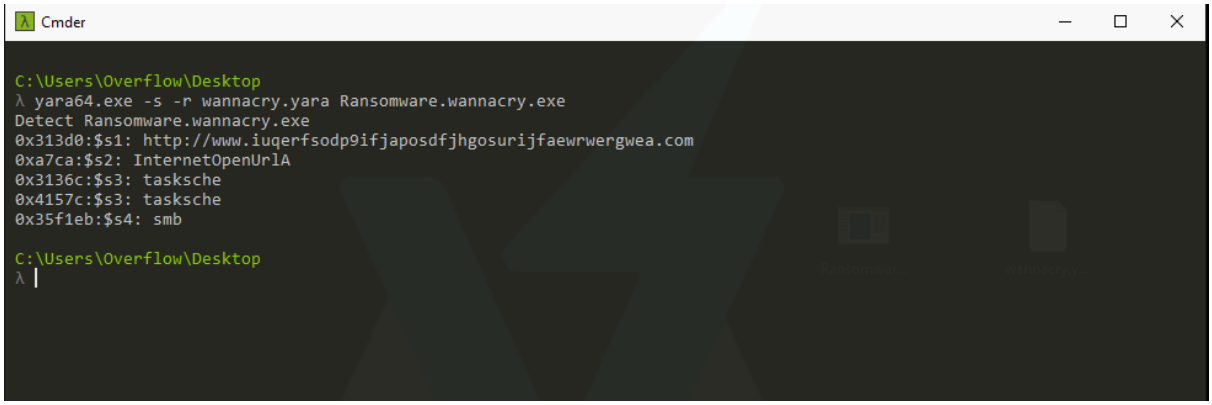
Taskhsvc opens port 9050 to a listen state



Rules & Signatures

```
rule Detect
        {
            meta:
                    description = "Detect wannacry"
            strings:
                    $s1 =
"http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com"
                    $s2 = "InternetOpenUrlA"
                    $s3 = "tasksche"
                    $s4 = "smb"
            condition:
                (all of them)

                    }
```



WannaCry Ransomware
Feb 2023
v1.0