Malware Analysis and Detection

Assignment-2

Submitted by:

Muhammad Osama Khalid

20I-1955 (MSCNS)

Section: MSCNS

Table of Contents

List of Figures

Static analysis is a type of malware analysis in which we examine the malware without running it. In the static analysis, we extract the information of the malware through its binary to analyze its type, signature, machine information, DLLs and functions it will use, etc. In this assignment, I have to perform static analysis on the given malware samples with the help of Ghidra.

Malware-1 W32.SecretKAN.Trojan

This malware belongs to the family of trojans. To analyze malware I open it in Ghidra and then perform auto analysis on the malware sample.

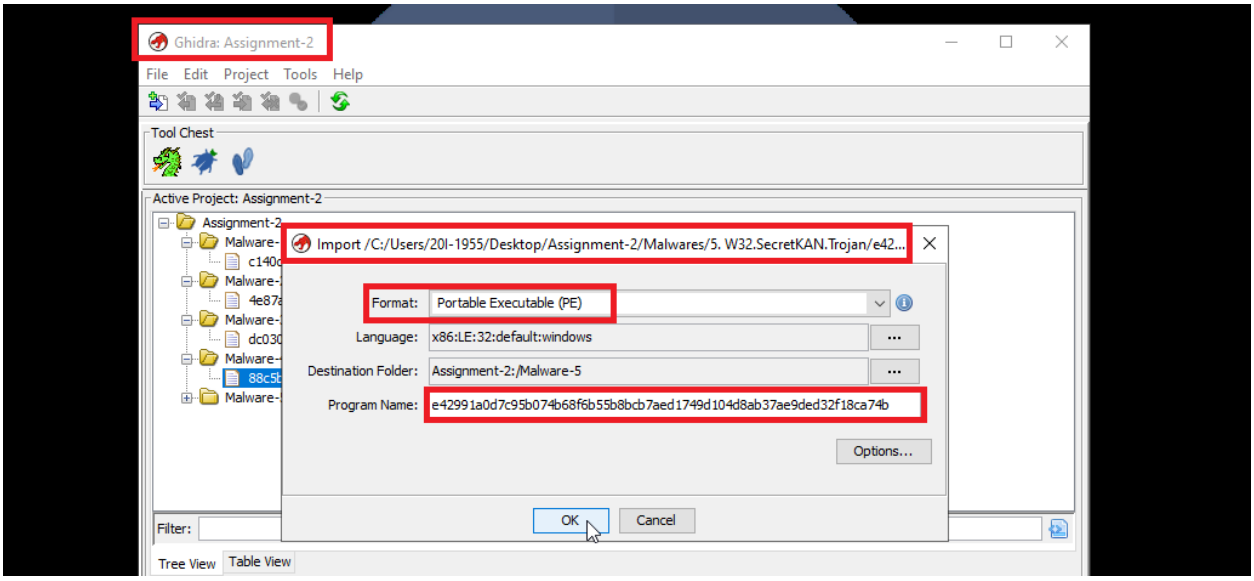


Figure 1: Malware-1: Opening malware sample in Ghidra

On opening the malware sample in the Ghidra I found that the malware is PE executable.

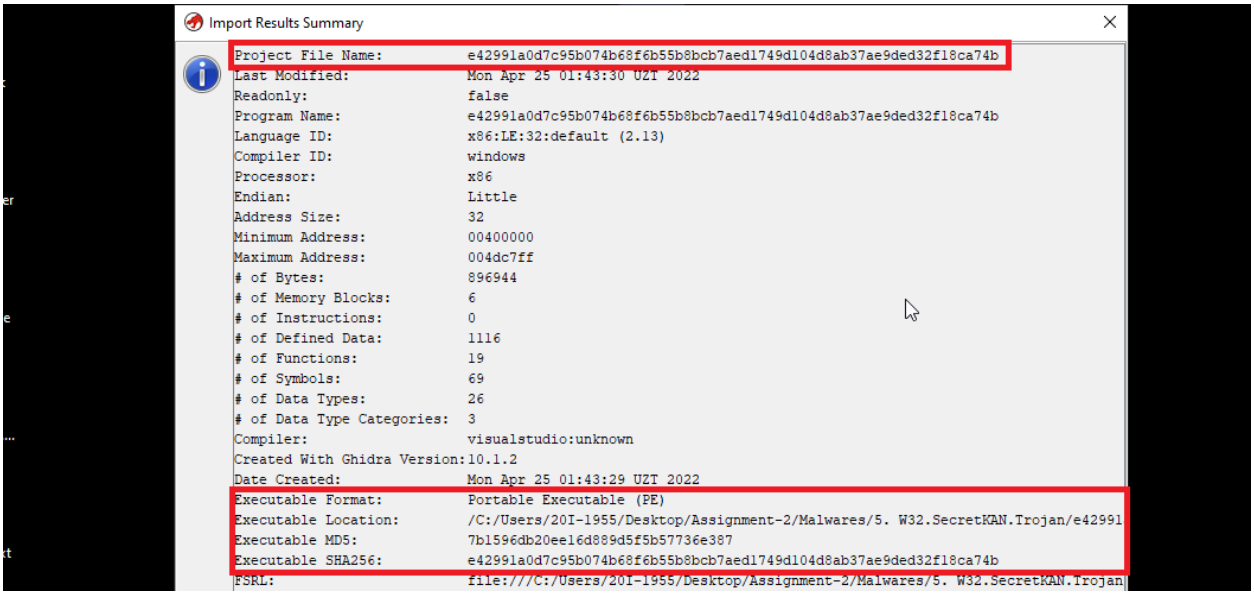


Figure 2: Malware-1: Basic details exreacted by Ghidra about the malware sample

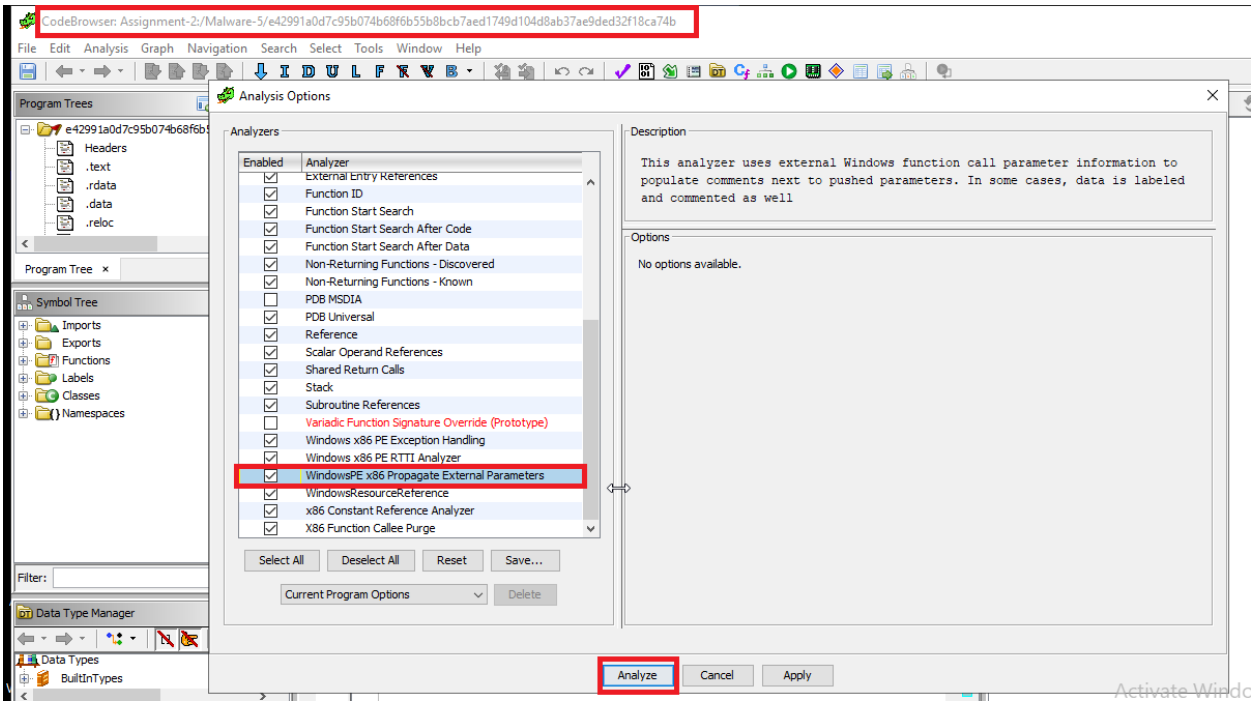


Figure 3: Malware-1: Ghidra auto analyze the malware

Task-1 What are the different segments or sections in case of each malware?

After Ghidra complete the auto analysis I found that the magic byte oif the malware which is MZ, moreover I found the details of different sections used by malware that includes ".text", ".rdata", ".data", ".reloc".

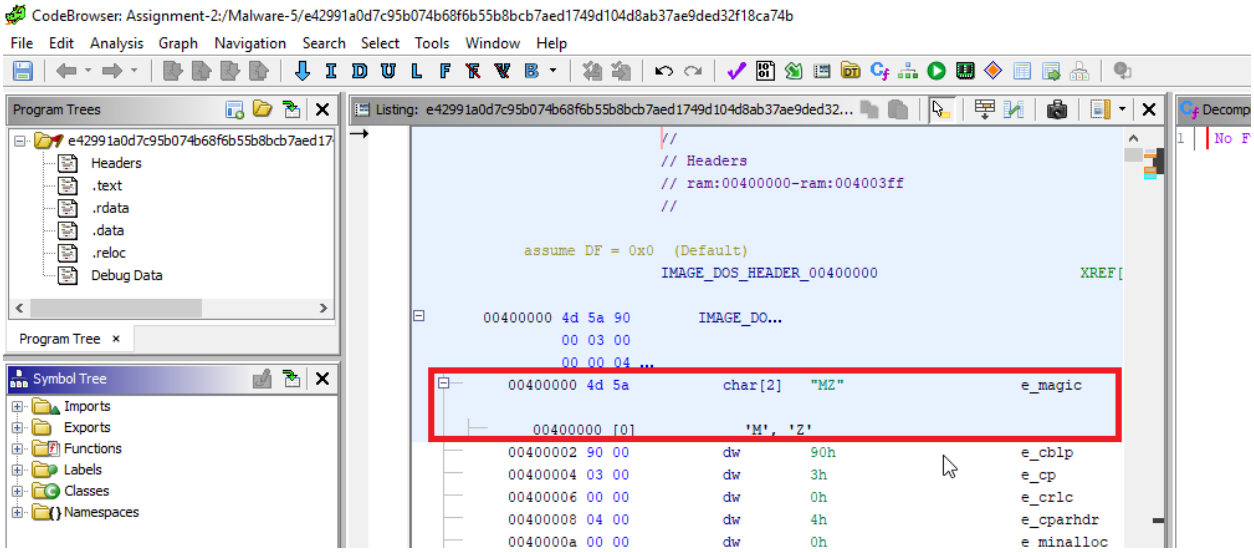


Figure 4: Malware-1: Magicbyte of the malware

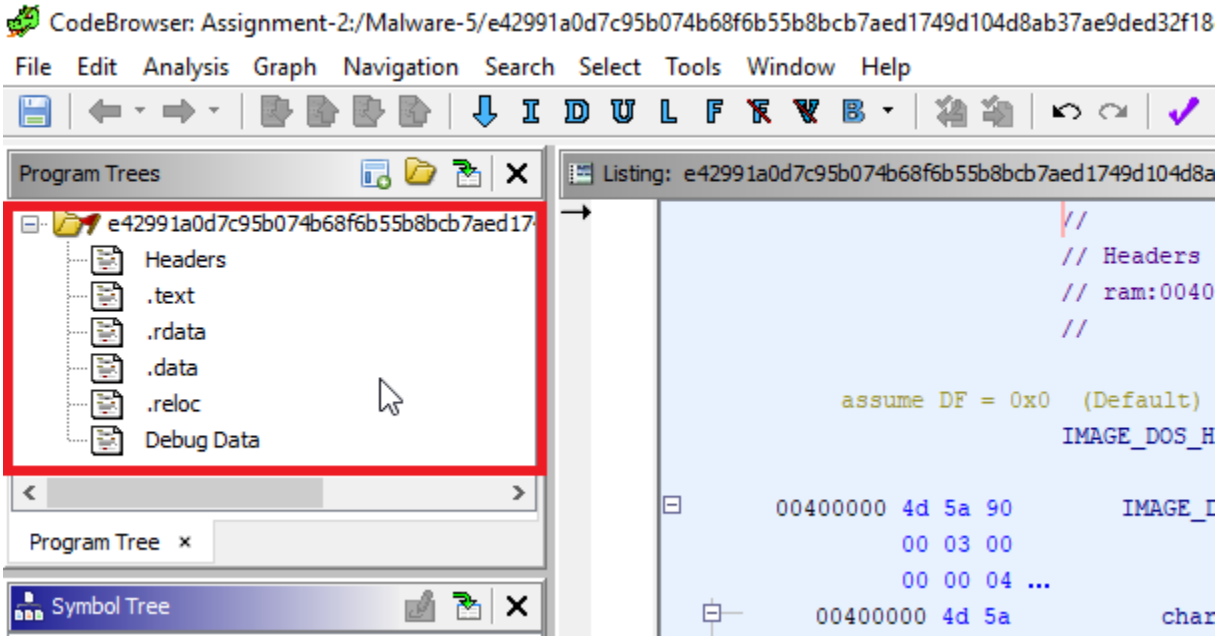


Figure 5: Malware-1: Details of the sections used by the malware

Task-2 What are different functions, imports and exports of each Malware?

To perform its functionality malware imports different DLL's that includes "ADVAPI32.dll", "KERNEL32.dll", "OLE32.dll", "SHELL32.dll", "USER32.dll", "WININET.dll". Moreover it also use different funcitons to perform it functionality.

