Malware Analysis Report

WannaCry Malware

July 2022 | Jyotishman Deka

Basic Static Analysis

md5sum hash	24D004A104D4D54034DBCFFC2A4B19A11F39008A5 75AA614EA04703480B1022C

-md5sum.exe

Strings – Extracted using Floss

```
floss -n 6 Ransomware.wannacry.exe.malz > floss.txt
```

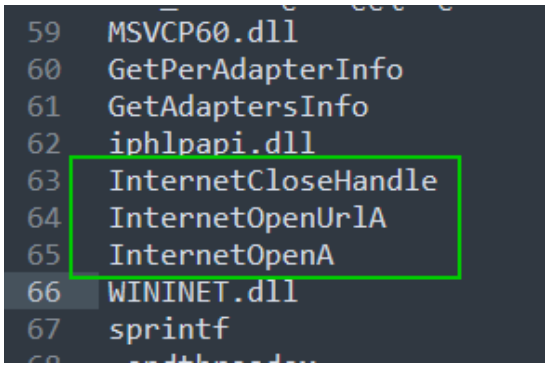


Fig 1: Modules used to open a URL

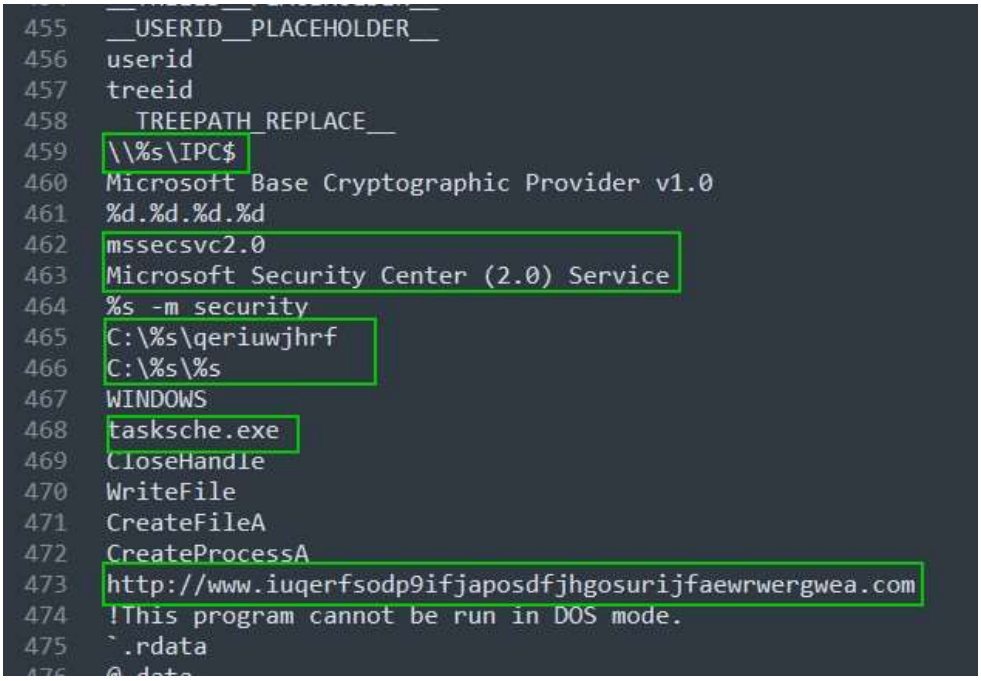


Fig 2: Service names used, Kill Switch URL and random paths

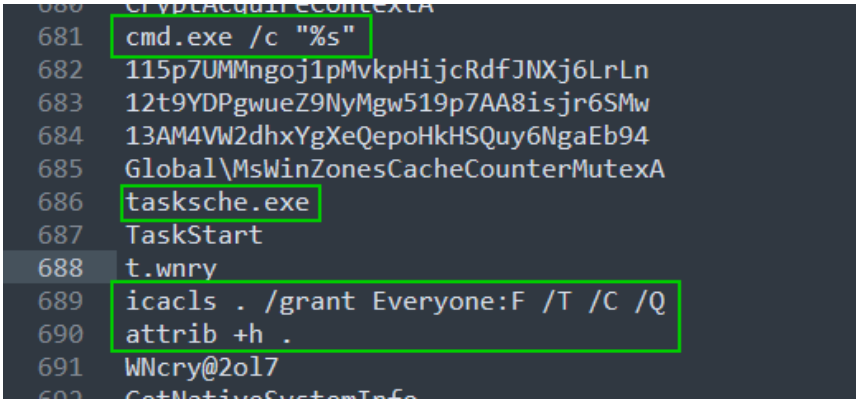
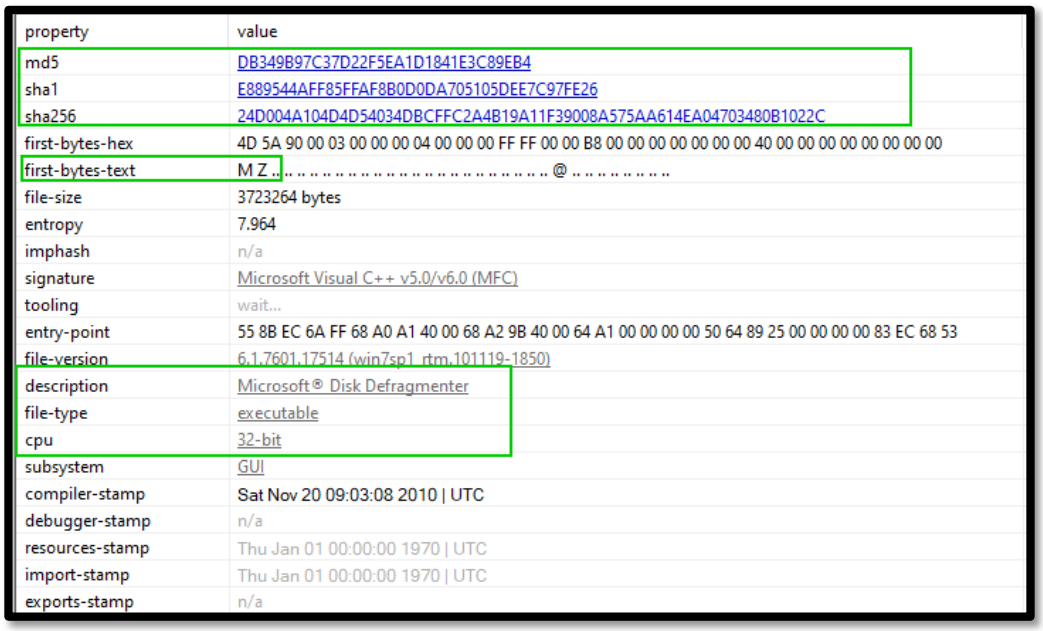


Fig 3: Service names used, random paths
icacls used for modifying access controls on files
attrib +h . used to hide the file attribute

PEStudio



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++ v5.0/v6.0 (MFC)
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	Thu Jan 01 00:00:00 1970 | UTC
import-stamp	Thu Jan 01 00:00:00 1970 | UTC
exports-stamp	n/a

Fig 4: Basic Information about the executable

Basic Dynamic Analysis

Analysis with inetsim turned on

When the malware is executed with inetsim turned on, the malware does not execute. It tries to connect to "hxxp://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com". On successful connection it does not infect the system.

