Icon

Description automatically generated

Practical Malware Analysis

Report By

**Nagunoori Prabhath Chandra**

**Chandraprabhath123@gmail.com**

**+91 6300764712**

# Table of Contents

[Executive summary 5](file:///C:\Users\pavan\AppData\Local\Microsoft\Windows\INetCache\IE\0FT6893A\PRACTICAL%20MALWARE%20ANALYSIS%20REPORT%5b2%5d.docx#_Toc85207996)

[Malware.Unknown.exe 5](file:///C:\Users\pavan\AppData\Local\Microsoft\Windows\INetCache\IE\0FT6893A\PRACTICAL%20MALWARE%20ANALYSIS%20REPORT%5b2%5d.docx#_Toc85207997)

[RAT.Unknown.exe 5](file:///C:\Users\pavan\AppData\Local\Microsoft\Windows\INetCache\IE\0FT6893A\PRACTICAL%20MALWARE%20ANALYSIS%20REPORT%5b2%5d.docx#_Toc85207998)

# Executive Summary

This report Summarises the penetration test that was conducted by Prabhath chandra as an assignment for the Cyber Security Bootcamp, IARE. This report is an attempt at showcasing my skillset and methodology of conducting a Malware Analysis.

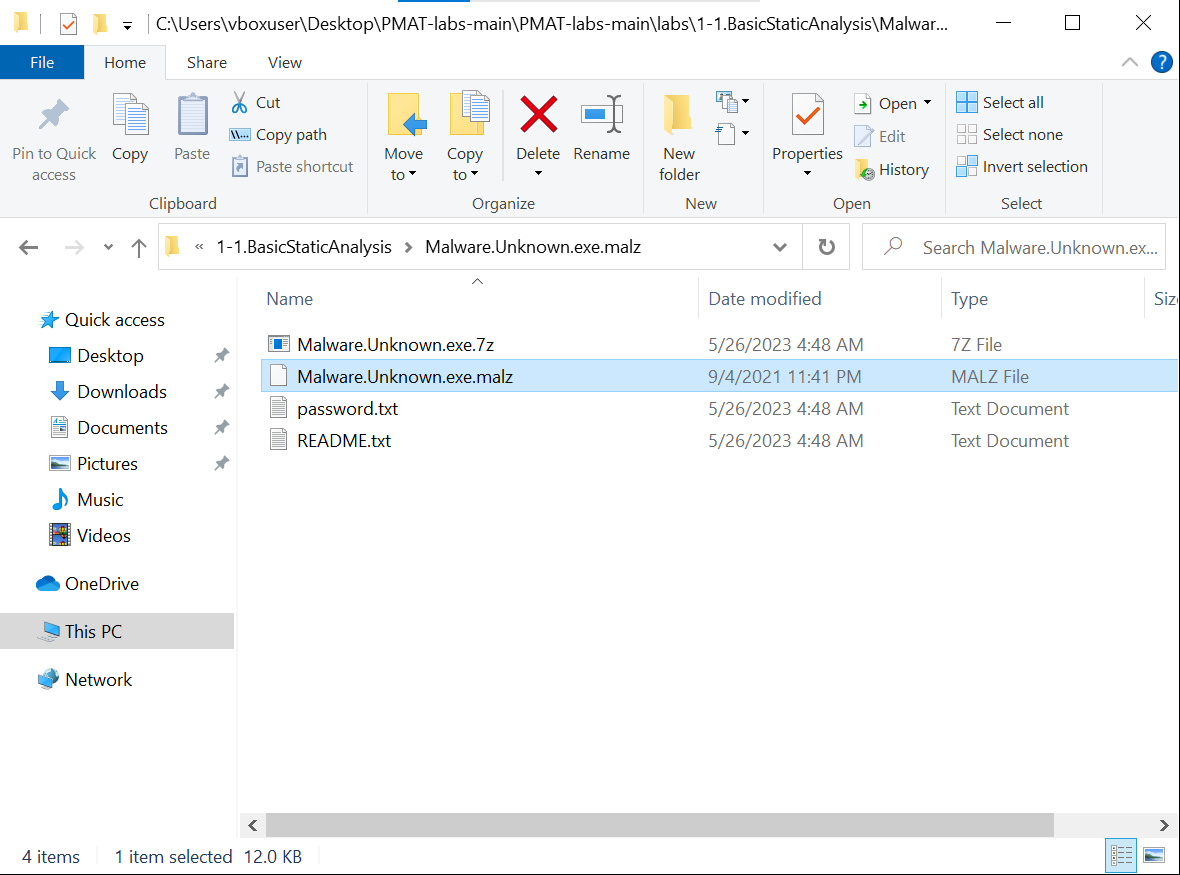
In the malware analysis, we encounter with two different types of malware analysis, static and dynamic analysis.

The Static Analysis states that the malware is examined without executing the malware whereas the Dynamic Analysis observes malware when it is being executed.

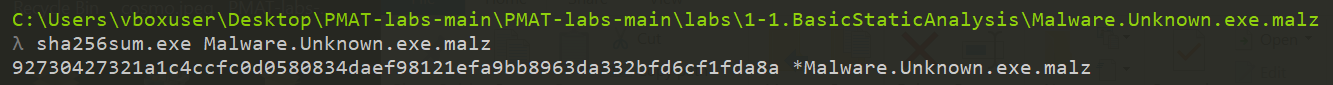
# Malware.Unknown.exe

# Basic Static Analysis

Static analysis is a method of debugging that is done by automatically examining the source code without having to execute the program. This provides developers with an understanding of their code base and helps ensure that it is compliant, safe, and secure.

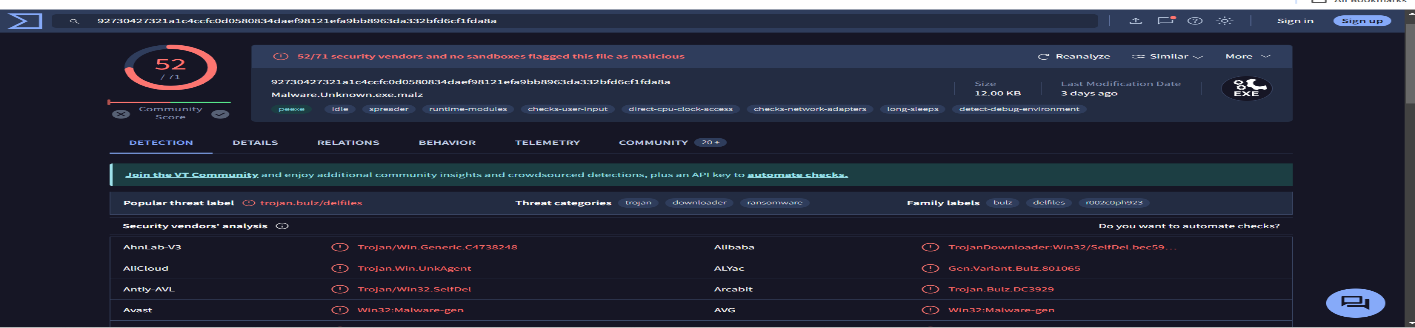
 To Perform basic static analysis, Firstly we have to extract the zip file “Malware.unknown.exe.7z ” into “Malware.unknown.exe.malz”.

Next step of malware analysis change malware file into hash key using the command “sha256sum.exe Malware.unknown.exe.malz” in the cmder.