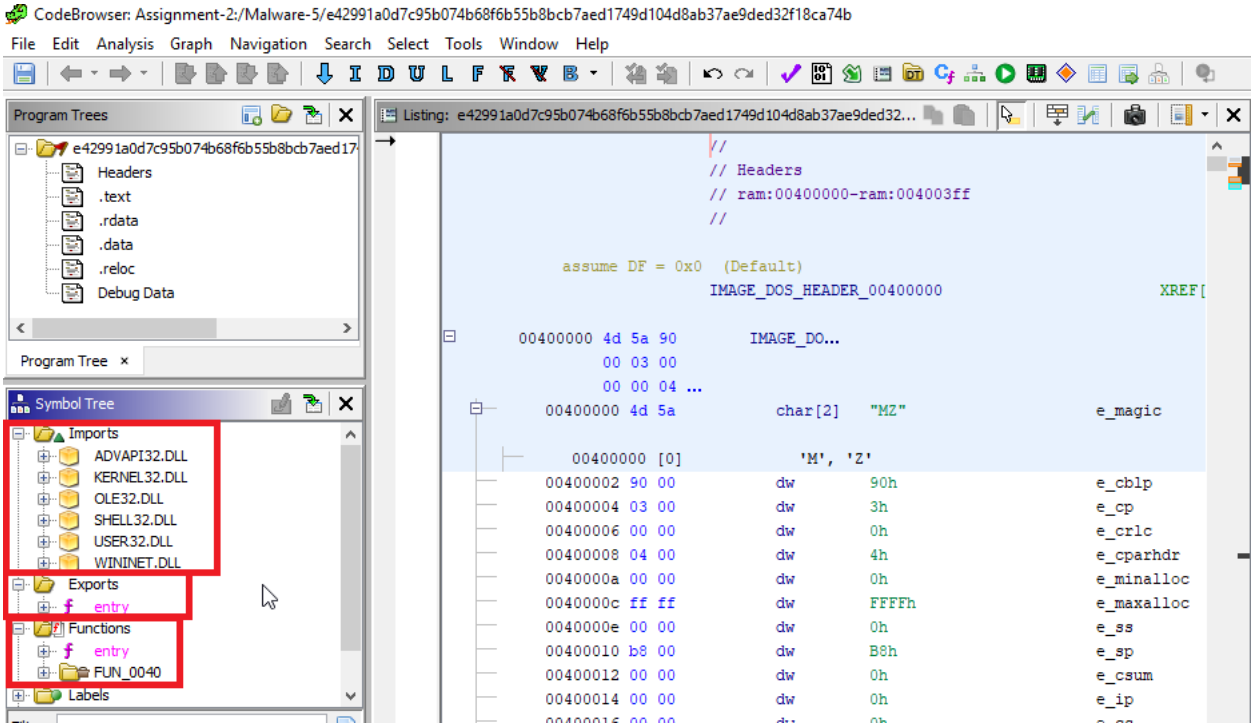


Figure 6: Malware-1: Details of the functions, imports and exports used by malware

Task-3 What is flow of functions in case of each malware? Is there any suspicious function? Give detail (name, arguments, call mechanism) of suspicious functions?

The flow of the funcitons of this malware is that if first intract with the system programs like “notepad.exe”, “explorer.exe”, “svchost.exe”, etc. then connects the computer to some minning pool to perfrom crypto mining also checking the CPU running status. After perform the mining it connect backs to the attacker to send the results back to him/her. Moreover after completing the mining process it deletes the zone file.

Task-3.1 Function FUN_004030d0

In this function malare intract with the system programs which includes “notepad.exe”, “explorer.exe”, “svchost.exe”, etc.

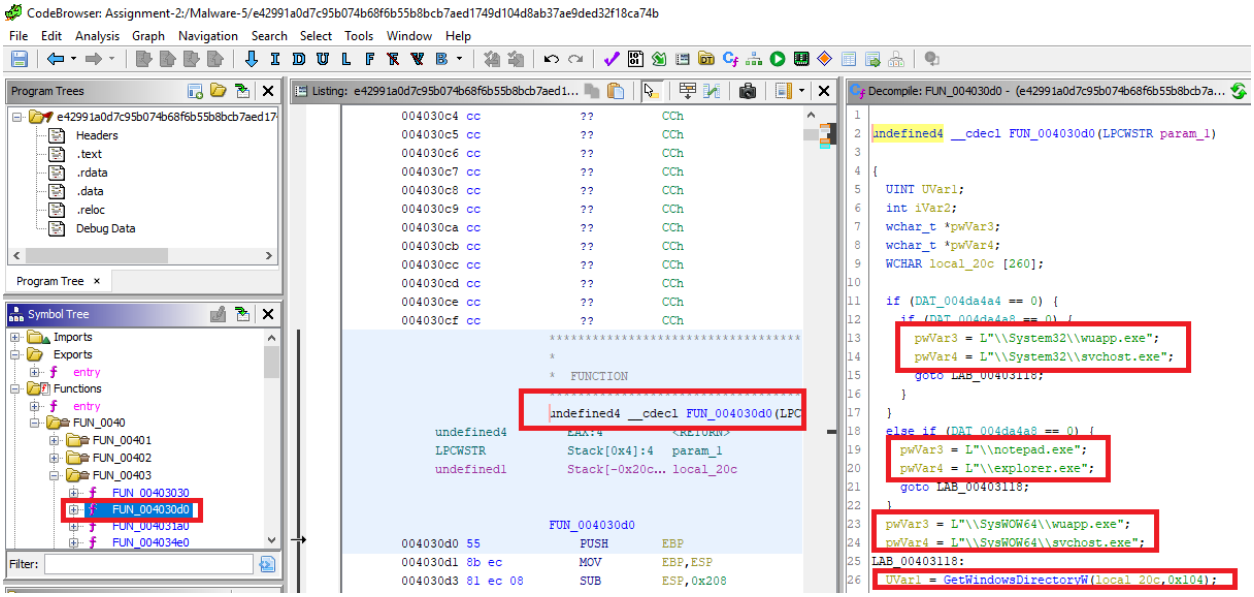


Figure 7: Malware-1: Malware intract with some programs installed on the machine

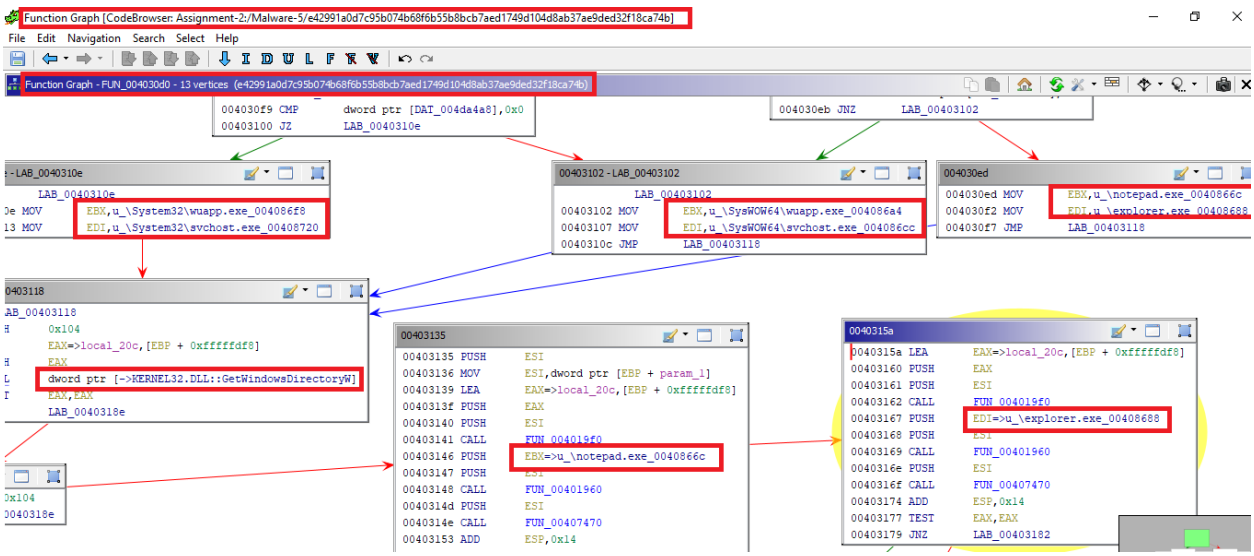


Figure 8: Malware-1: Programs and DLLs that is accessed by the malicious function

Task-3.2 FUN_00403b00

In this function I found the details of the cryptomining that malware performs rainging form cryptocurrency mining hashing algorithms “CryptoNight”, “CryptoNight-lite”, “CryptoNight-heavy” that is used by certain Proof of Work blockchains. Also I found the details of the mining pool, api, worker-id, ccess token etc.