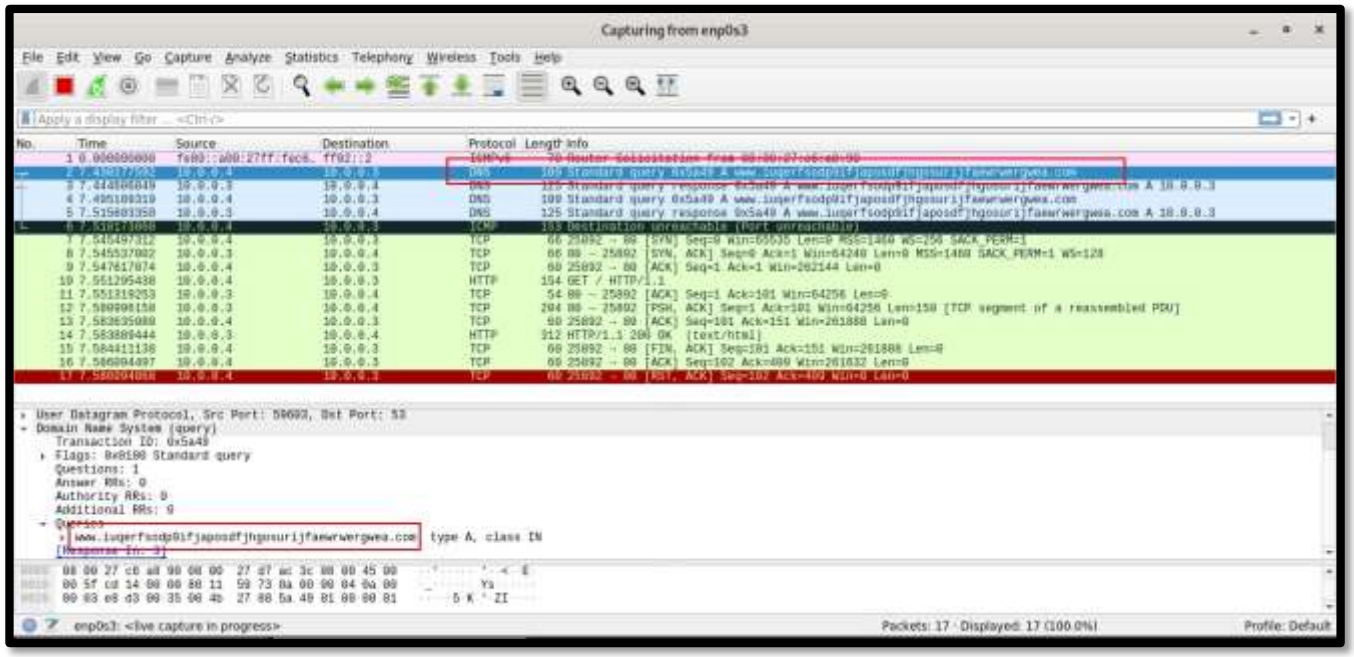


Fig 5: Network traffic when malware is executed

Analysis with inetsim turned off

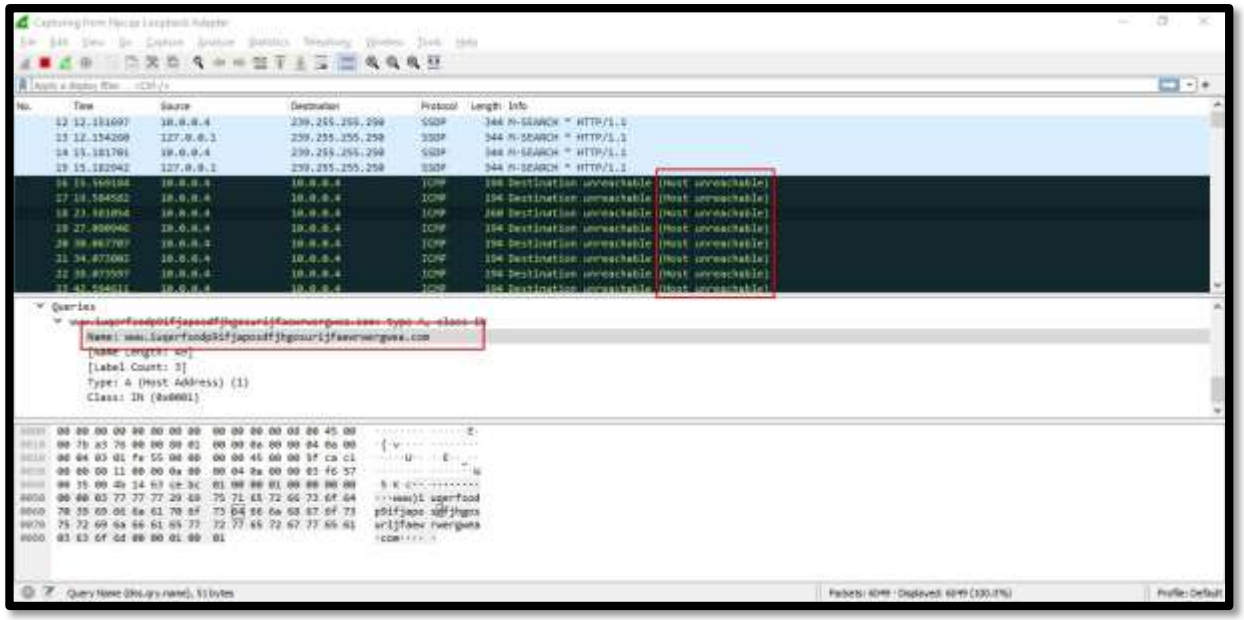


Fig 6: Network traffic when malware is executed. The requests are unreachable because inetsim is turned off