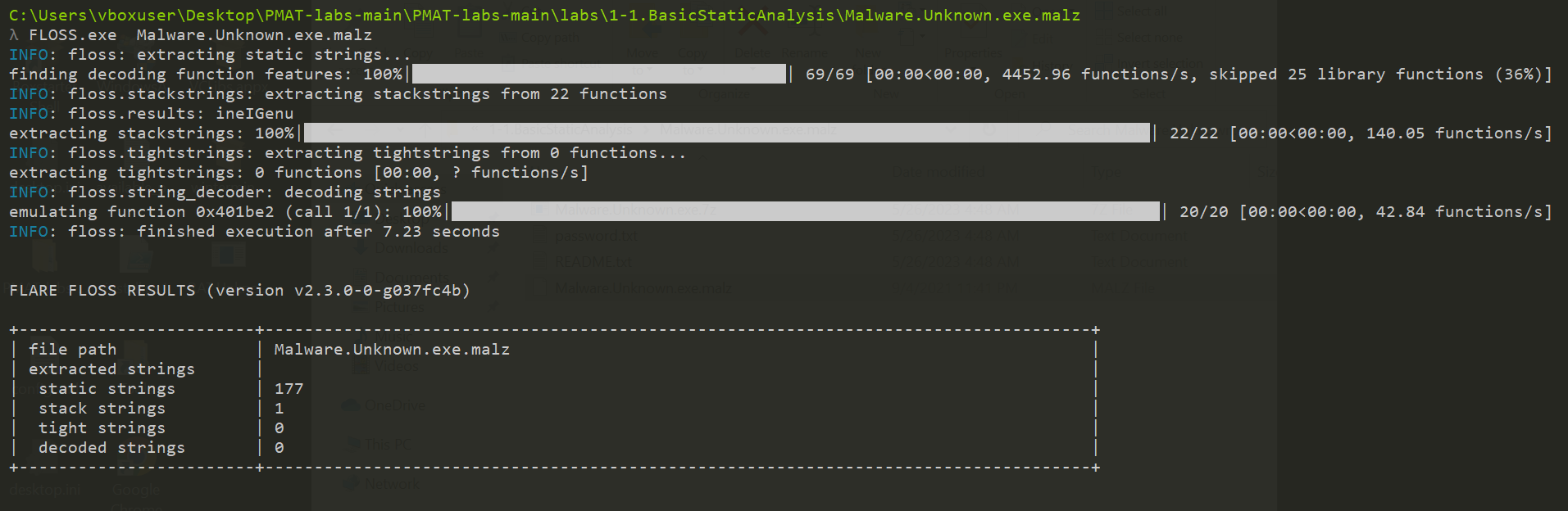


From above we can get the hash key, that hash key should be copied and place in the virus total website. Which detects the virus in the malware file.

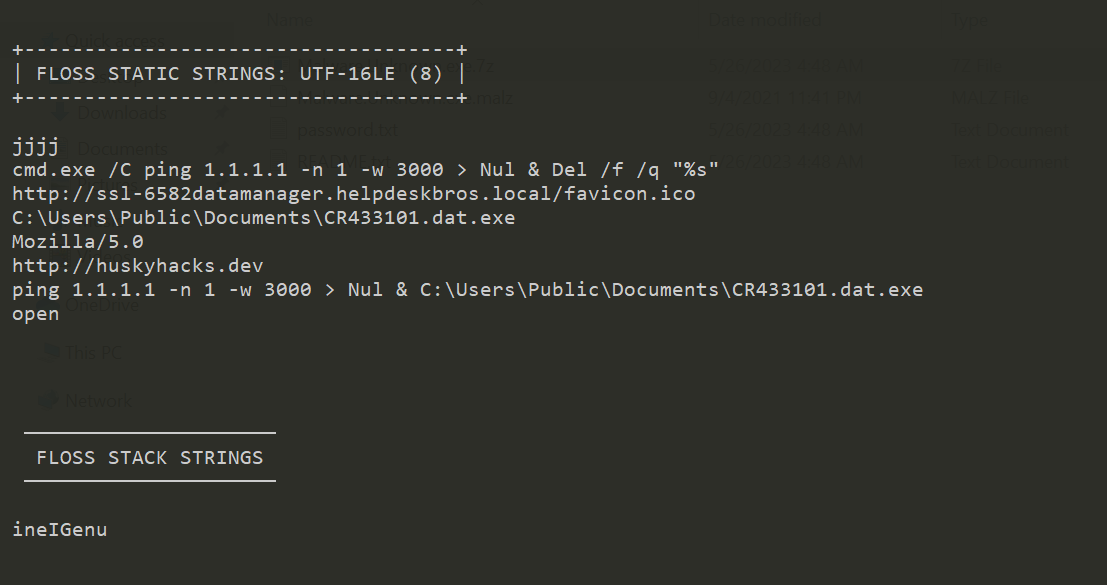
Virus Total is an online service that analyzes suspicious files and URLS to detect types of malware and malicious content using antivirus engines and website scanners.

****

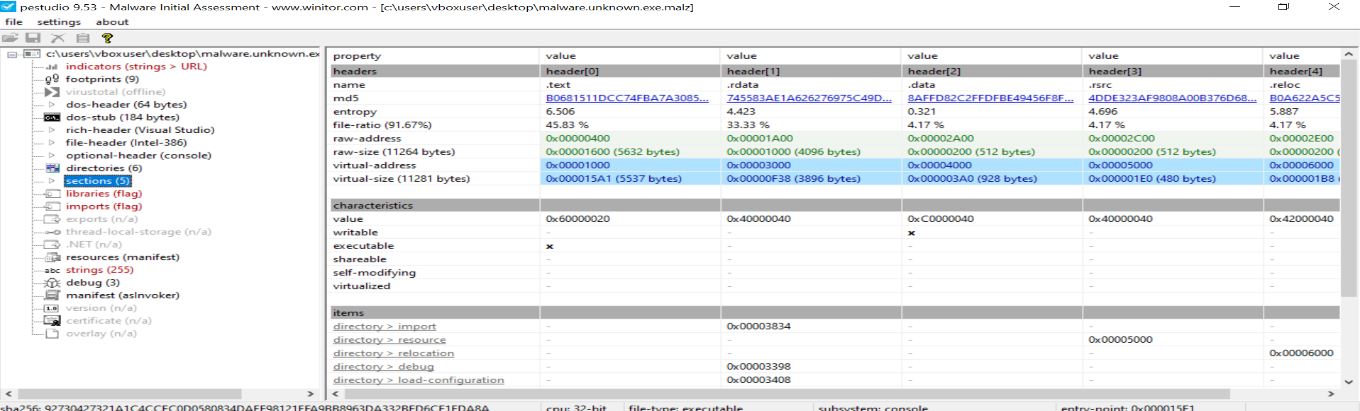
By using the virus total we got around 52 out of 71 virus has detected in our hash key.

 Next step we going to find out the suspicious strings in the malware file named “Malware.unknown.exe.malz” using the command “FLOSS.exe “Malware.unknown.exe.malz”.