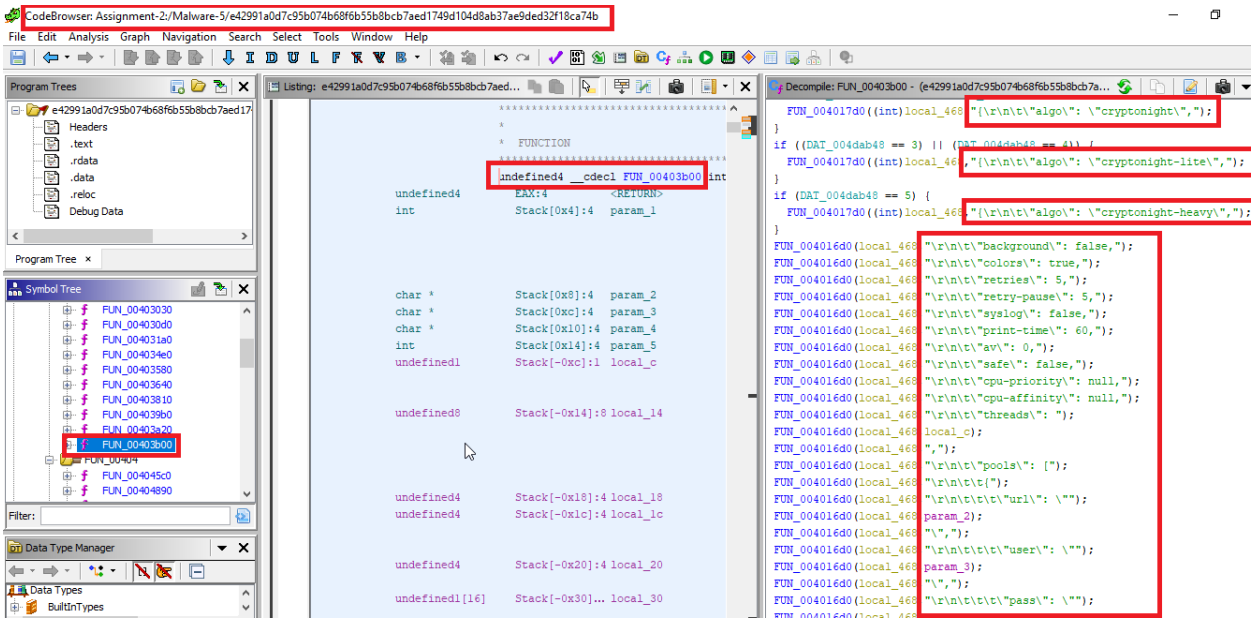


Figure 9: Malware-1: Details of Cryptomining hash algorithm

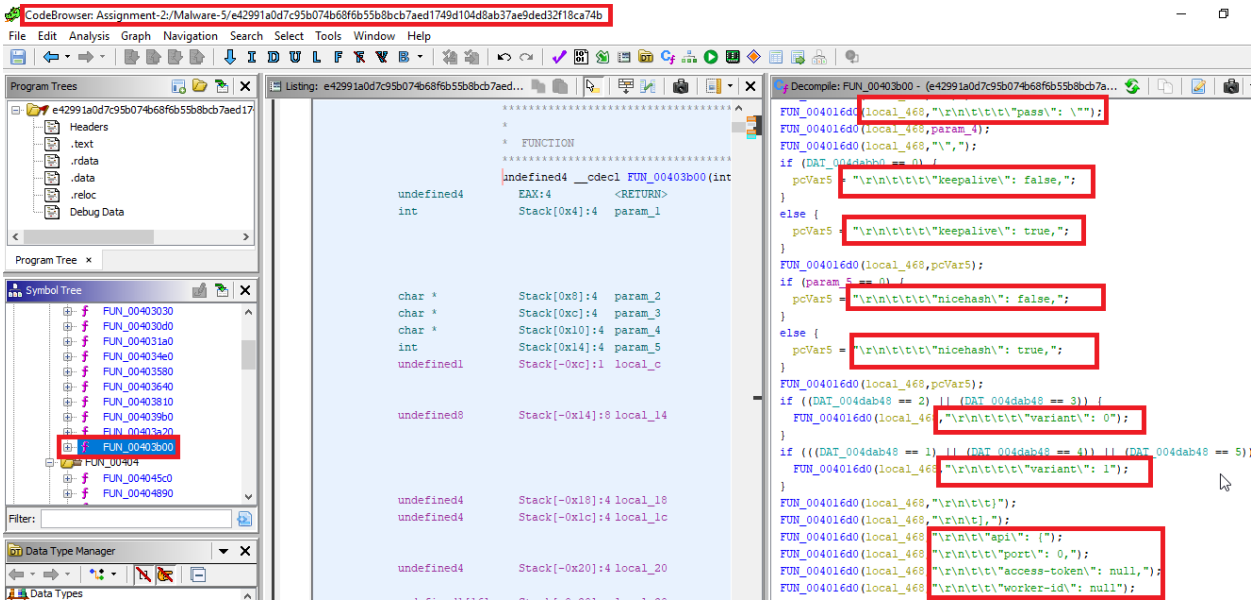


Figure 10: Malware-1: Other details of the crypto miner

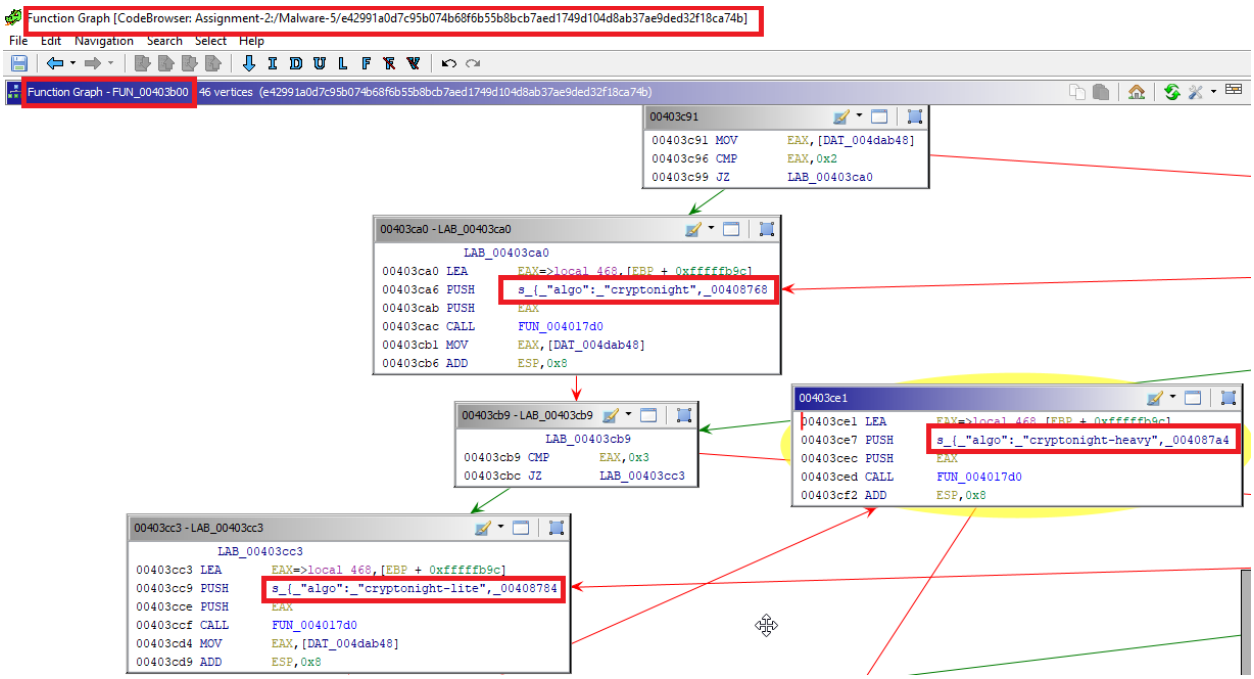


Figure 11: Malware-1: Details of Cryptomining hash algorithm

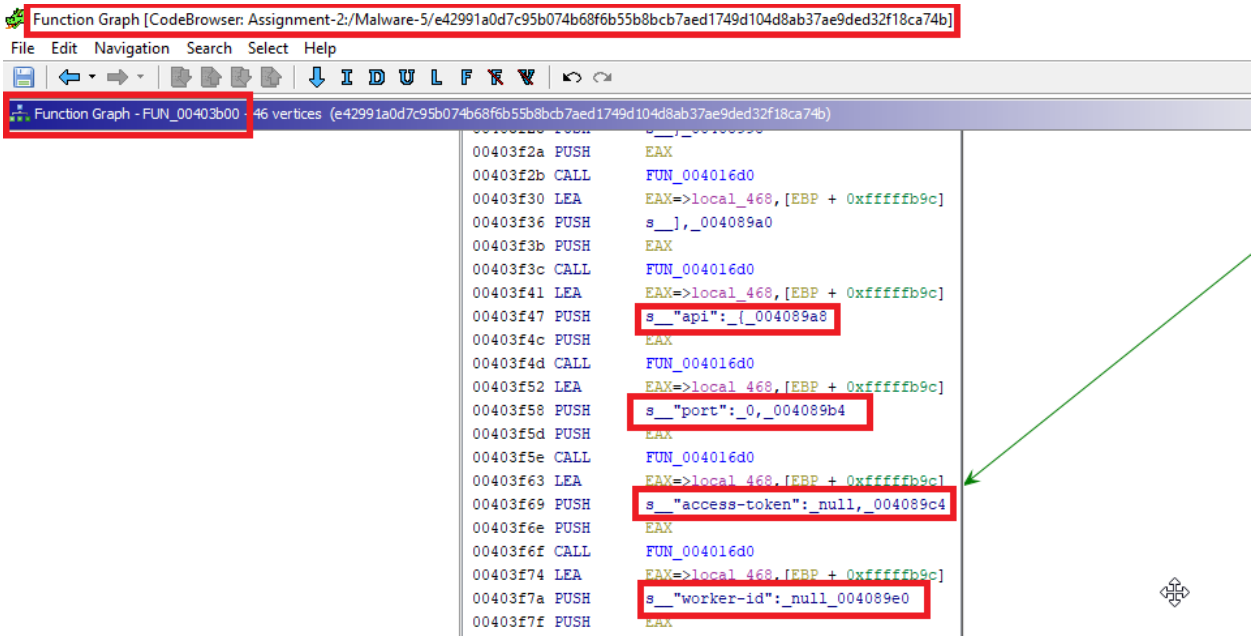


Figure 12: Malware-1: Other details of the cryptominer

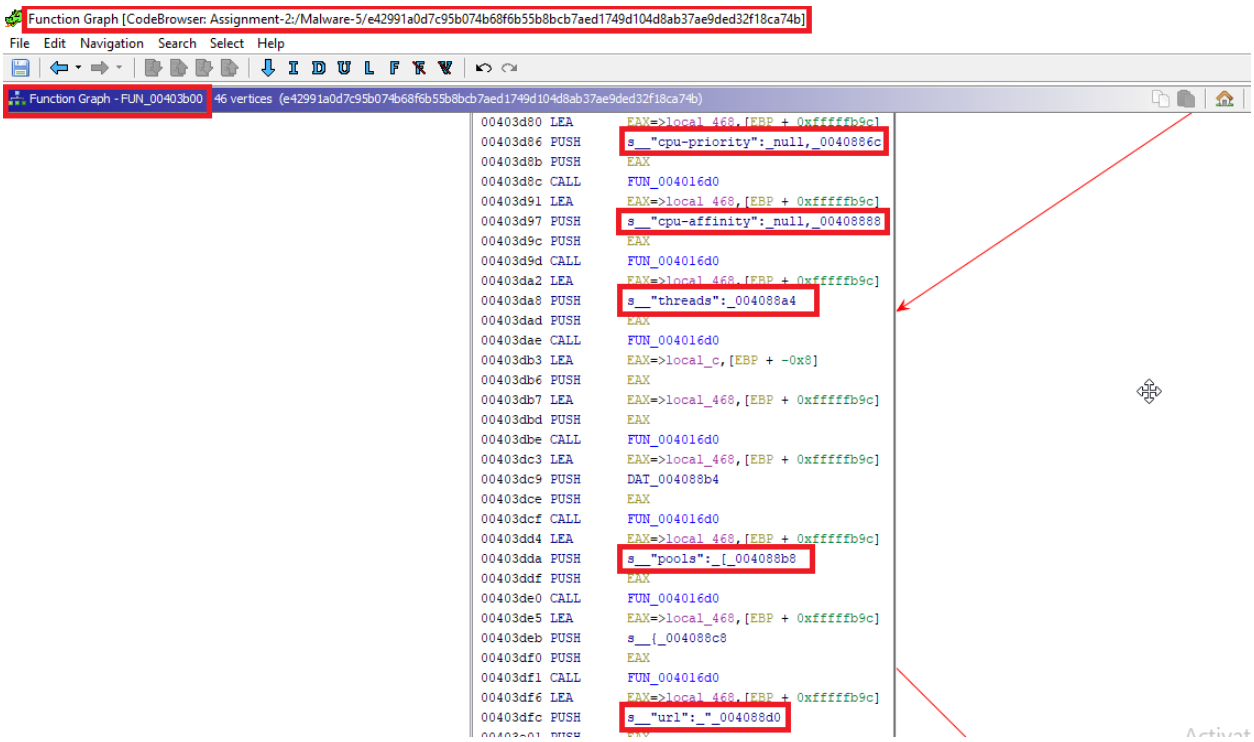


Figure 13: Malware-1: Other details of the cryptominer

Task-3.3 FUN_004031a0

In this fnction I found the detail of the CPU usage used by the malware while it connects to “nicehash.com” which is a cryptocurrency mining platorm on which it connects the sellers that have hashing power with the buyers that want hashing power to mine their cryptocurrencies.

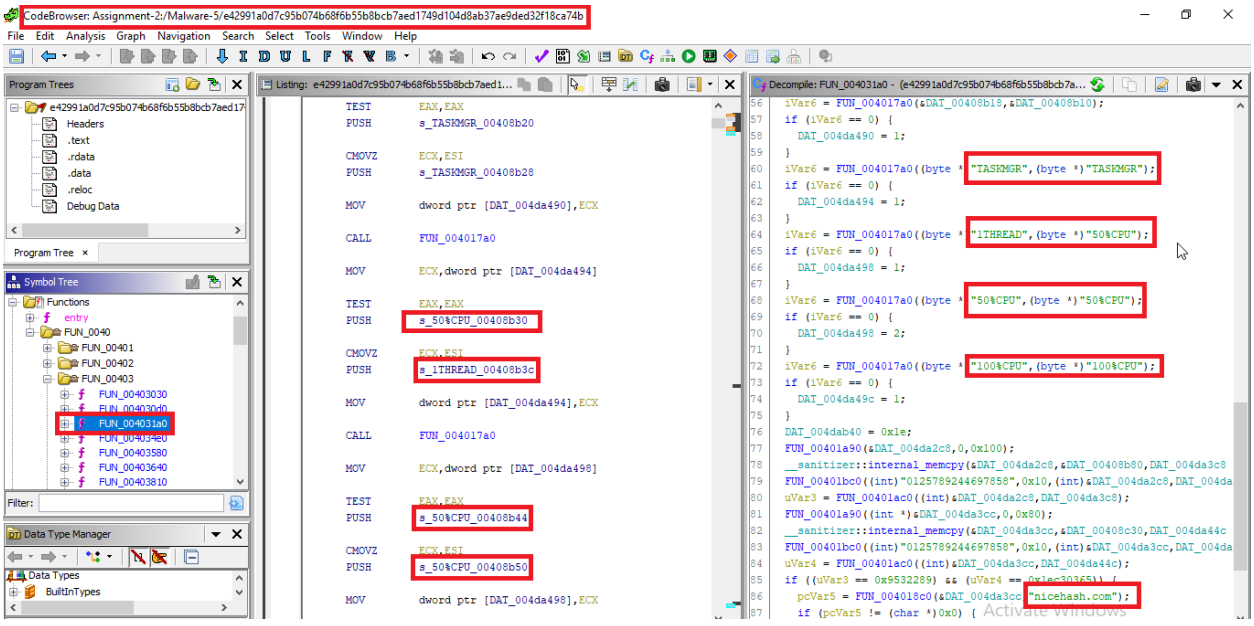


Figure 14: Malware-1: Details of CPU usage of the victim machine when malware connects to nicehash.com

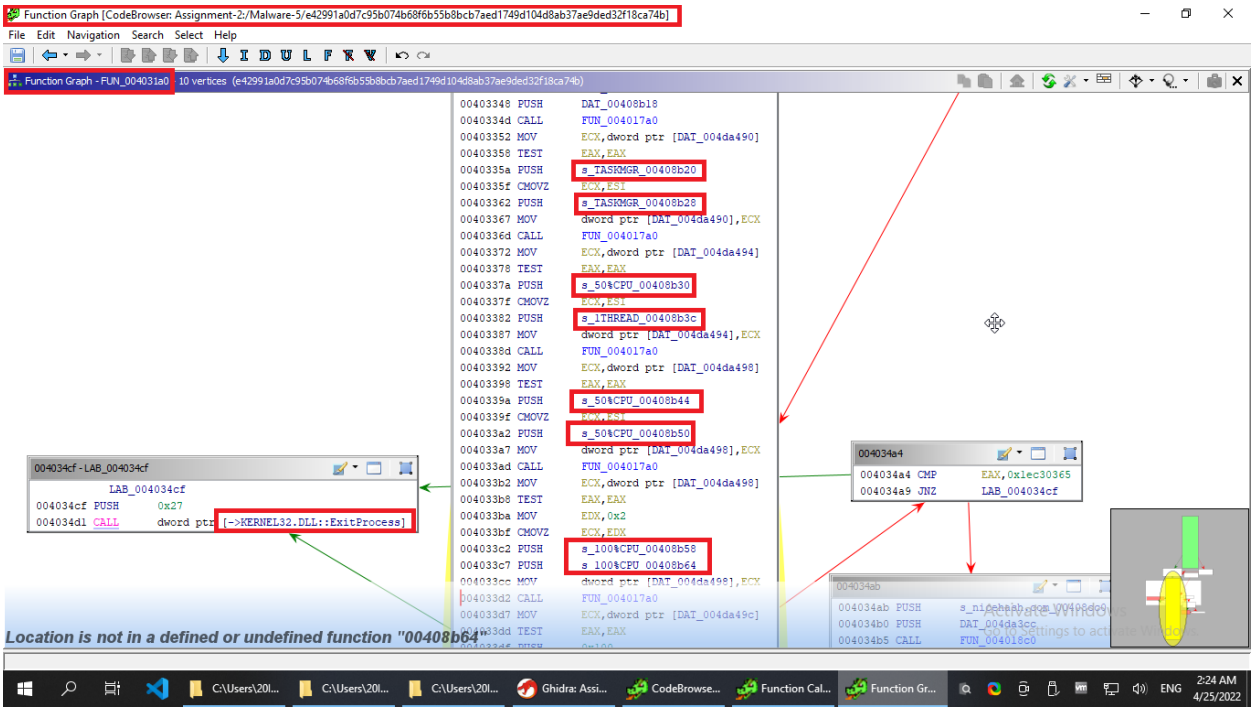


Figure 15: Malware-1: CPU usage details and the details of DLL's used by the malware

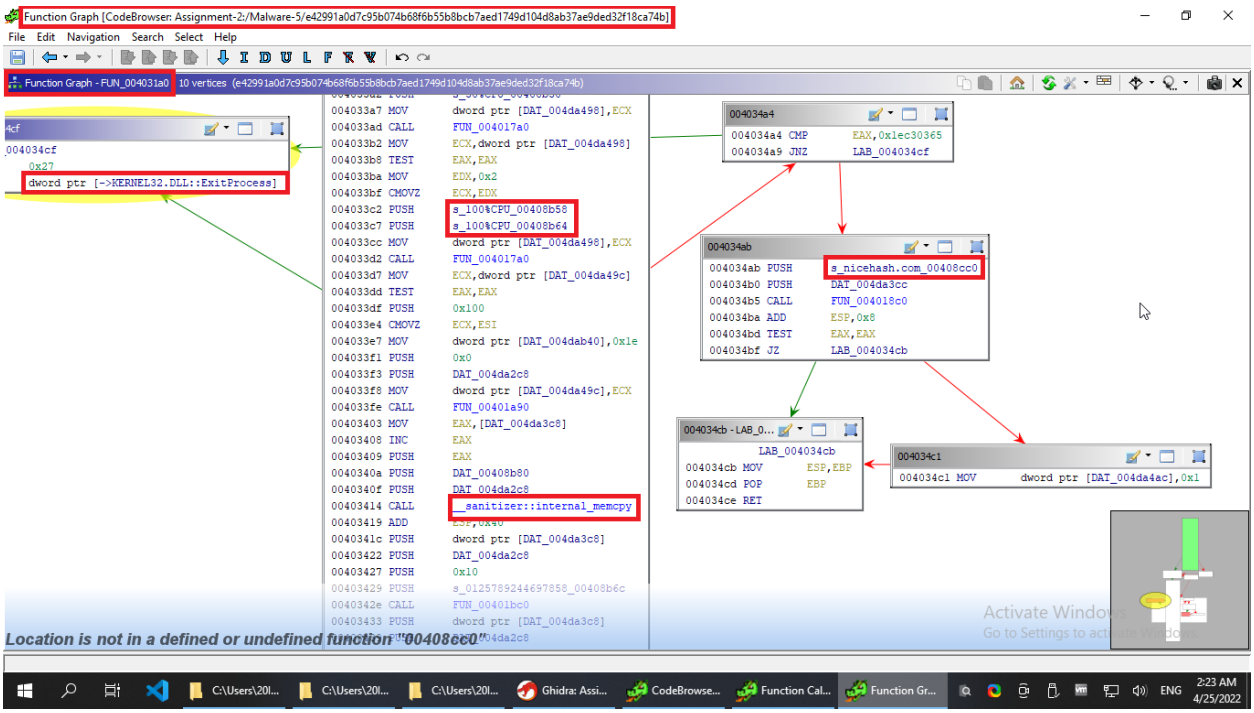


Figure 16: Malware-1: CPU usage details and the details of DLL's used by the malware

Task-3.4 FUN_00404a30

In this function I found the details of the mining address, mining pool, miner proxy and miner password used by the cryptominner to mine cryptocurrecy.