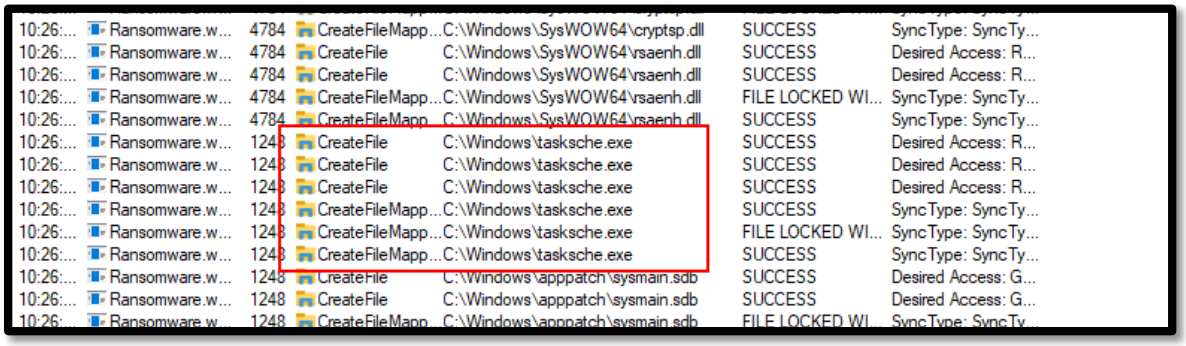


Fig 7: Procmon analysis. Creation of tasksche.exe file

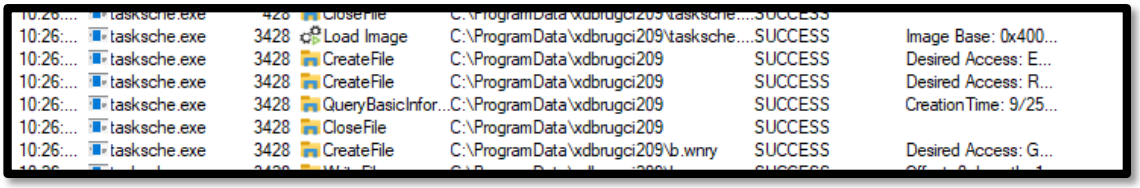


Fig 8: Wannacry creates tasksche.exe and executes it. Tasksche.exe creates a file with a random name in C:\ProgramData\{random name}. This folder is a staging area for wannacry ransomware