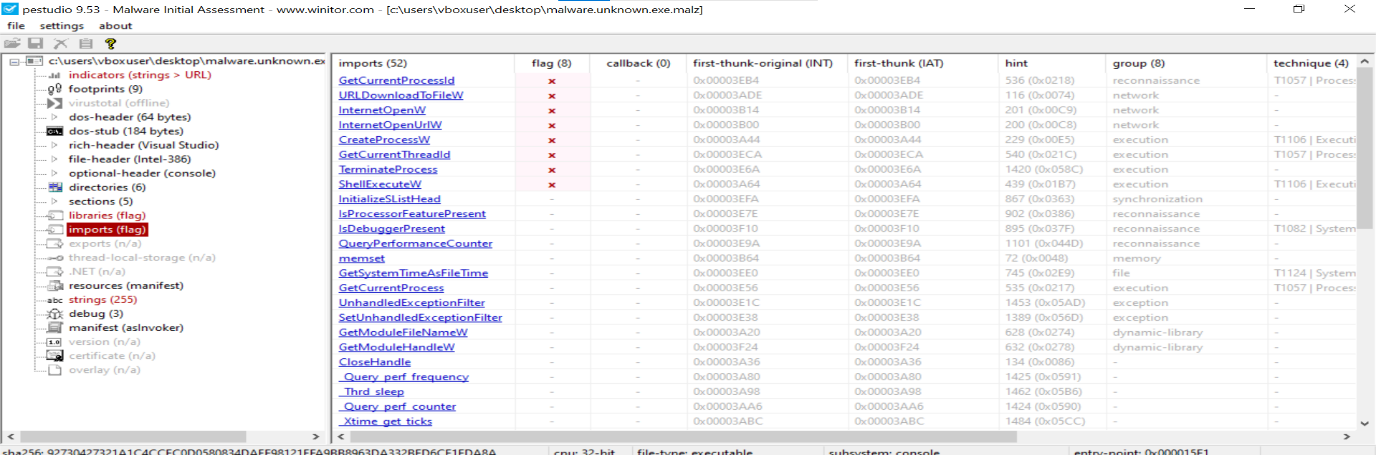
These are some strings which I got using the floss command.

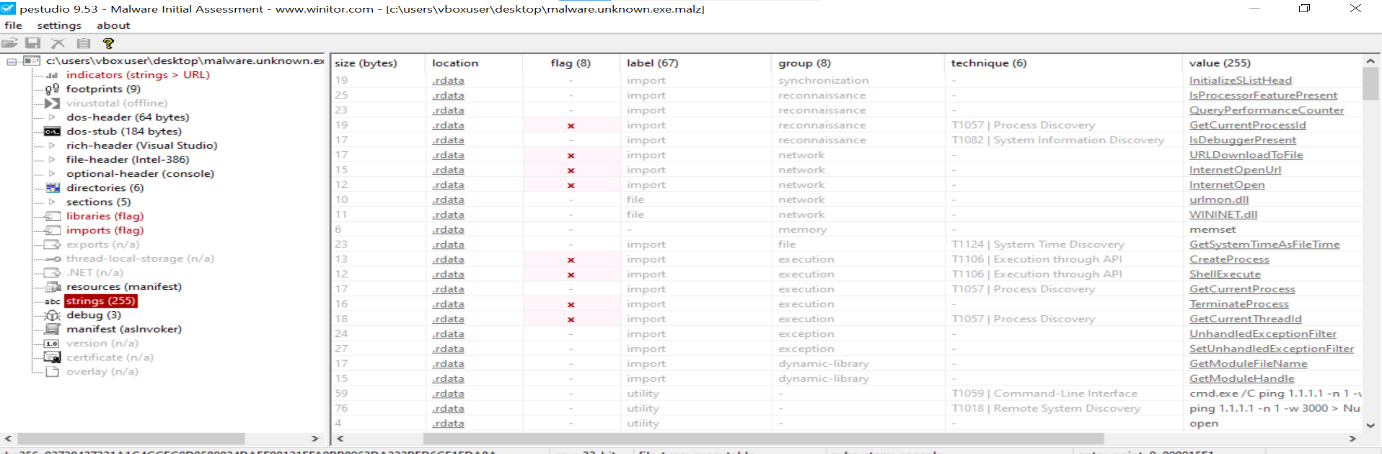


And next I performed static analysis using tool called “pestudio” which stands for portable executable studio. After opening tool open the malware file and start analyzing the malware file.



In imports I found some important flags in malware file.



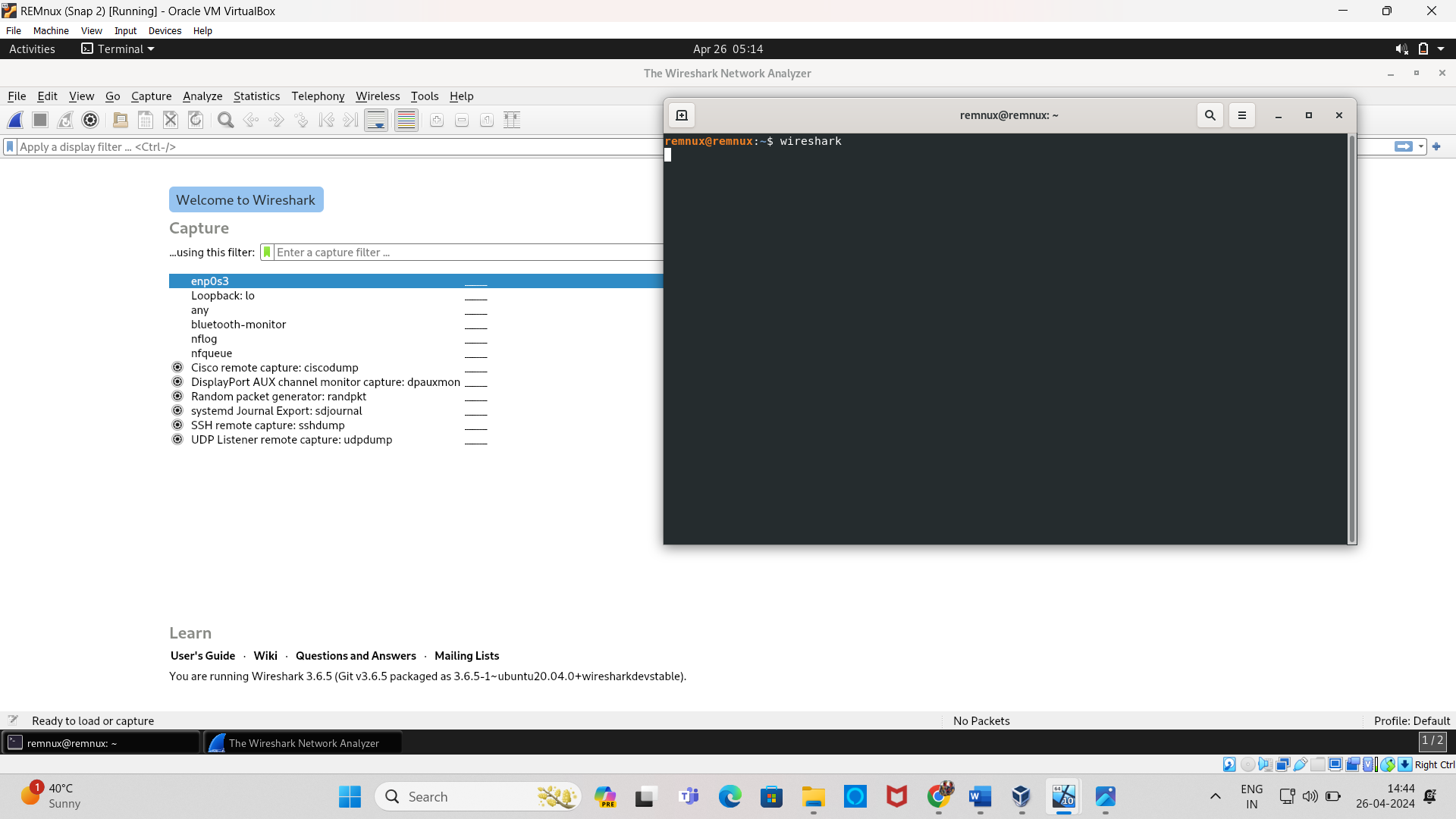
These are some strings which I got from strings section.