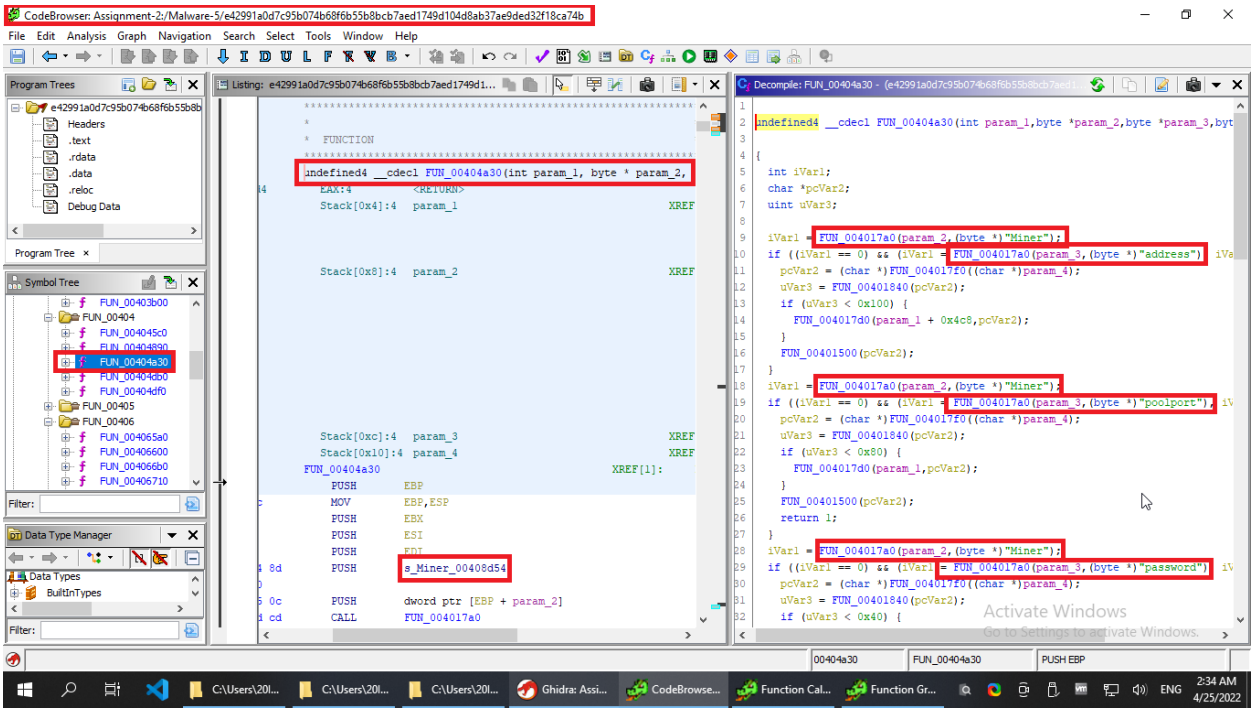


Figure 17: Malware-1: Details of the mining process

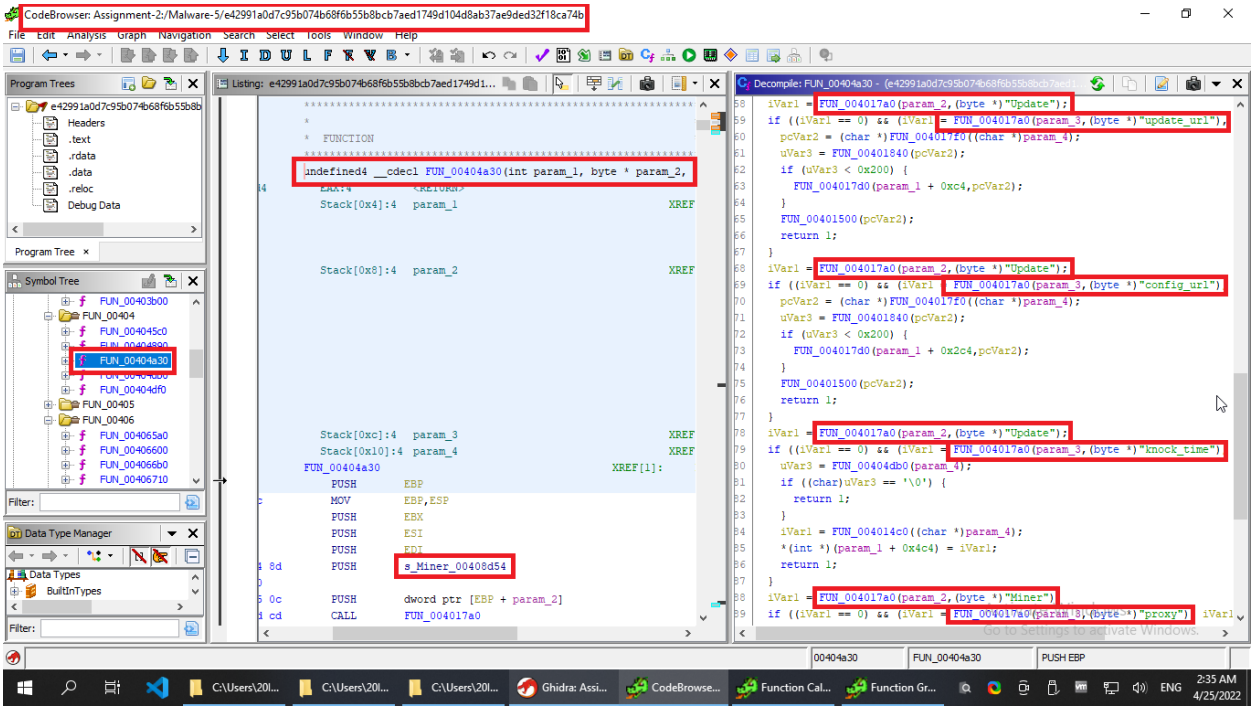


Figure 18: Malware-1: Details of the mining process

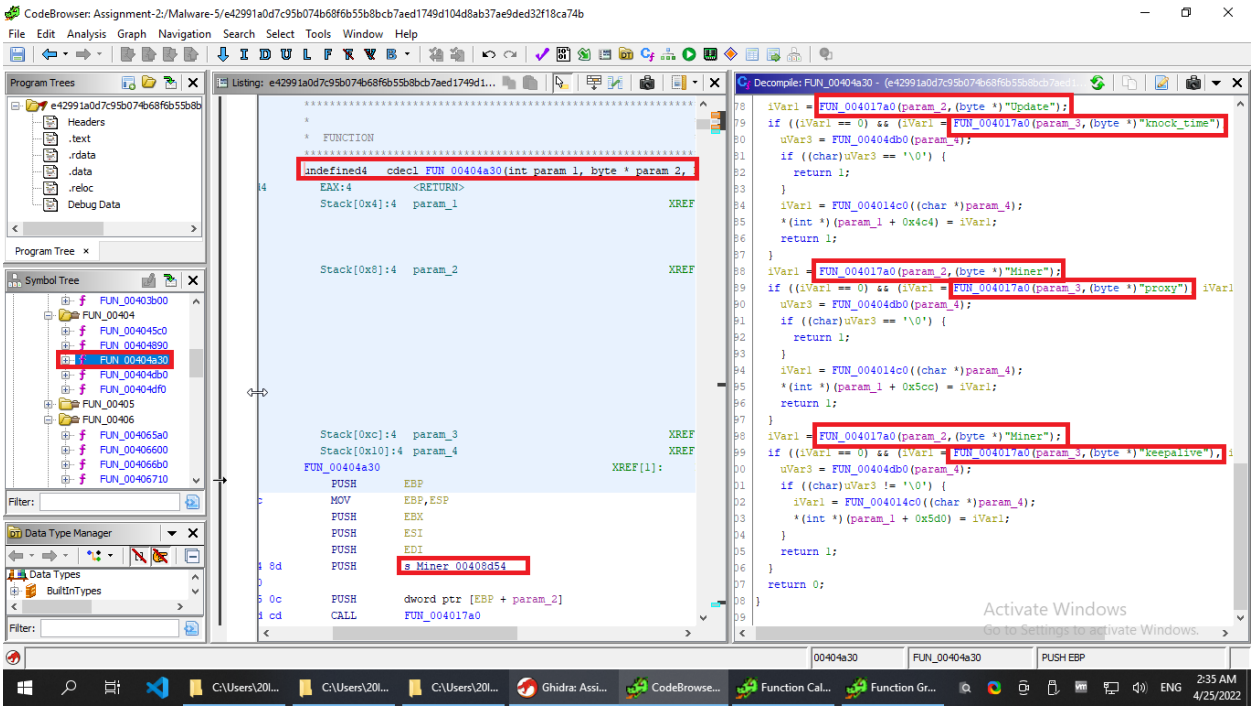


Figure 19: Malware-1: Details of the mining process

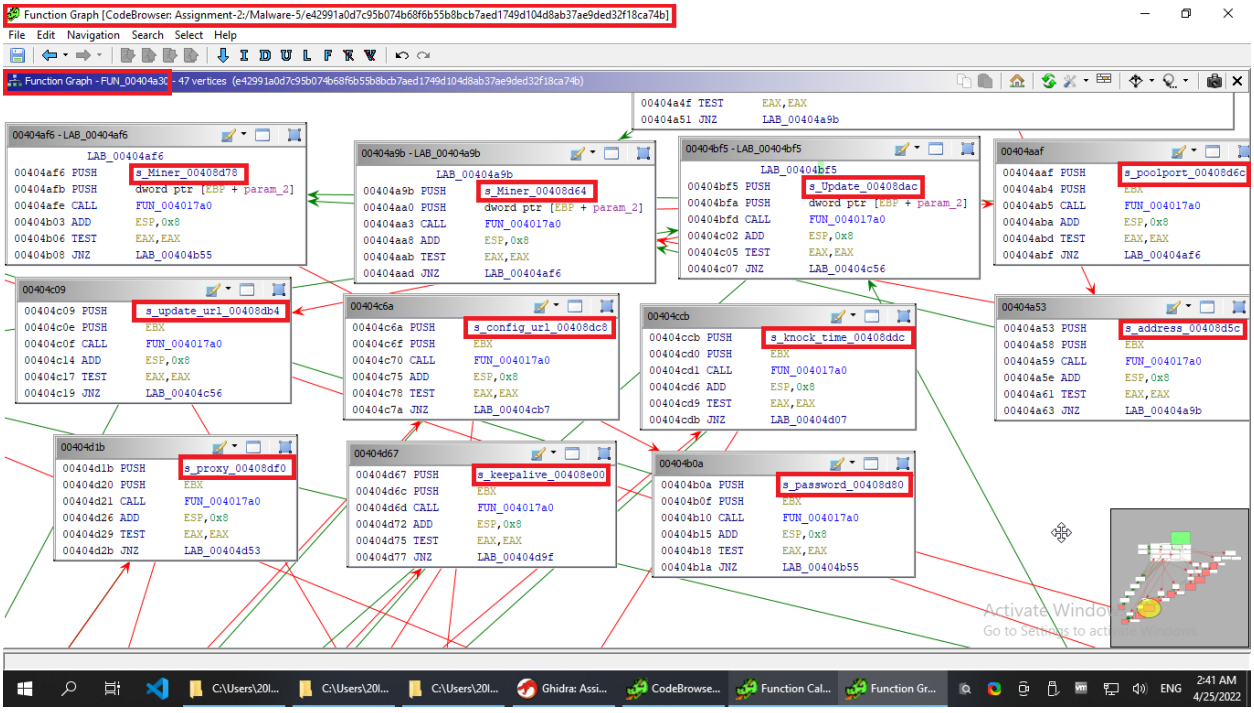


Figure 20: Malware-1: Details of the mining process

Task-3.5 FUN_00406710

After that I found that when the mining process completes malware delets the zone file used by it.

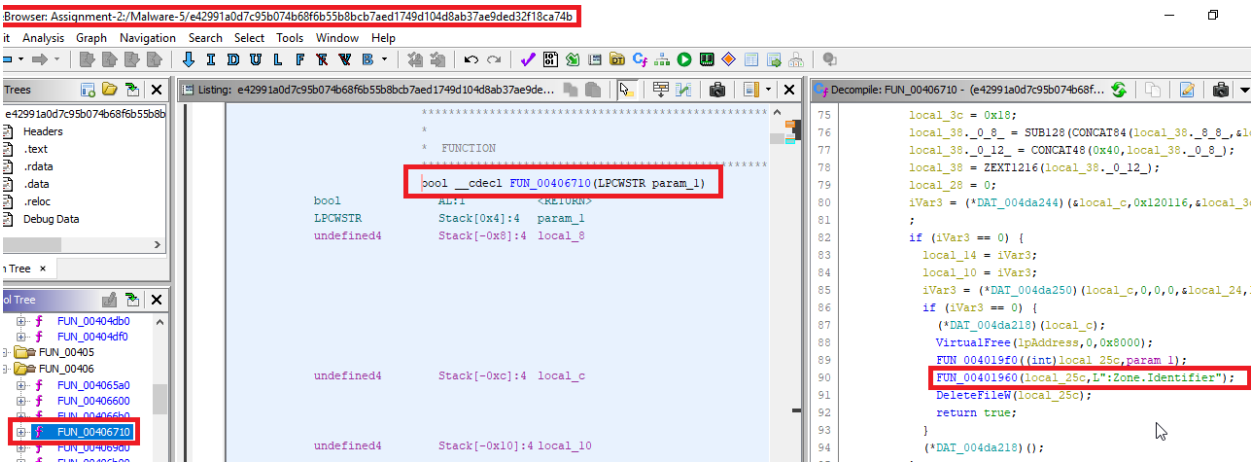


Figure 21: Malware-1: Delets the zone file on completion of the mining process

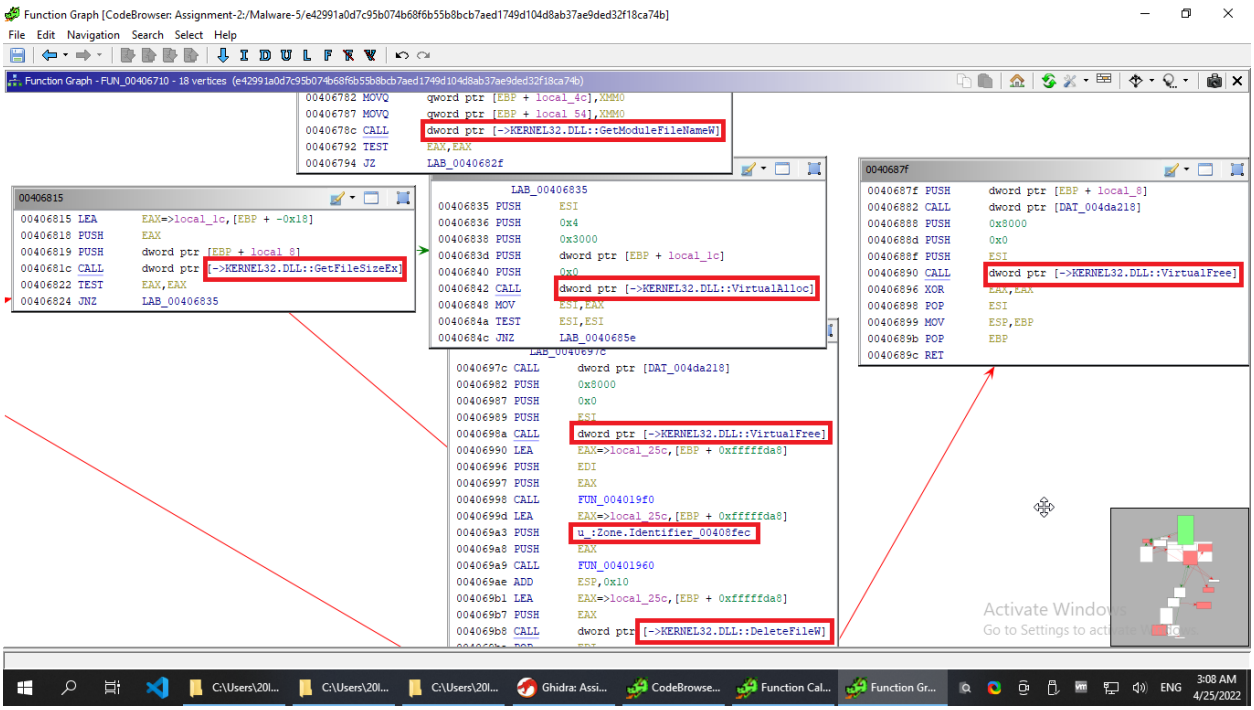


Figure 22: Malware-1: Deleting the zone file and the DLL's used by the malware

Task-4 What DLL's any malware includes? Are there any suspicious functionality called by these DLL's?