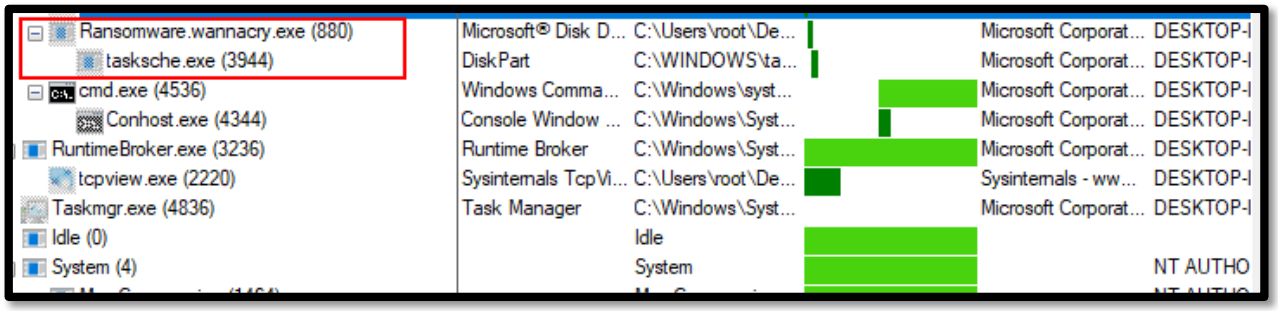


Fig 9: Procmon process tree

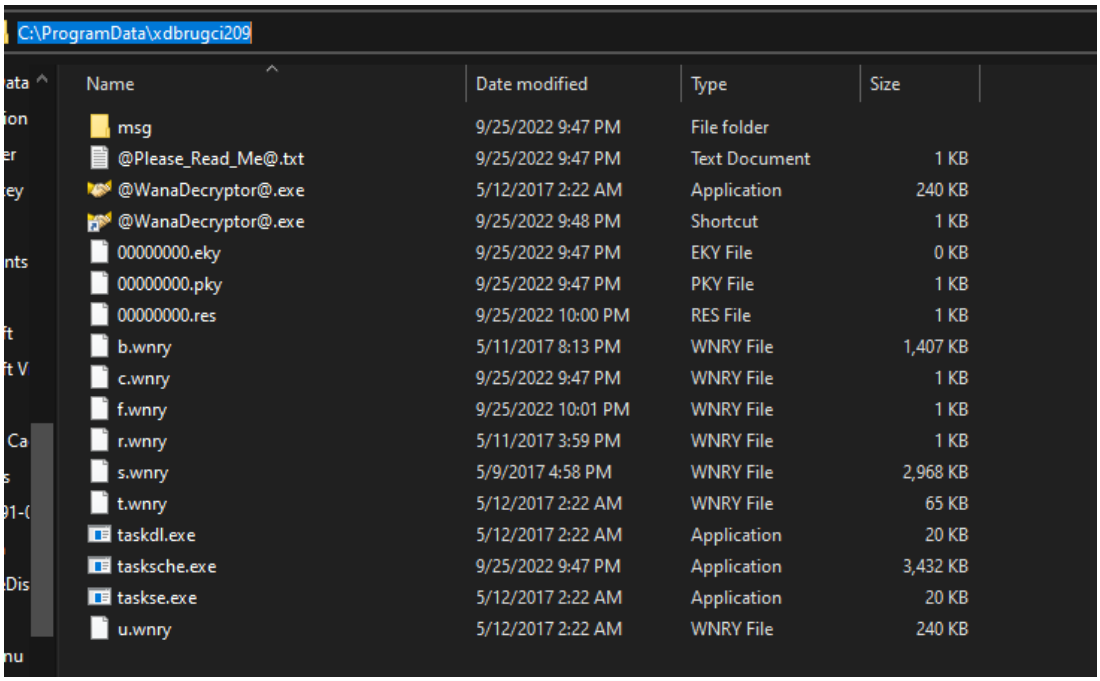


Fig 10: C:\ProgramData\{random name} folder which is staging area for wannacry

Fig 11: Task Manager. Service name is same as the random file name created by tasksche.exe