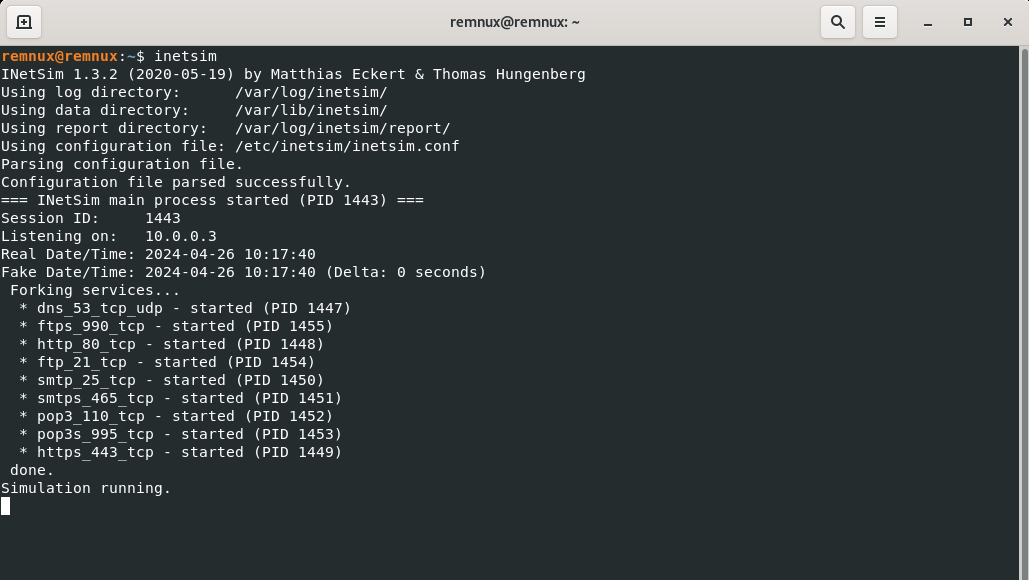
Hence, this the process of Basic static malware analysis.

# Basic Dynamic Analysis

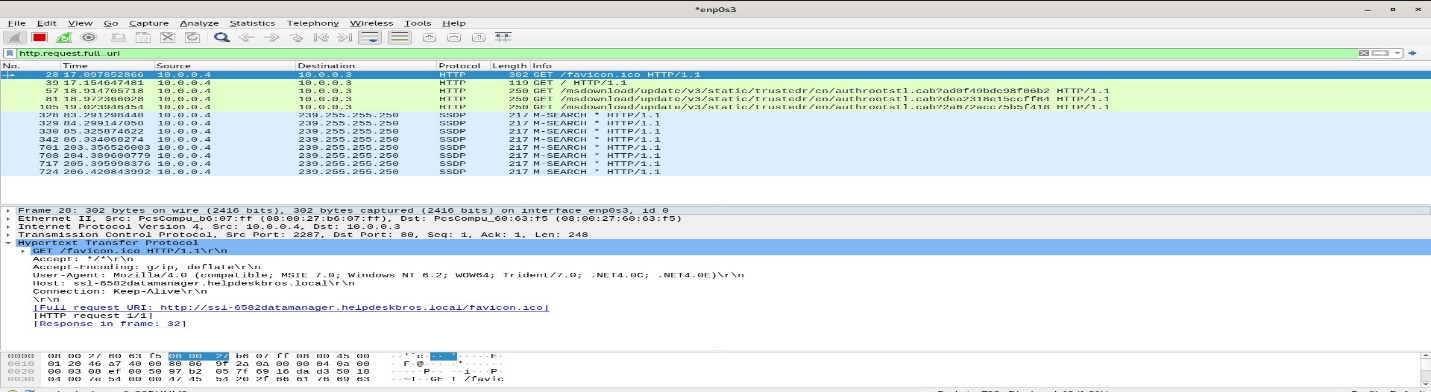
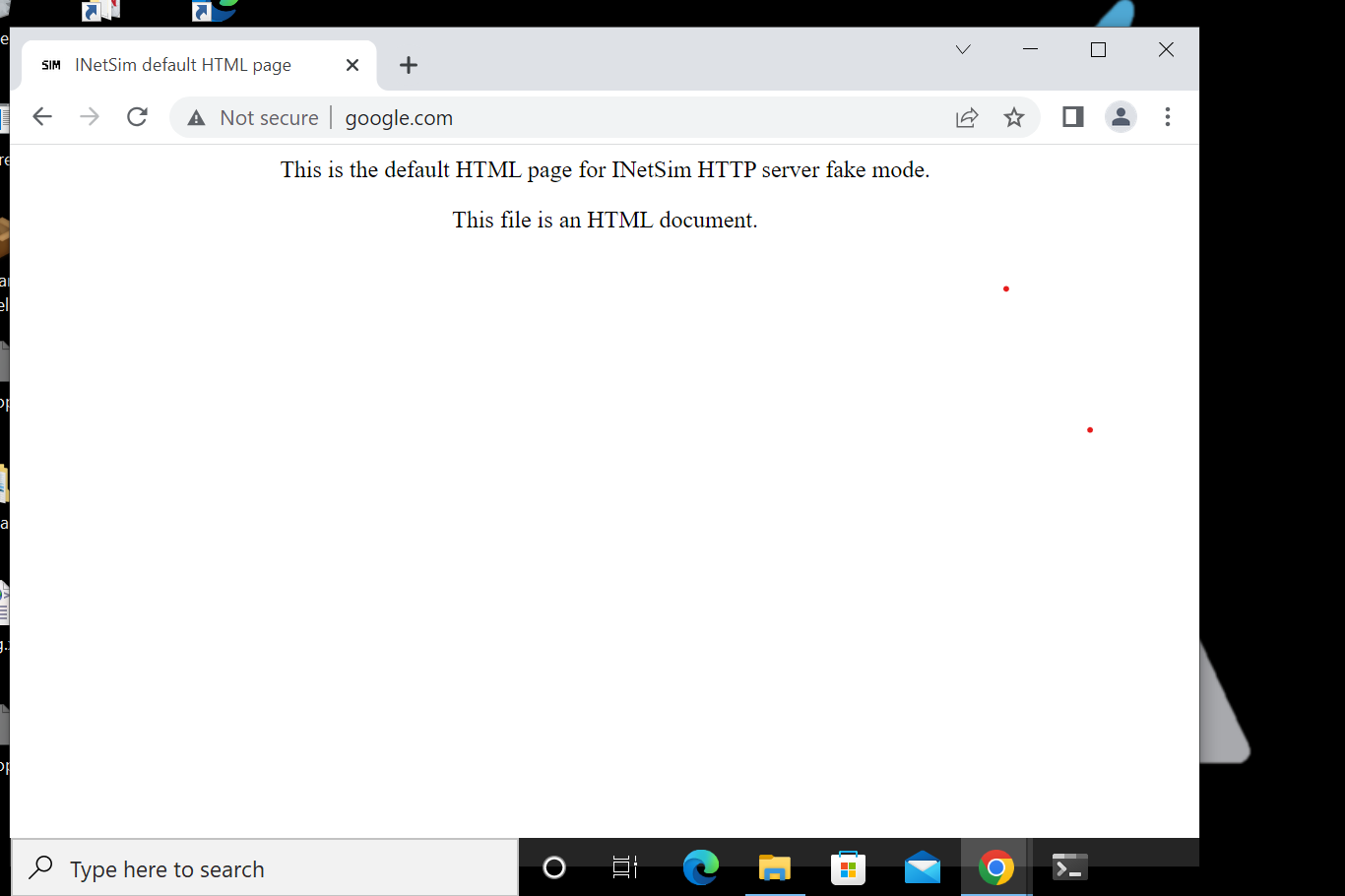
Dynamic analysis is the process of testing and evaluating a program—while software is running. Also referred to as dynamic code scanning, dynamic analysis improves the diagnosis and correction of bugs, memory issues, and crashes of an application during its execution.