The DLL's used by this malware includes "ADVAPI32.dll", "KERNEL32.dll", "OLE32.dll", "SHELL32.dll", "USER32.dll", "WININET.dll".

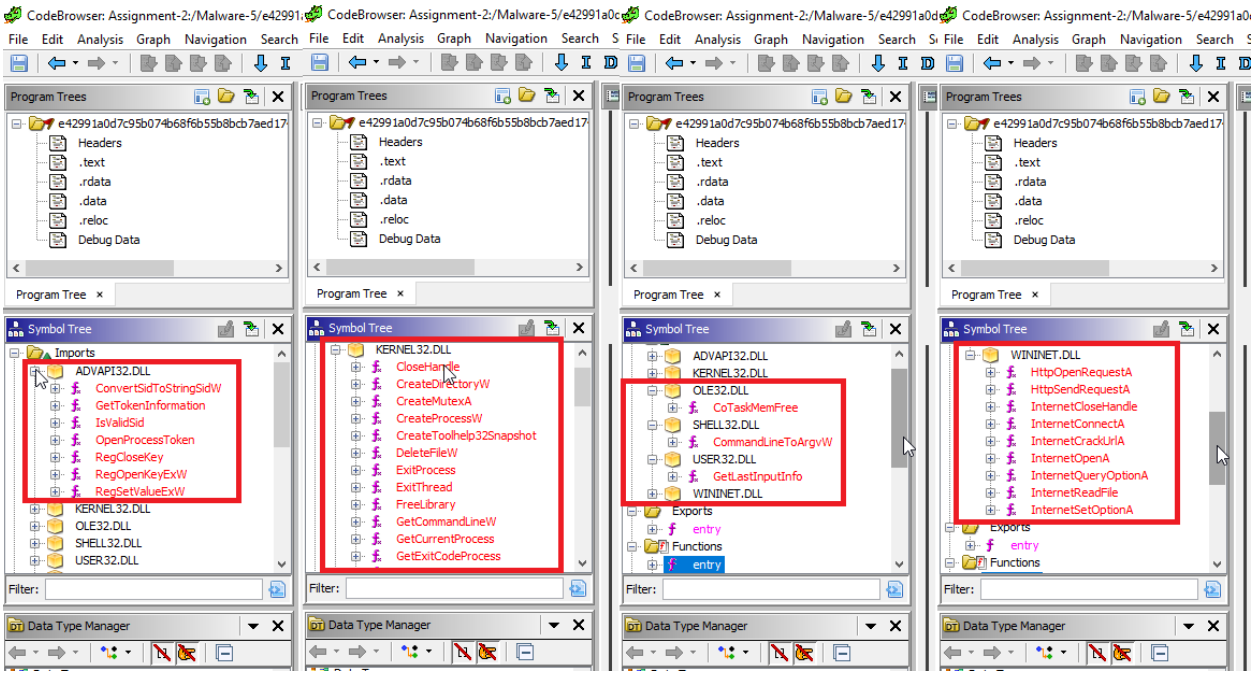


Figure 23: List of DLLs used by the malware with their functions

The suspicious functionality called by the DLLs includes the "Kernel32.dll" calling its function "GetWindowsDirectoryW" when the malicious function of malware "FUN_004030d0" is intract with the system programs including "notepad.exe", "explorer.exe", "svchost.exe" etc.

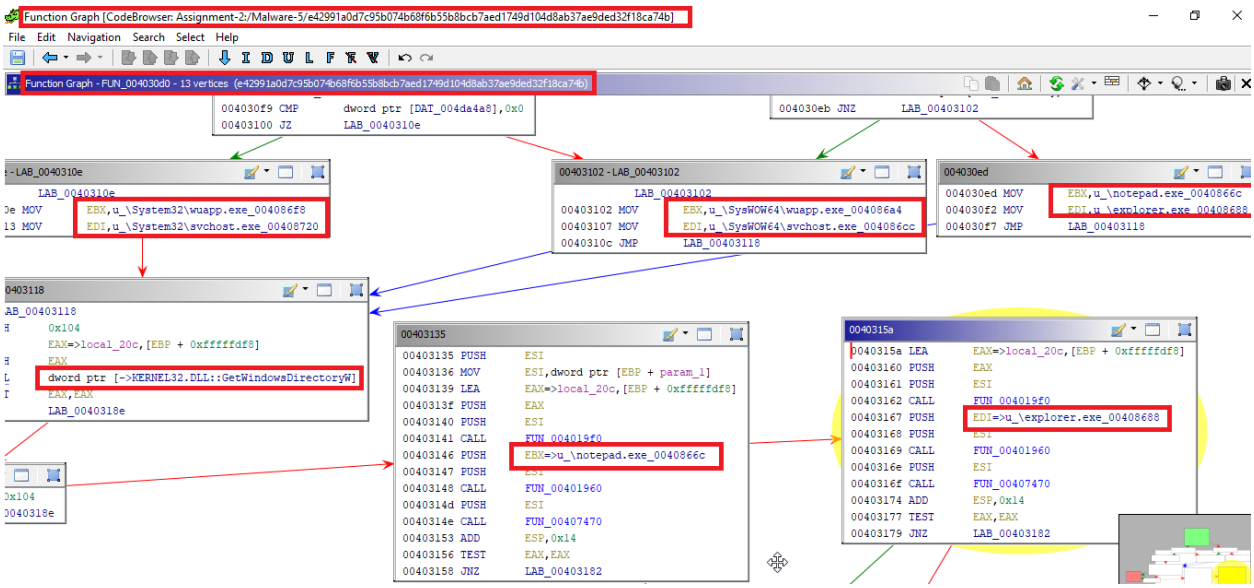


Figure 24: Malware-1: Malicioys DLL fucniton used by malware

Anoher suspicious functionality called by the “Kernel32.dll” DLLs includes “GetModuleFileName”, “GetFileSizeEx”,“DeleteFileW”,“VirtualAlloc” , and “VirtualFree” when the malicious functon of the malware “FUN_00406710” deletes the zone file after completion of the mining process.

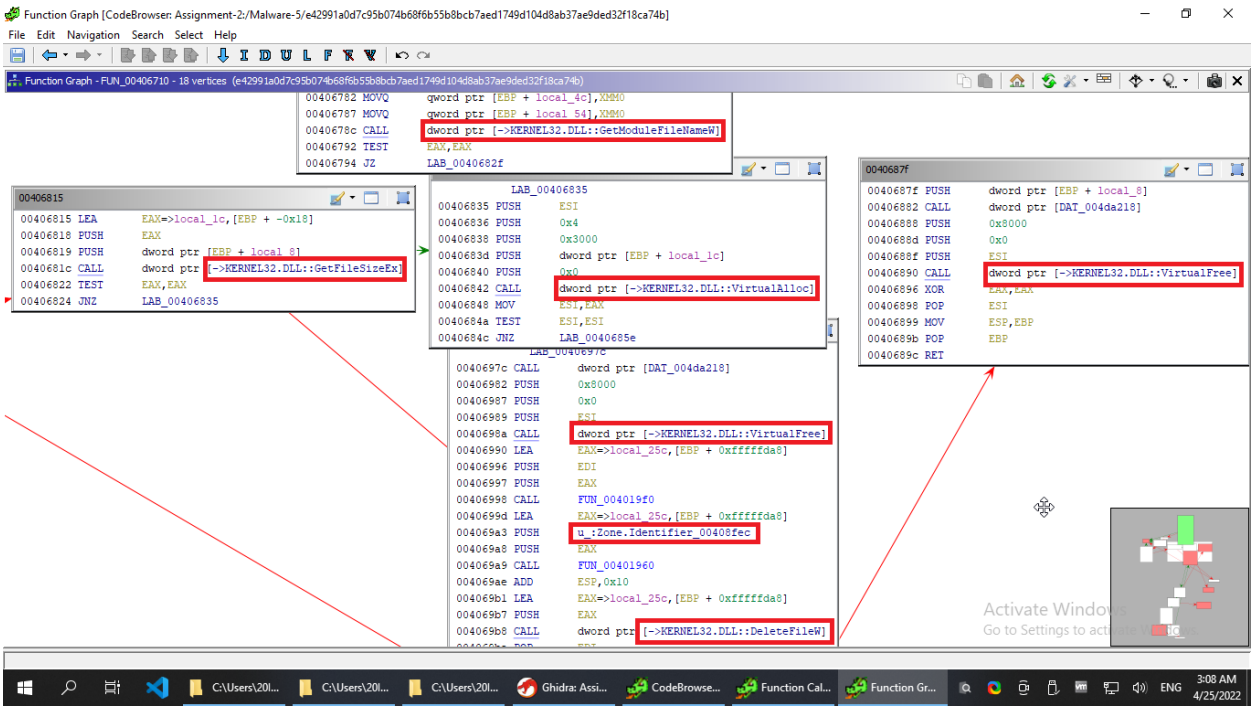


Figure 25: Malicioys DLL fucniton used by malware

Malware-2 Password-Stealer (003bbfec1)

This is a type of malware that steals the account information of the victim machine. To analyze malware I open it in Ghidra and then perform auto analysis on the malware sample.

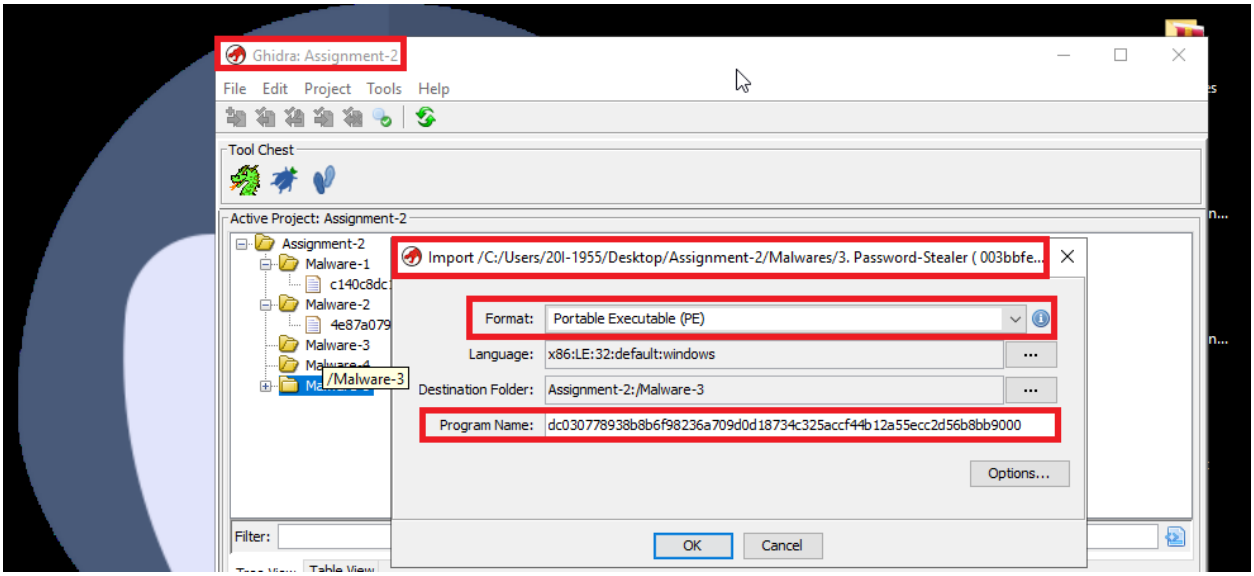


Figure 26: Malware-2: Opening malware in Ghidra

On opening the malware sample in the Ghidra I found that the malware is PE executable.

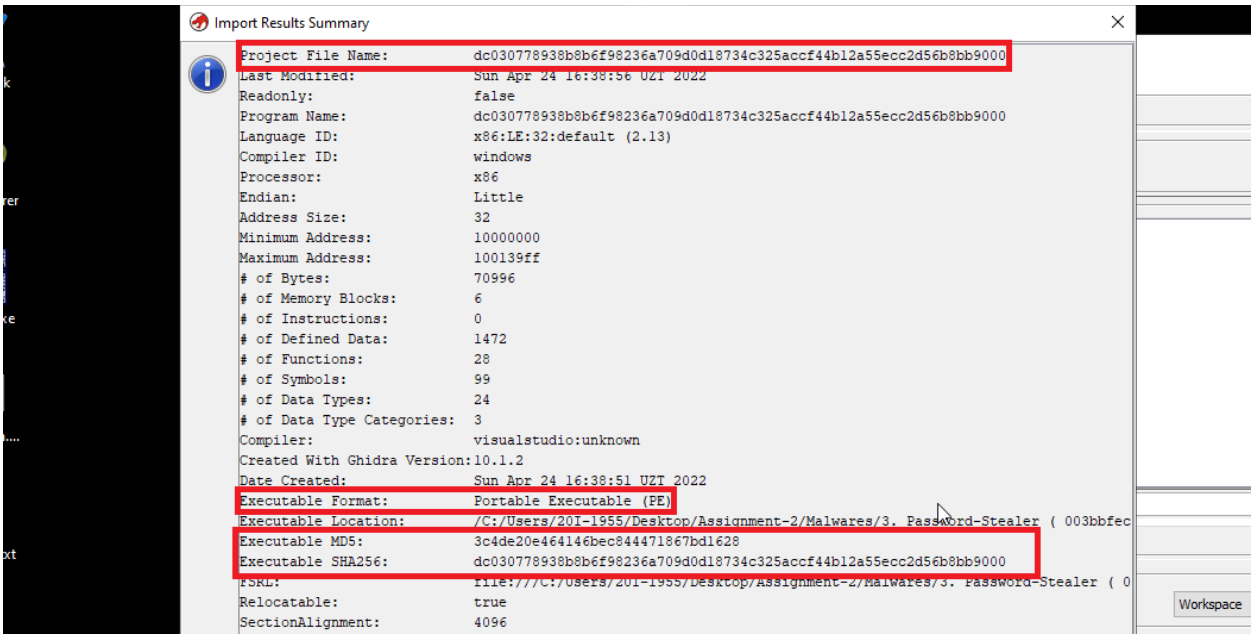


Figure 27: Malware-2: Basic details exreacted by Ghidra about the malware sample

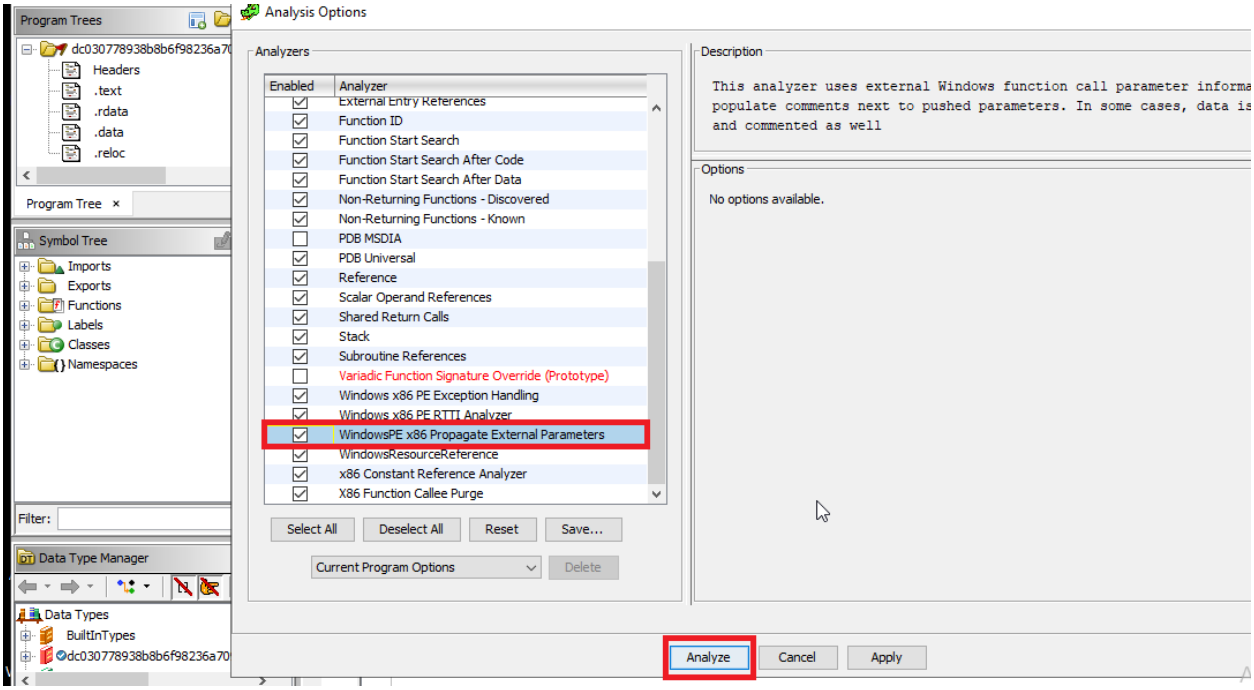


Figure 28: Malware-2: Ghidra auto analyze the malware

Task-1 What are the different segments or sections in case of each malware?