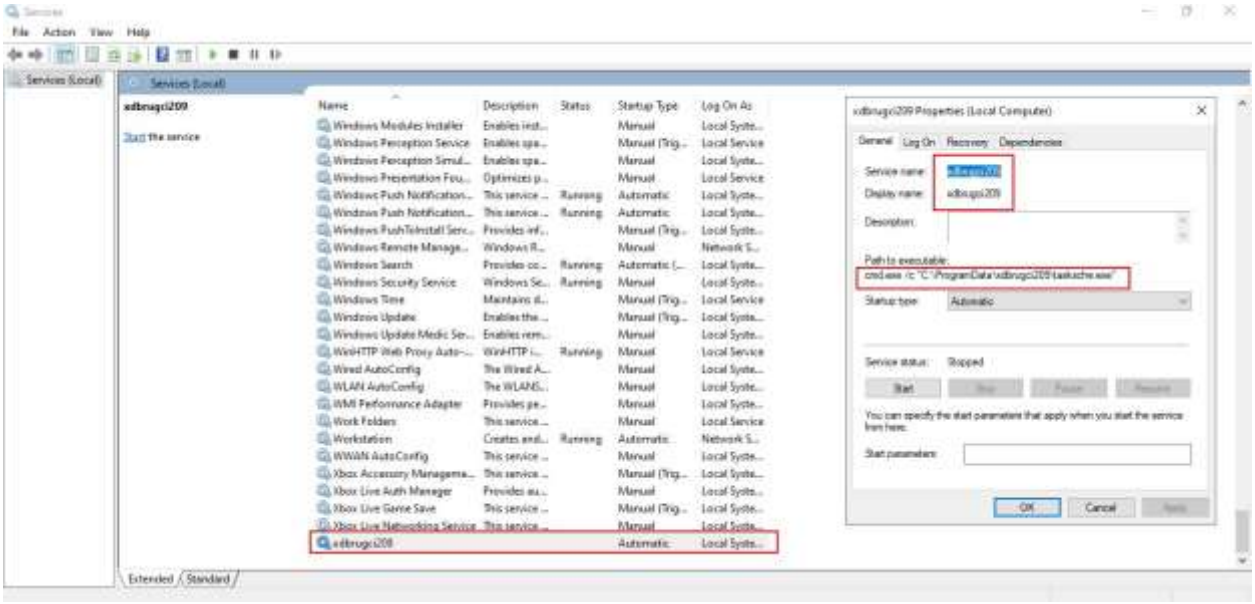


Fig 12: Service. Service name is same as the random file name created by tasksche.exe. This service just invokes the tasksche.exe command on startup.