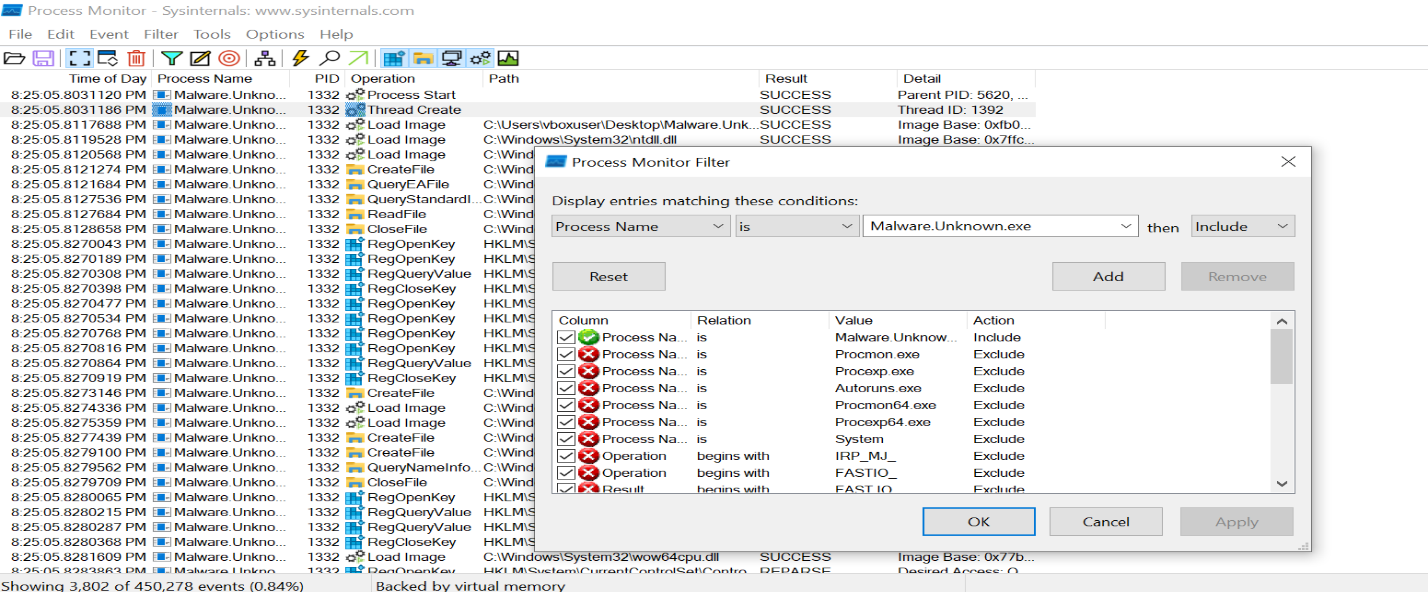
First step is to open wireshark which widely used, open source network analyzer that can capture and display real-time details of network traffic in the terminal of remnux machine using the command “Wireshark”.



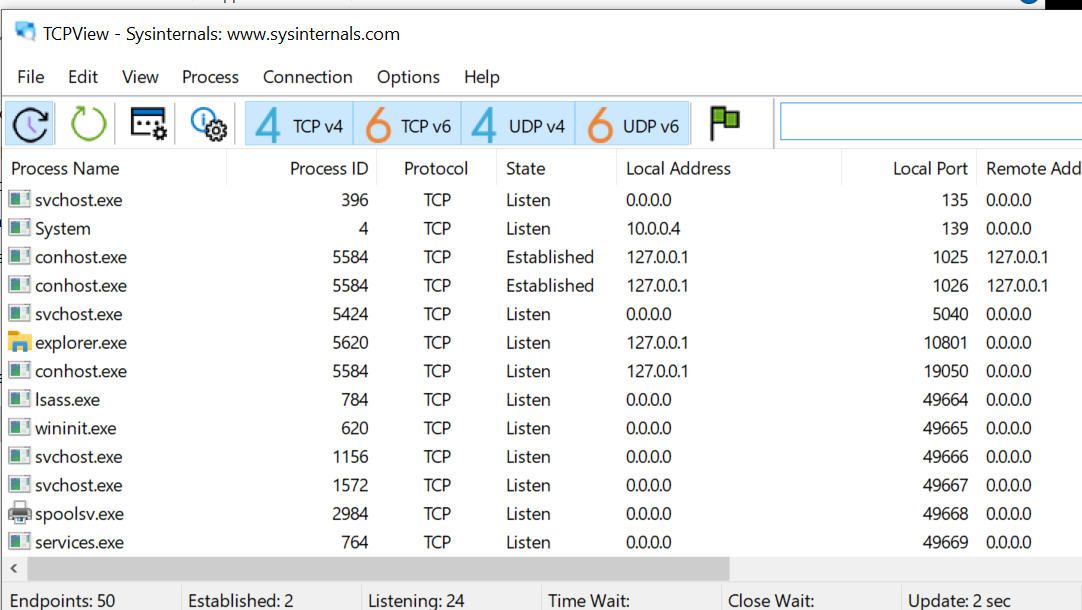
To Simulating the common internet services in lab environment we are going to run the internet services simulation in remnux machine terminal using the command “inetsim”.

To check the network services are working, Open the google chrome in the flareVM and search for something. Then you are going to get the Html page as in the screenshot below.

If this page opens that we can assume that the network services and working properly and Now open the Wireshark and filter top layers in the OSI like Http. Here are some suspicious stuff that I got from filter using http.

And next process in dynamic analysis is to open the tool called procmon in flareVM. Now use the filter option and try to filter the malware file as shown below. To know some suspicious files ,urls and paths.

And analyze the malware file using another tool called tcpview. And got some suspicious ip address in it.

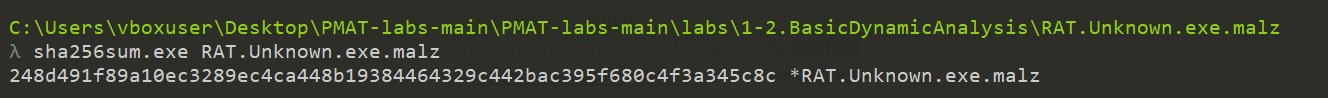


Hence, we can observe that the executed malware installs another piece of malware in the device.