After Ghidra complete the auto analysis I found that the magic byte oif the malware which is MZ, moreover I found the details of different sections used by malware that includes ".text", ".rdata", ".data", ".reloc".

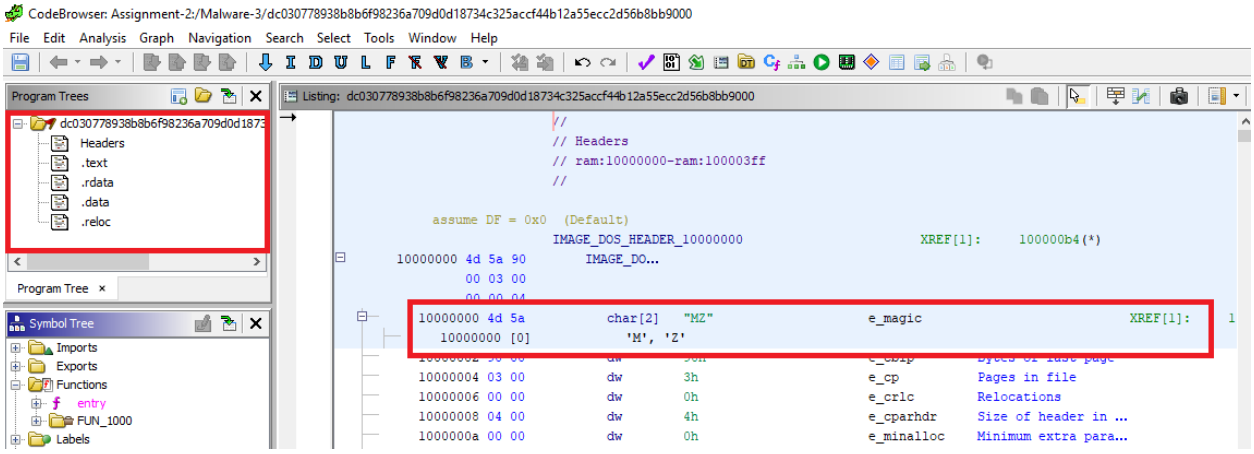


Figure 29: Malware-2: Magic byte and details of the sections used by malware

Task-2 What are different functions, imports and exports of each Malware?

To perform its functionality malware imports different DLL's that includes "ADVAPI32.dll", "KERNEL32.dll", "OLE32.dll", "SHLWAPI.dll", "URLMON.dll", "USER32.dll", "USERENV.dll", "WININET.dll" and "WSOCK32.dll". Moreover it also use different funcitons to perform it functionality.

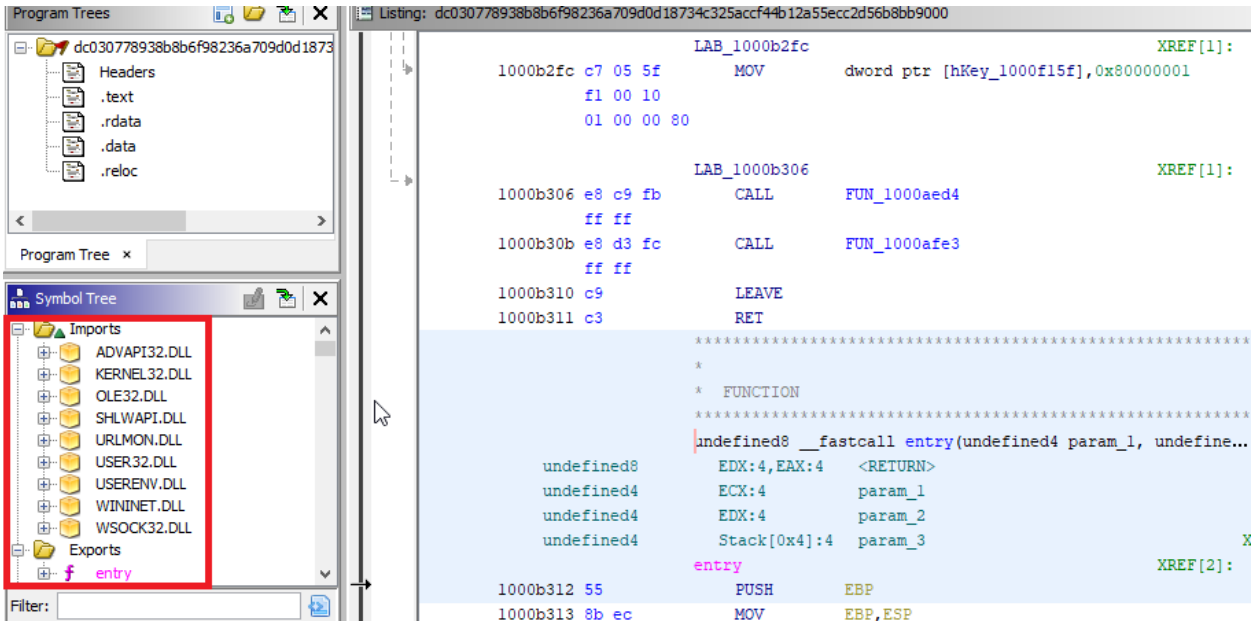


Figure 30: Malware-2: Details of the functions, imports and exports used by malware

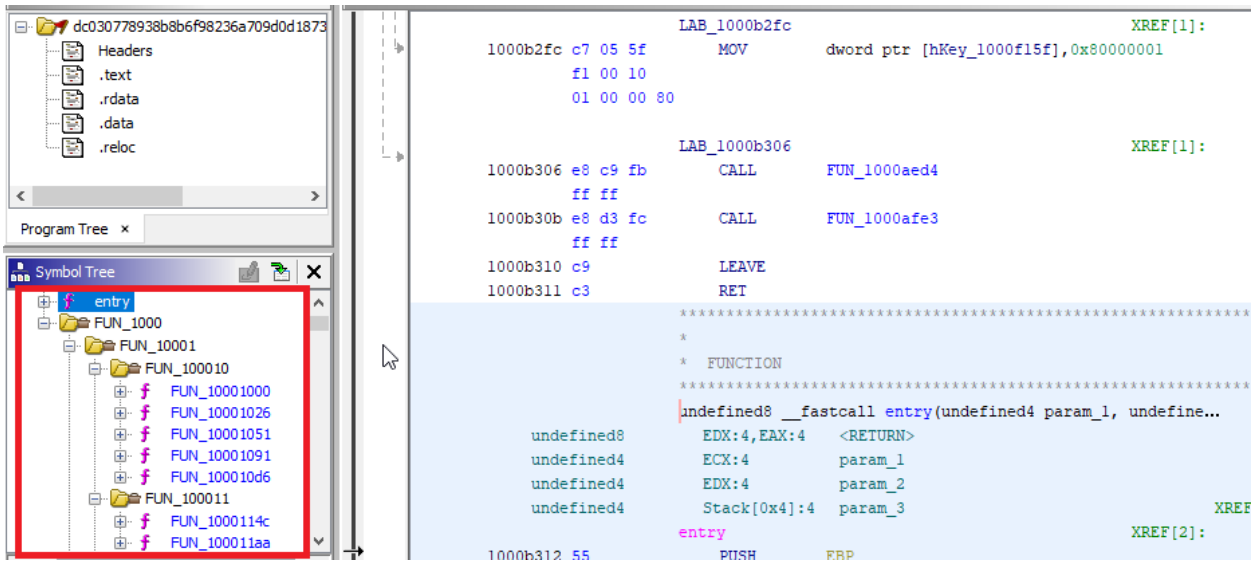


Figure 31: Malware-2: Different functions used by malware

Task-3 What is flow of functions in case of each malware? Is there any suspicious function? Give detail (name, arguments, call mechanism) of suspicious functions?

The flow of the funcitons of this malware is that if first collects the informaiton of the victim machine that includes name of host machine, username and password, collects the information of the victims facebocck account and collect the information of the mail server inclusing email accounts and then upload that details to some malicious link.

Task-3.1 FUN_10005

In this function malware collects the details of the victim host machine including the username, password, details of the remote directory and ots port number.