Fig 13: After Infection. Ransom message

Advanced Static Analysis

Cutter

Fig 14: Main function viewed inside cutter graph mode

Advanced Dynamic Analysis

X32dbg

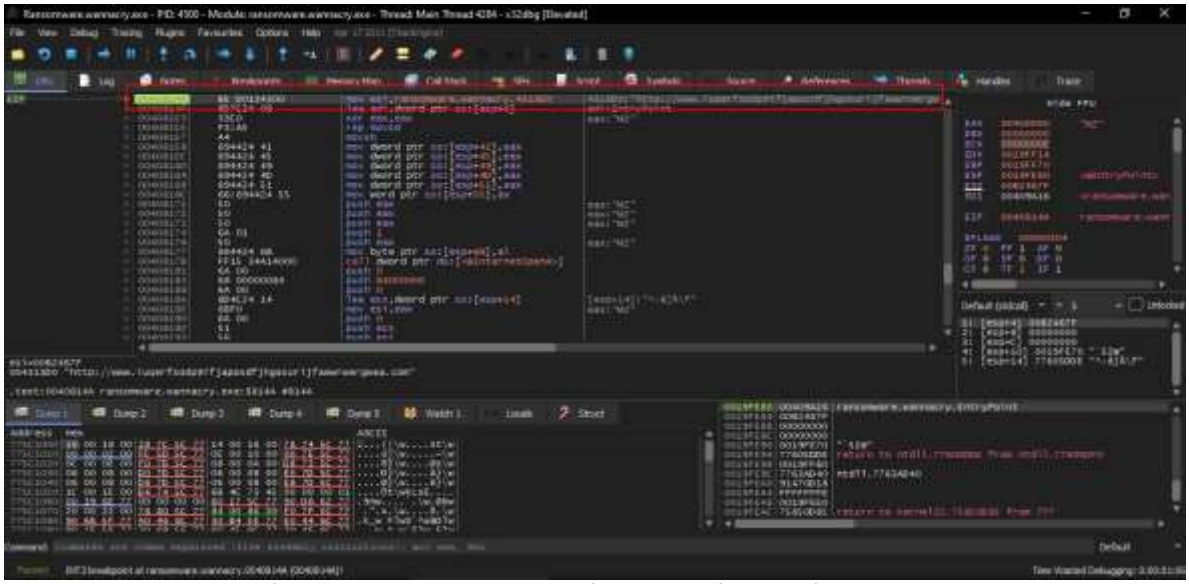


Fig 15: Set a breakpoint on kill switch URL

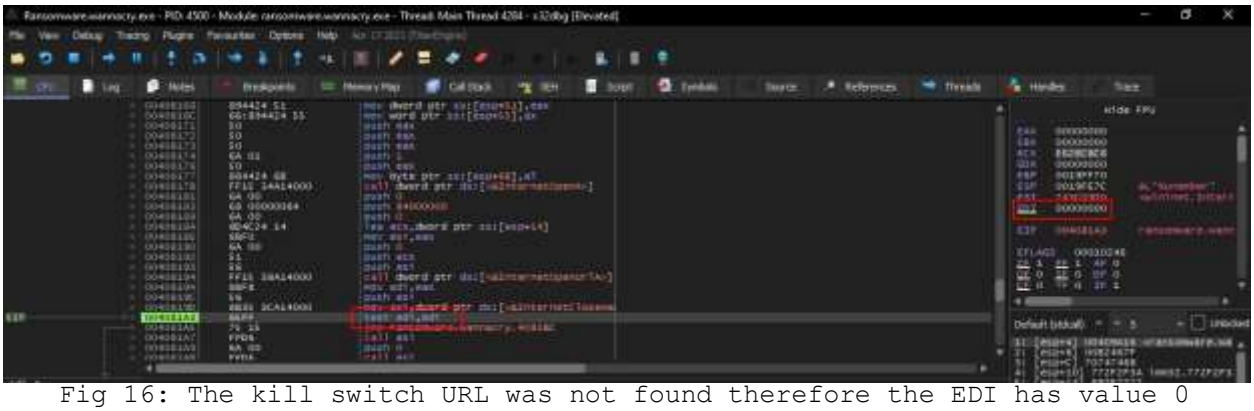


Fig 16: The kill switch URL was not found therefore the EDI has value 0

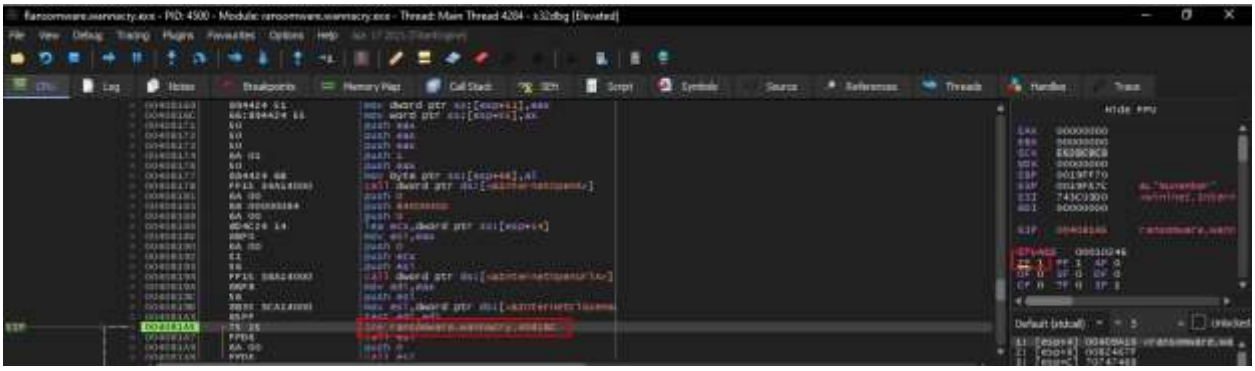


Fig 17: The zero flag is evaluated to 1 but we change it to 0

Fig 18: Changing the zero flag to 0. This makes the program to take the jump call and the malware is not executed.

Recommendations for organizations to become more resilient against wannacry malware:

1.Keep Systems Updated: Regularly apply security patches and updates for operating systems, software, and applications. Vulnerabilities often arise from outdated software versions, so timely updates can help mitigate the risk.
2.Use Reliable Security Software: Deploy reputable antivirus and anti-malware solutions across your organization's network. Ensure that the software is regularly updated and configured to perform real-time scanning.
3.Network Segmentation: Implement network segmentation to isolate critical systems and data from the broader network. By segmenting your network, you limit the lateral movement of malware in case of an infection, containing the impact.
4.Least Privilege Principle: Enforce the principle of least privilege, granting users only the necessary permissions required to perform their duties. Restrict administrative privileges to reduce the potential impact of malware and limit unauthorized access.
5.User Awareness Training: Conduct regular security awareness training for all employees. Teach them about the risks associated with opening suspicious emails, clicking on unknown links, or downloading files from untrusted sources. Emphasize the importance of vigilance and reporting any suspicious activities.
6.Regular Data Backups: Implement a robust backup strategy that includes regular backups of critical data. Ensure backups are stored securely and tested periodically to ensure data can be restored effectively in case of an incident.

7.Disable Unnecessary Services: Disable or uninstall unnecessary services and protocols to reduce the attack surface. Unused or outdated services can often serve as entry points for malware attacks.

8.Regular Vulnerability Assessments and Penetration Testing: Conduct regular vulnerability assessments and penetration testing to identify weaknesses in your network and systems. Address any discovered vulnerabilities promptly to minimize the risk of exploitation.