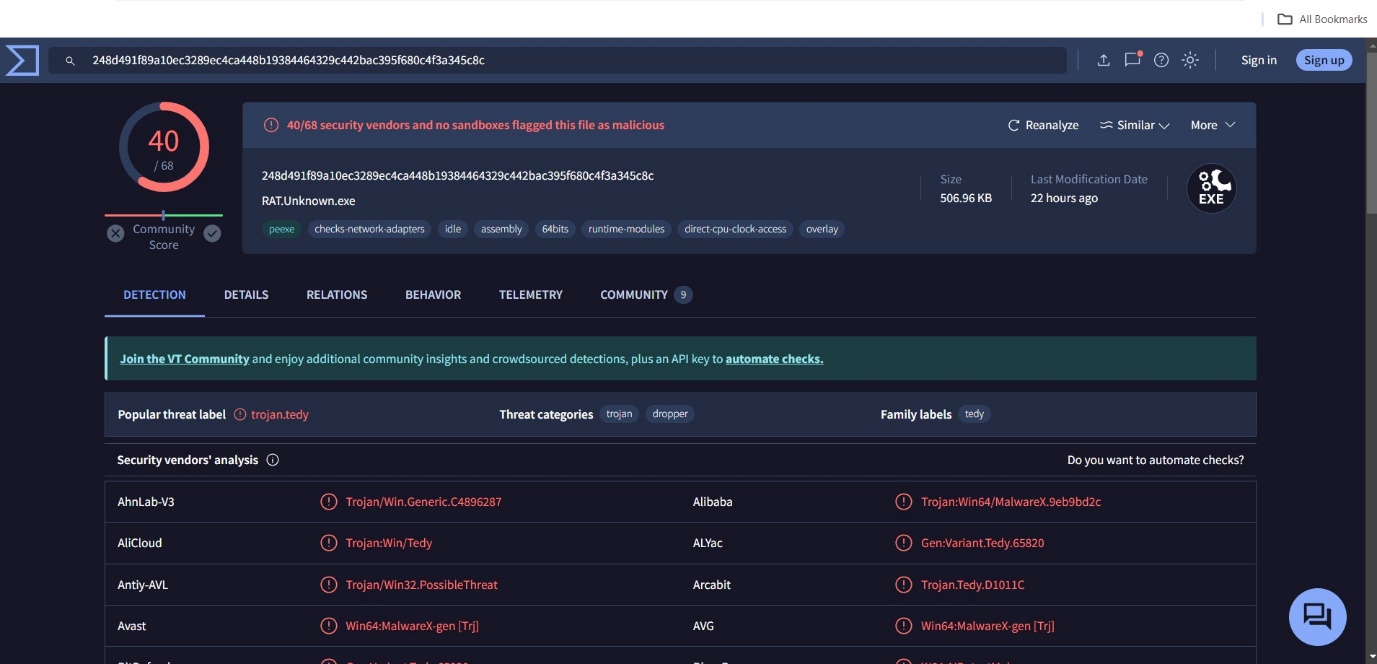
**RAT.Unknown.exe.malz**

# Basic Static Analysis

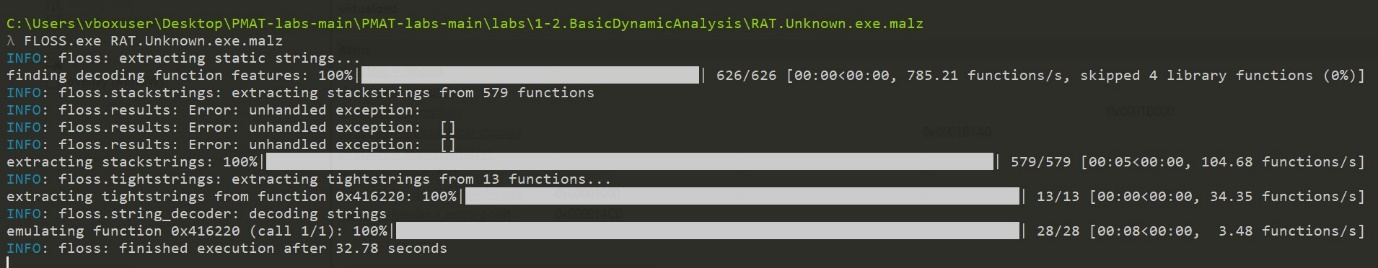
Extract the zip file “RAT.unknown.exe.malz.7z” into “RAT.unknown.exe.malz”. Next step is to change malware file into hash key using the command “sha256sum.exe RAT.unknown.exe.malz” in the cmder.

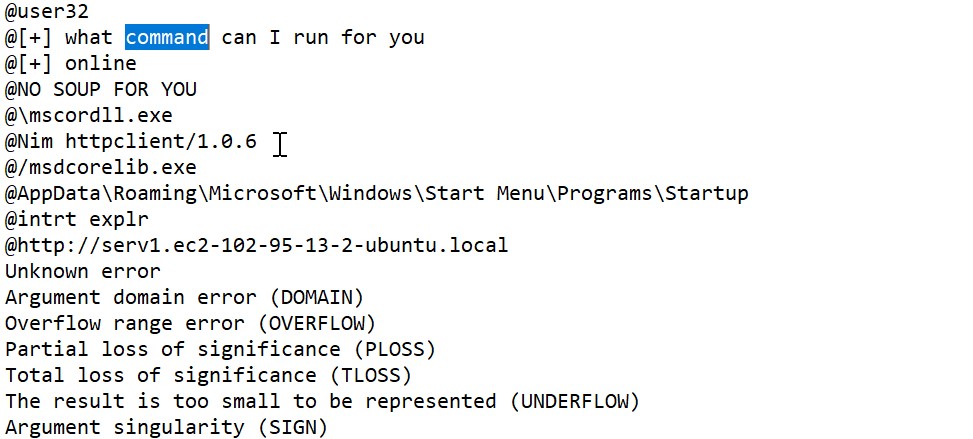


From above we can get the hash key, that hash key should be copied and place in the virus total website. Which detects the virus in the malware file.

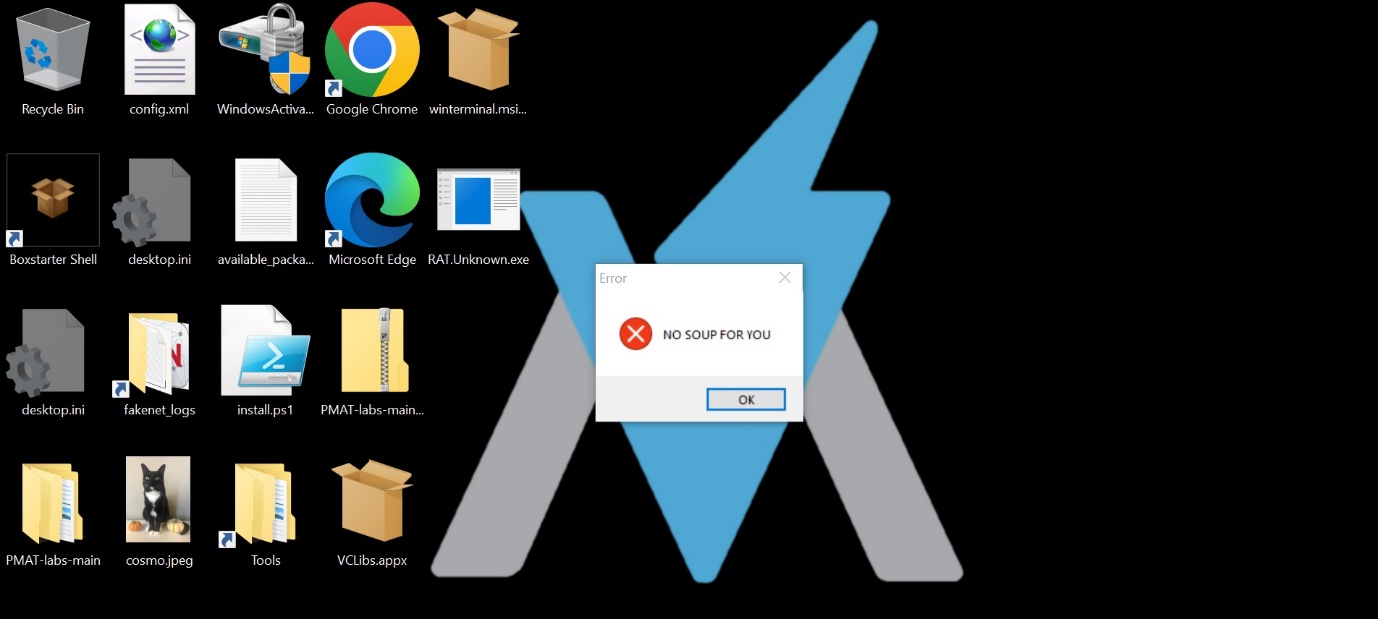


Next step we going to find out the suspicious strings in the malware file named “RAT.unknown.exe.malz” using the command “FLOSS.exe “RAT.unknown.exe.malz”.