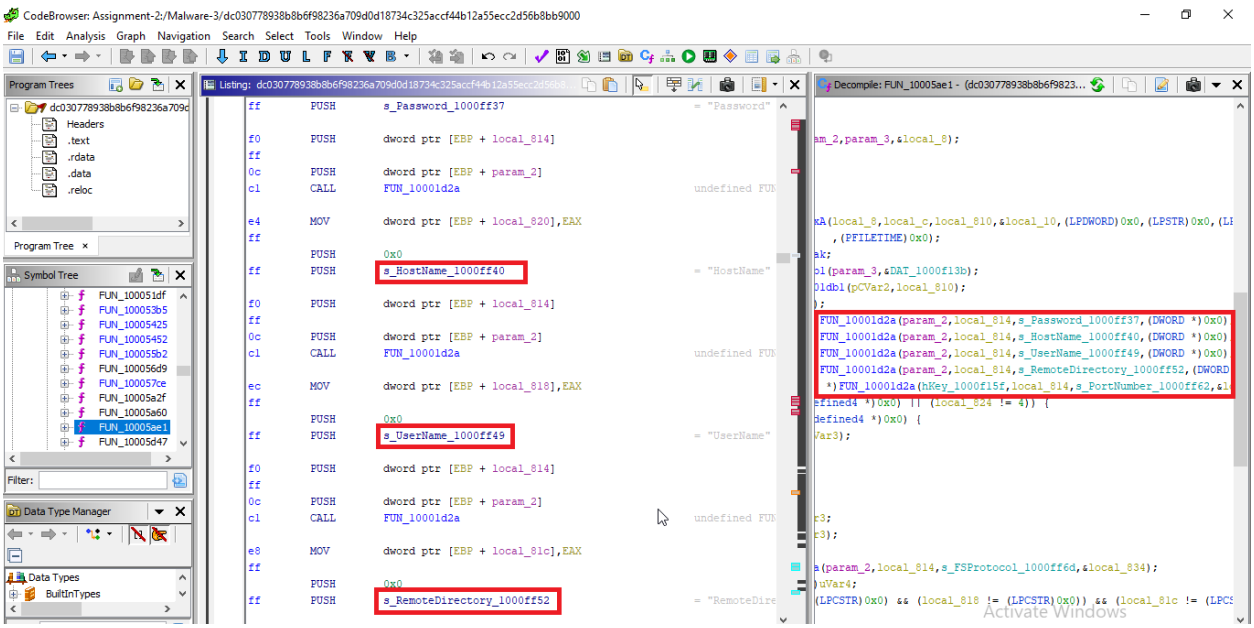


Figure 32: Malware-2: Malware capturing details of the host machine

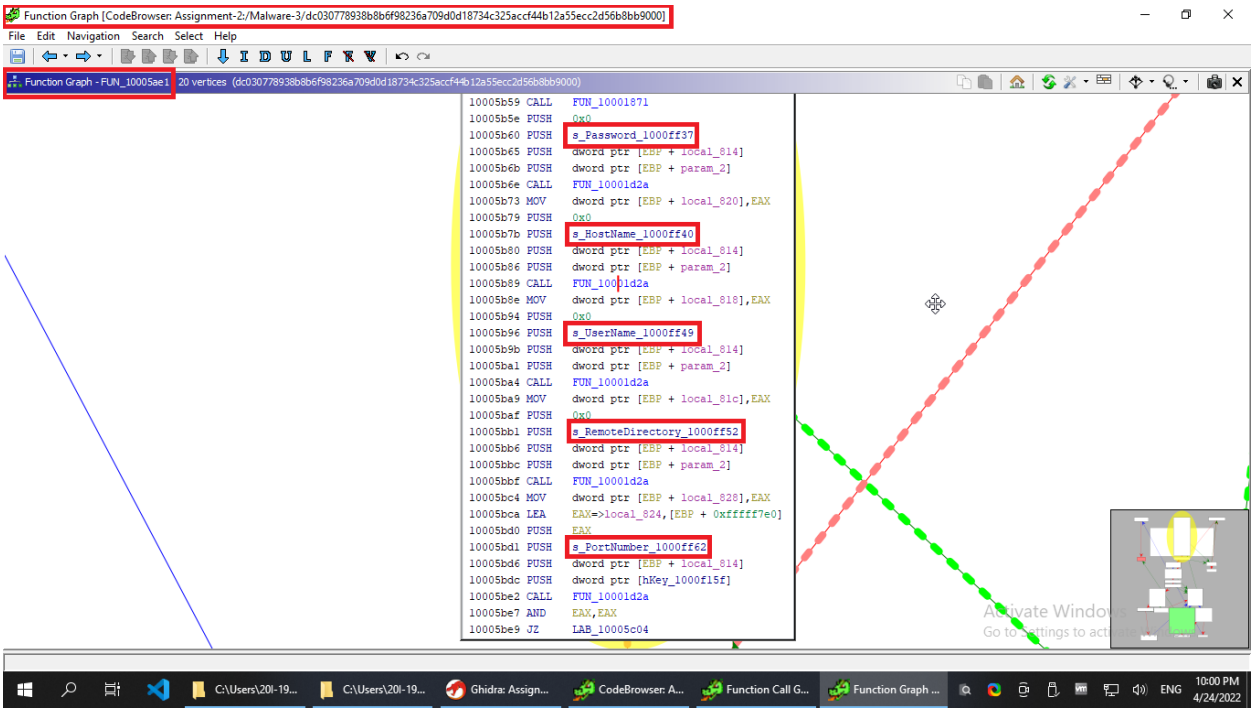


Figure 33: Malware-2: Malware capturing details of the host machine

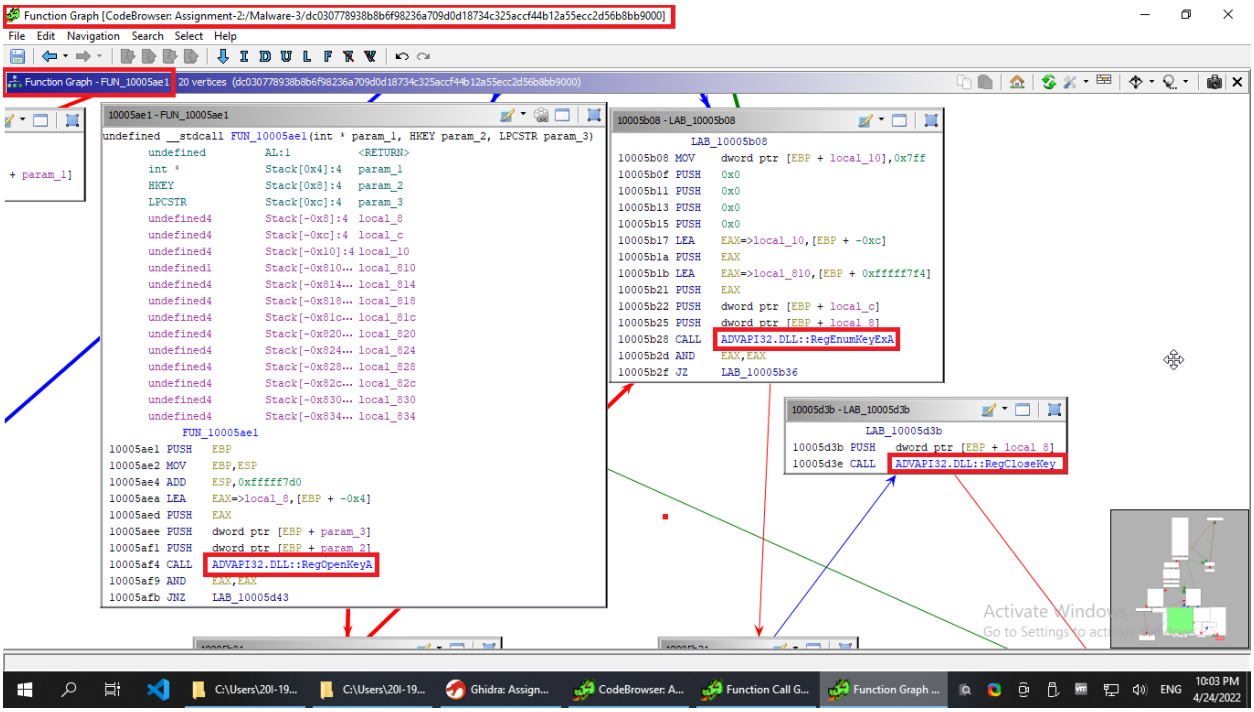


Figure 34: Malware-2: Malicious DLL fuctions used by malware

Task-3.2 05 FUN_100007

In this function malware collects the details of the victim facebook profile.

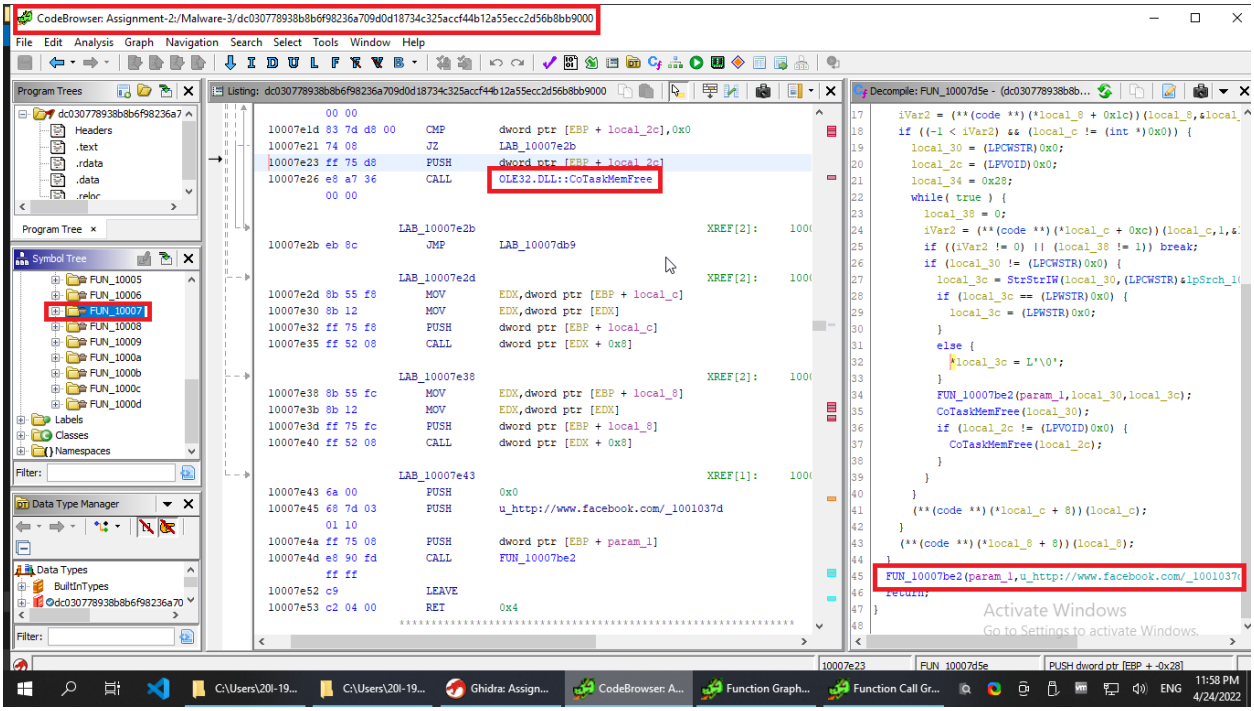


Figure 35: Malware-2: Gathering the details of Victims facebook account

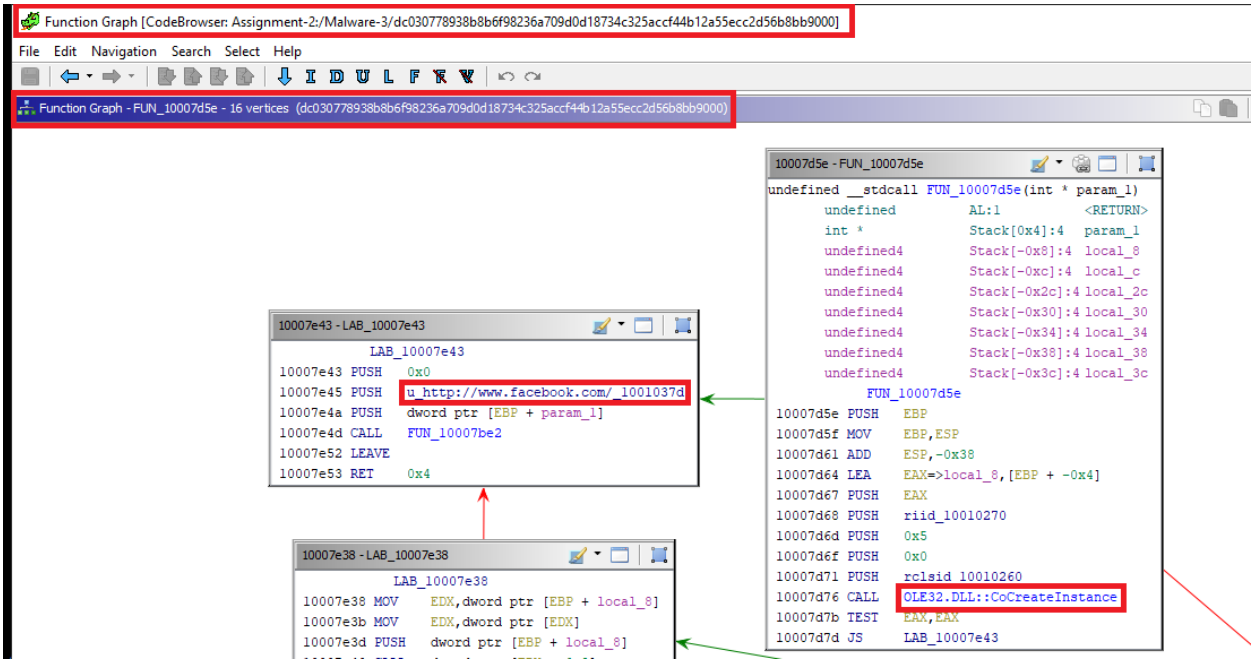


Figure 36: Malware-2: Gathering the details of Victims facebook account

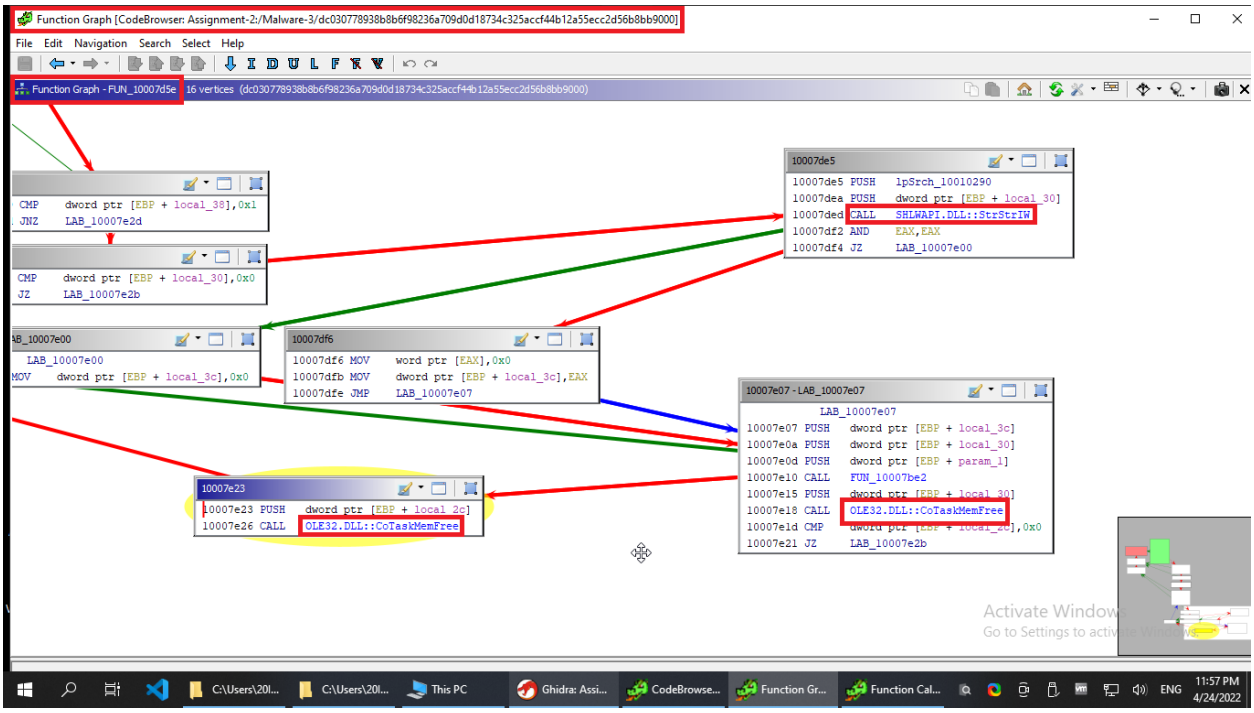


Figure 37: Malware-2: Malicious DLL fuctions used by malware

Task-3.3 FUN_10009

In this function malware collects the information of the victim email account including its email addres and password.

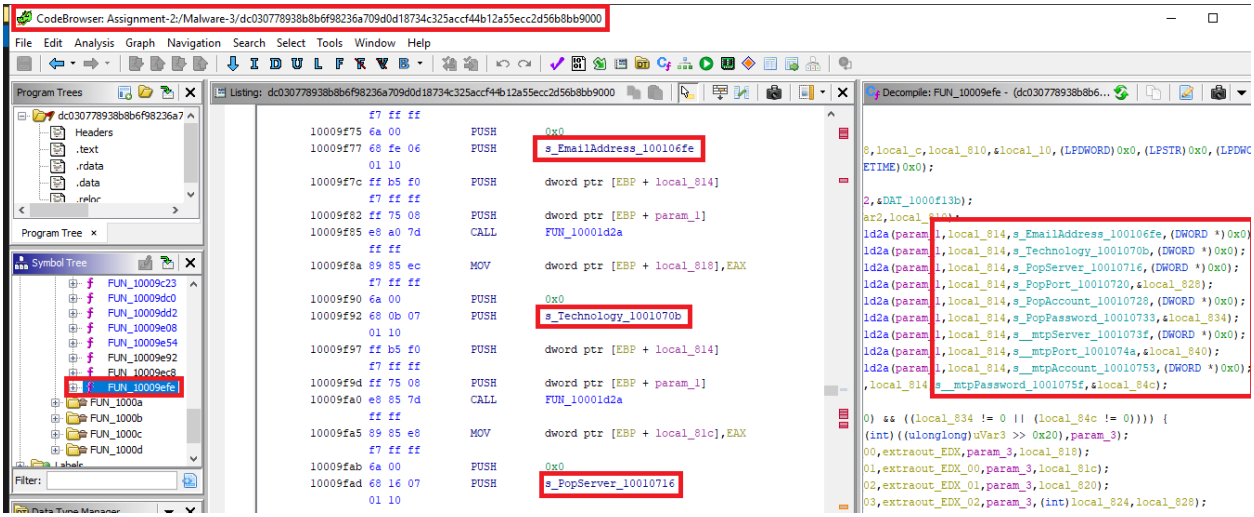


Figure 38: Malware-2: Malware collects the informaion of the email account of the victim