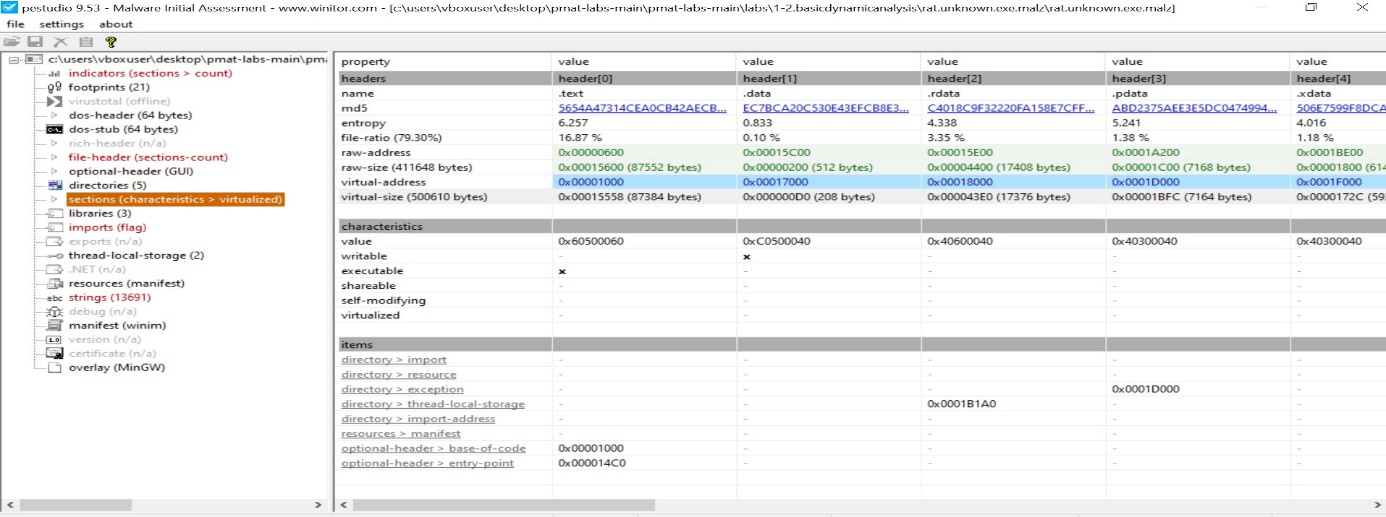


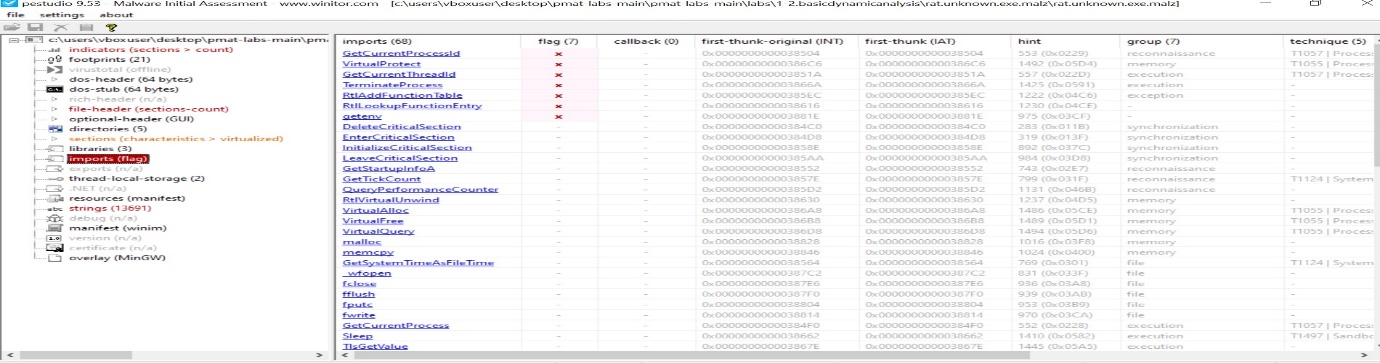


Before the connection establishment in the isolated network, the act of malware is seen as:



And next I performed static analysis using tool called “pestudio” which stands for portable executable studio. After opening tool open the malware file and start analyzing the malware file.



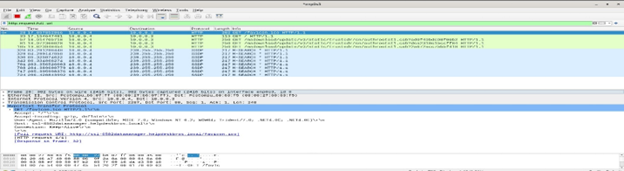
In imports I found some important flags in malware file.

Here end of static analysis of malware file.

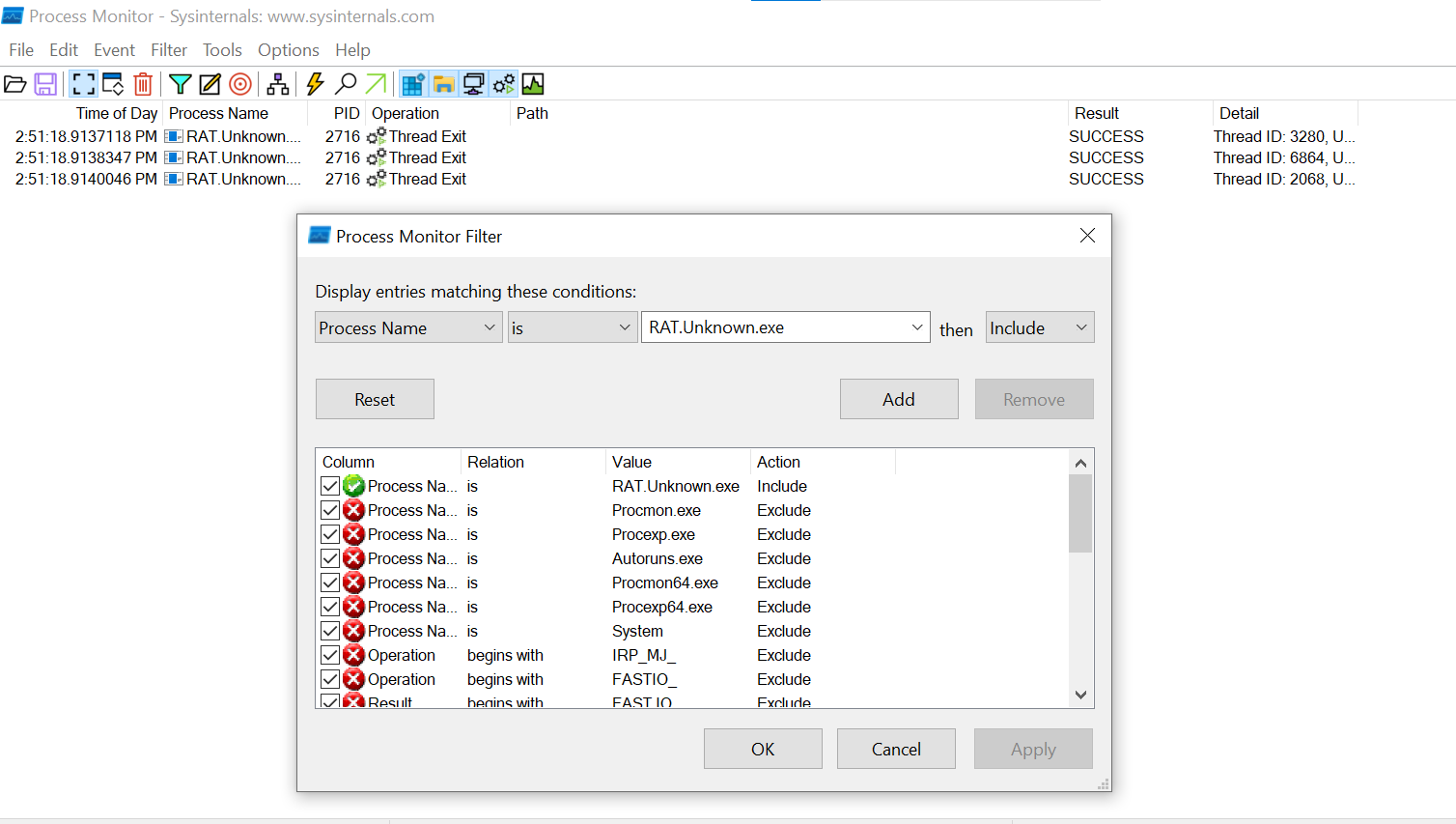
**Basic Dynamic Analysis**

First step is to open wireshark which widely used, open source network analyzer that can capture and display real-time details of network traffic in the terminal of remnux machine using the command “Wireshark”.

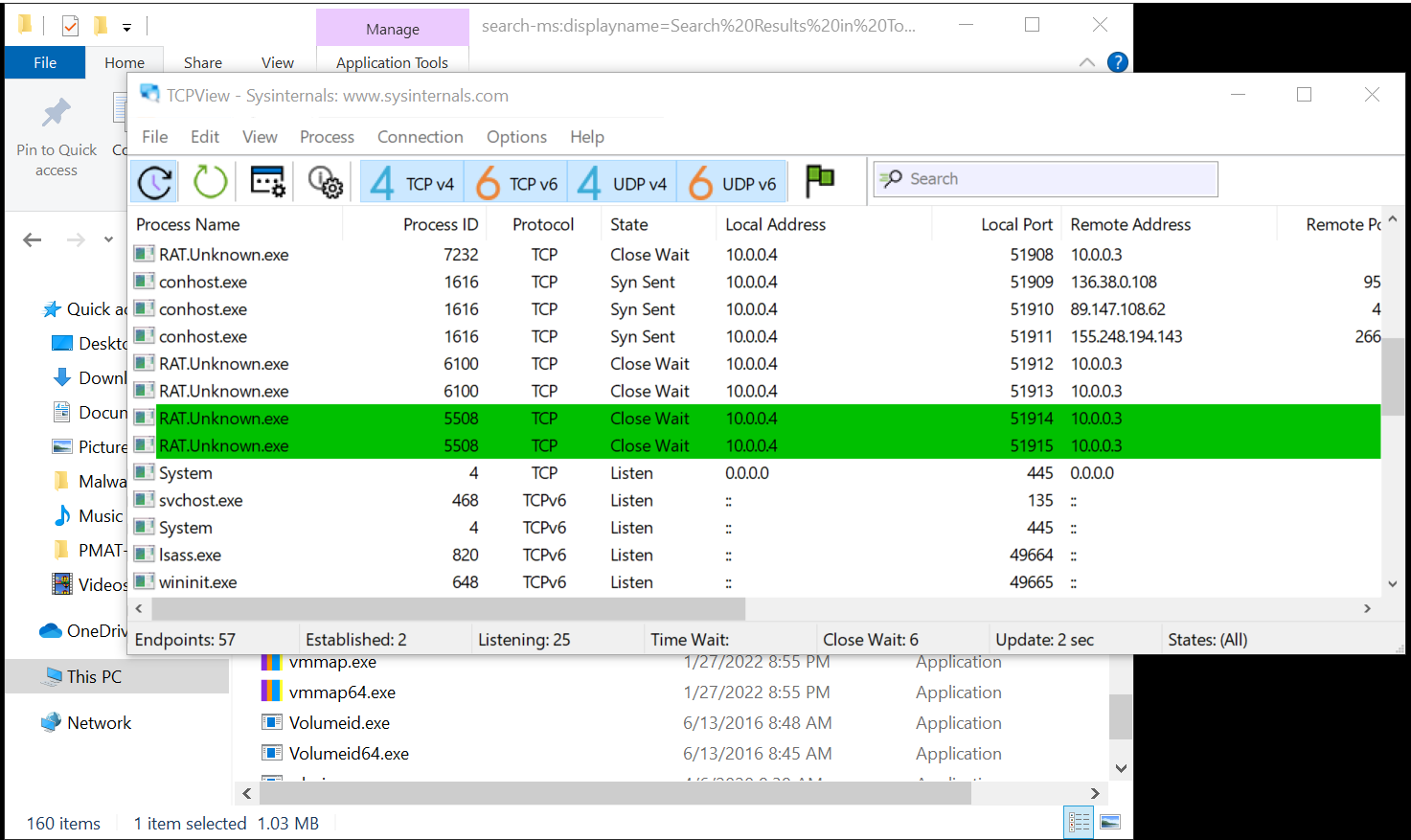
And use the filter http.



And next process in dynamic analysis is to open the tool called procmon in flareVM. Now use the filter option and try to filter the malware file as shown below. To know some suspicious files ,urls and paths.



Now analyze the malware using another tool called tcpview. And found some suspicious Ip address in it.



Hence, we can observe that the executed malware installs another piece of malware in the device.

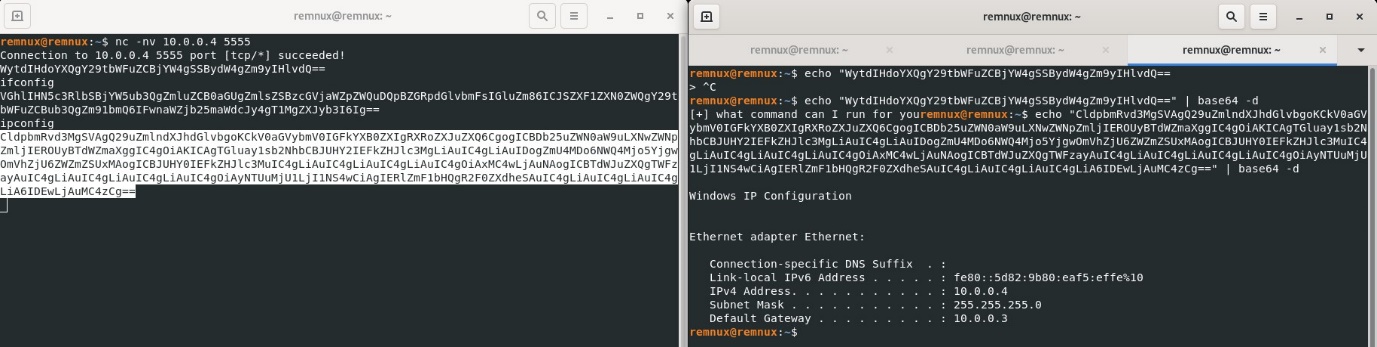
Then by the netcat, we can read and write data over this tcp network connection. In the remnux machine I’ve performed the command execution with the captured ports from tcpview.



Then decode the Base64 hash obtained by the netcat command execution. It returns as:



So lets try to execute some more commands.



So, from the above observations, we can conclude that the Remote Access Trojan is actually the Remote Command Execution Malware.