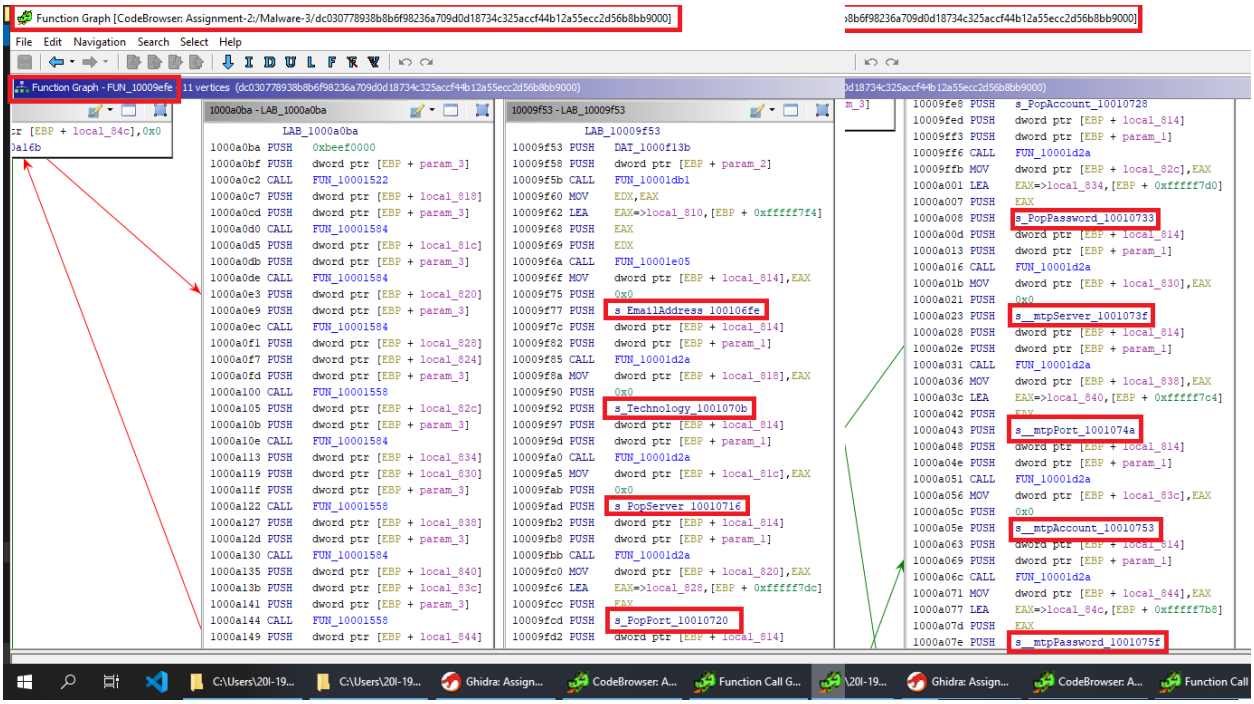


Figure 39: : Malware-2: Malware collects the informaion of the email account of the victim

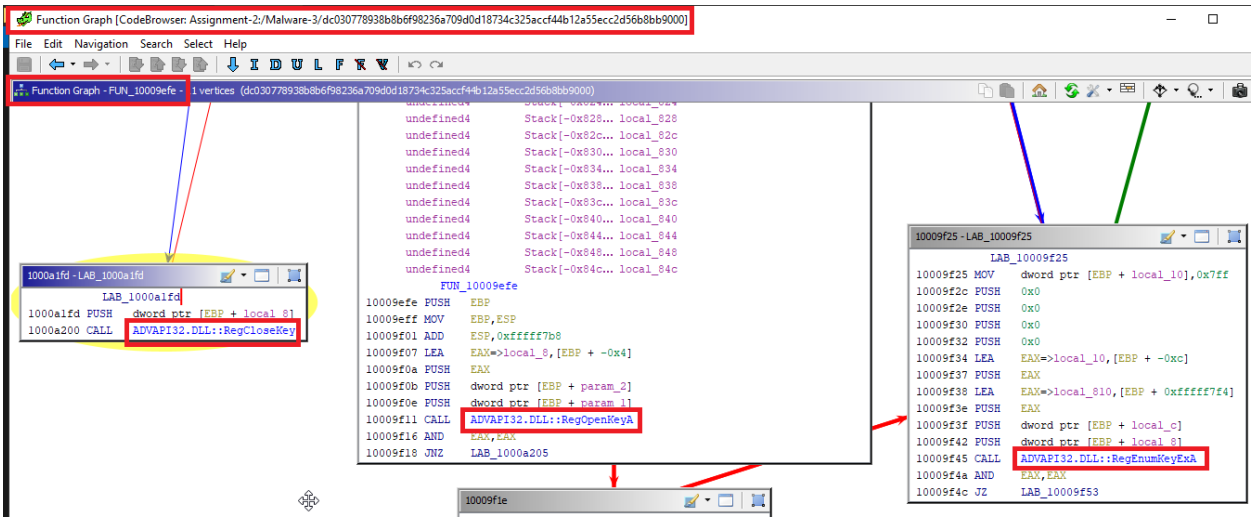


Figure 40: Malware-2: Malicious DLL fuctions used by malware

Task-3.4 FUN_10008

In this function malware connects to the some http and ftp server maybe to upload the collected informiton to attacker the server.

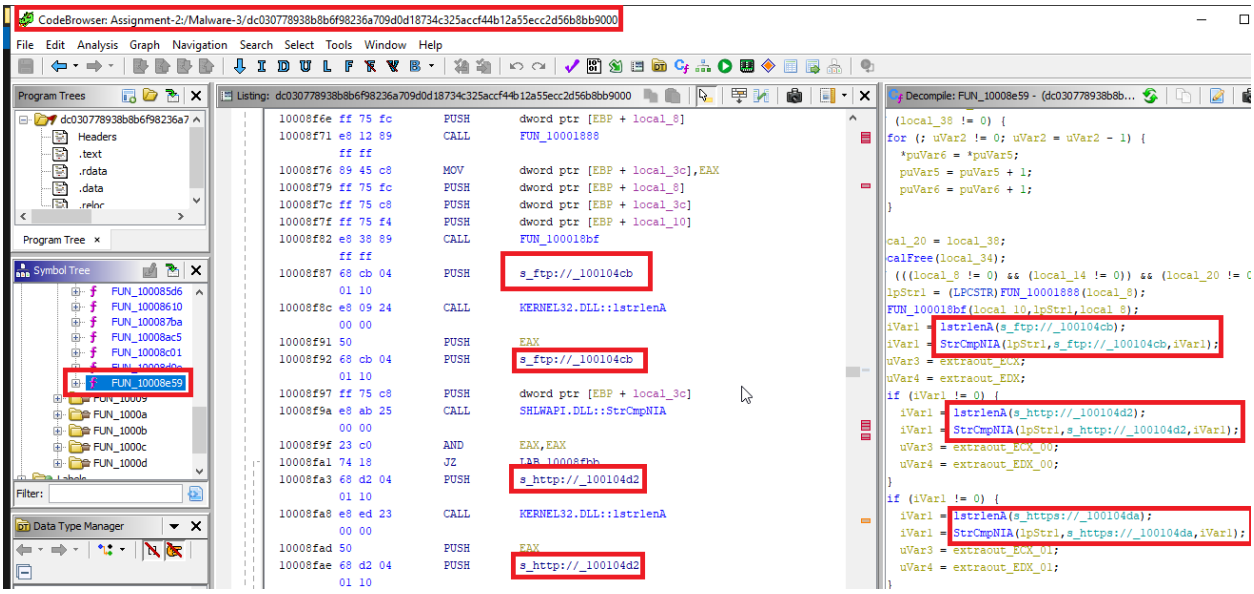


Figure 41: Malware-2: Connects to some malicious server

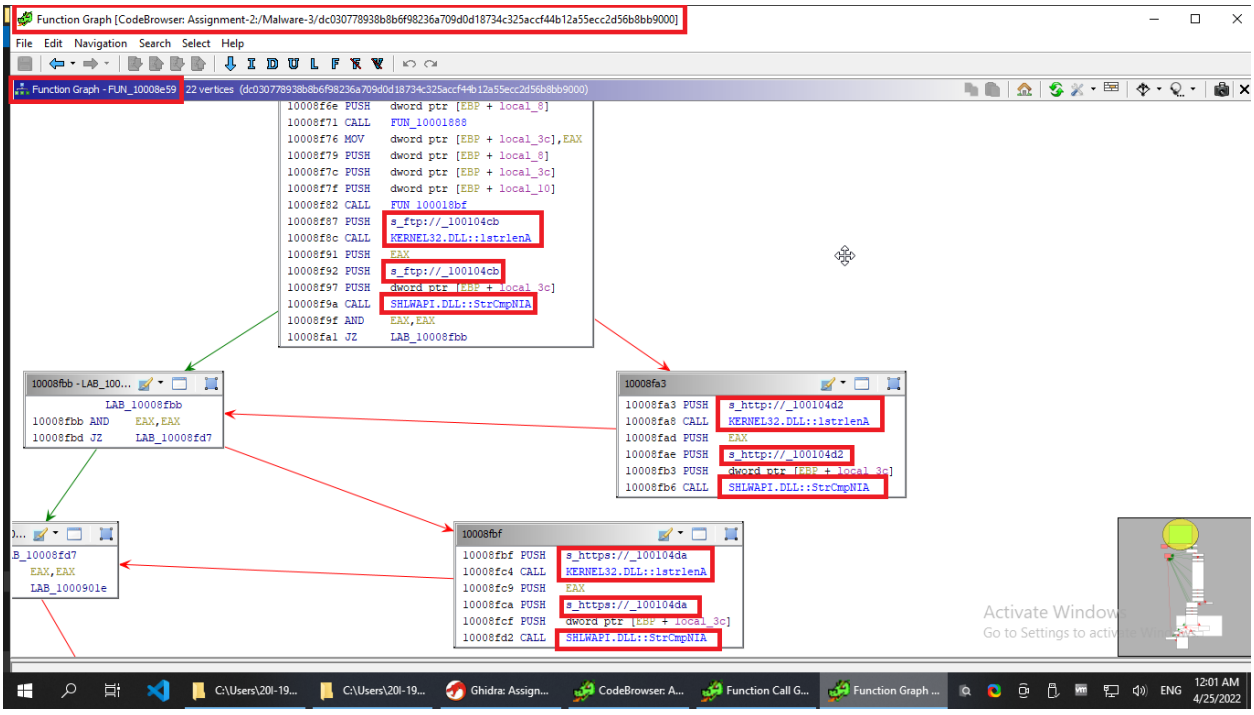


Figure 42: Malware-2: Connects to some malicious server also the DLL it used durint the process

Task-4 What DLL's any malware includes? Are there any suspicious functionality called by these DLL's?

The DLL's used by this malware includes "ADVAPI32.dll", "KERNEL32.dll", "OLE32.dll", "SHLWAPI.dll", "URLMON.dll", "USER32.dll", "USERENV.dll", "WININET.dll" and "WSOCK32.dll".

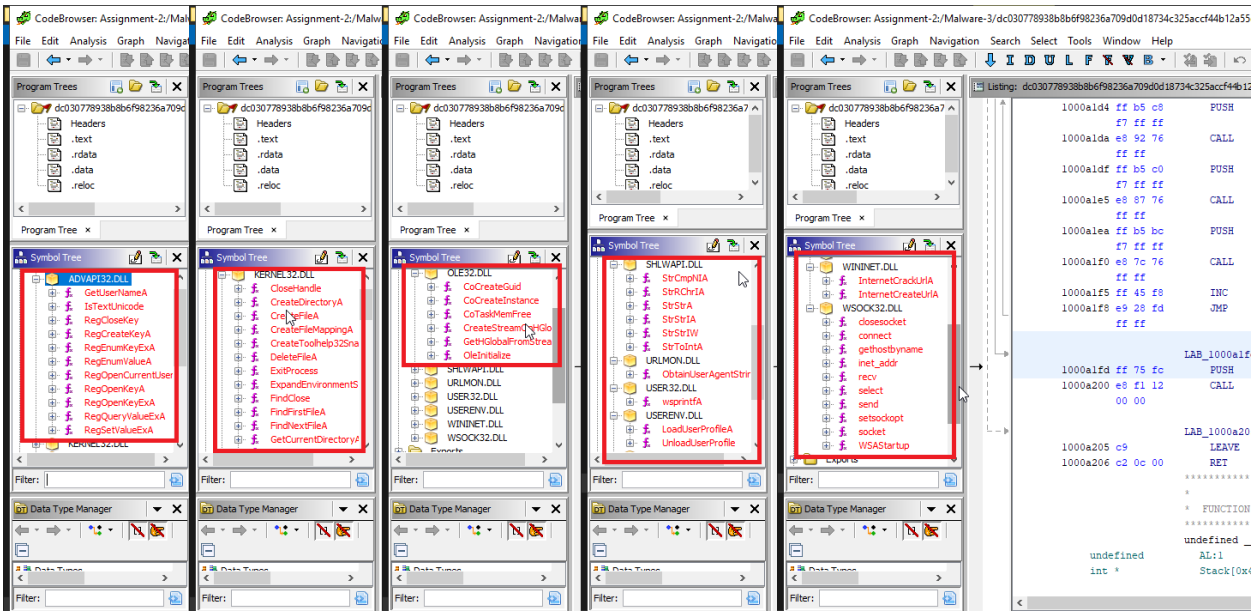


Figure 43: List of DLLs used by the malware with their functions

The suspicious functionality called by the DLLs includes the "ADVAPI32.dll" calling its function "RegOepenKeyA", "RegEnumKeyExA", and "RegCloseKey" when the malicious function of malware "FUN_10005ae1"collects the information of the victims host machine.

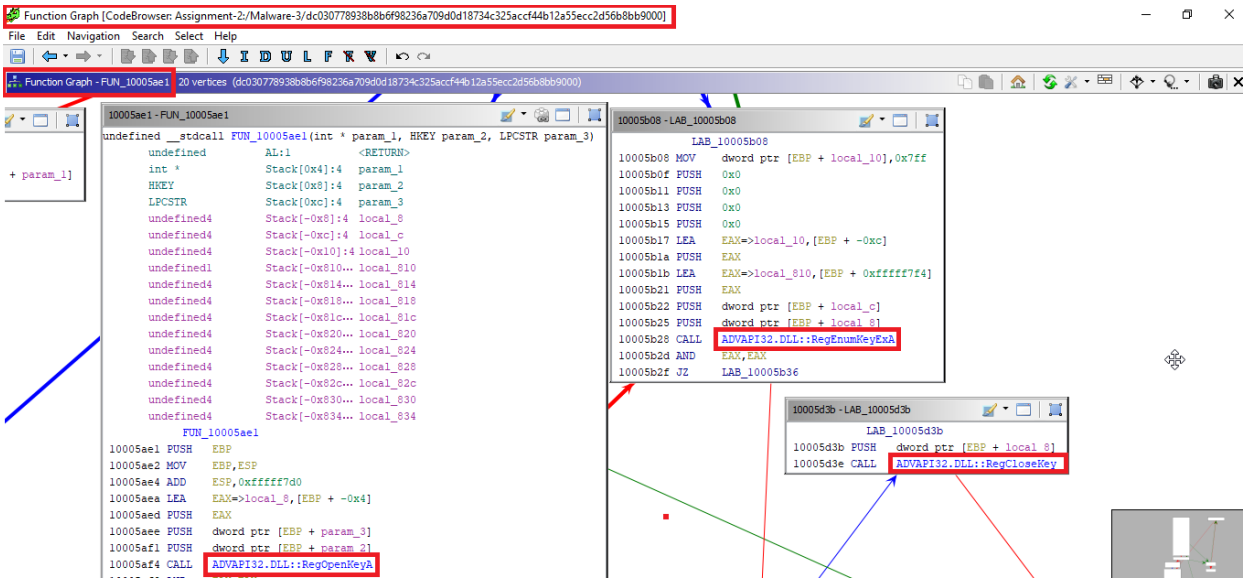


Figure 44: Malware-2 Malicious DLL functions used by malware

The suspicious functionality called by the DLLs includes the “OLE32.Dll” calling its function “CoCreateInstance”, “CoTaskMemFree”, and “SHLWAPI.dll” calling its function “StrStrIW” when the malicious function of malware “FUN_10007d5e”collects the information of the victims facebook profile.

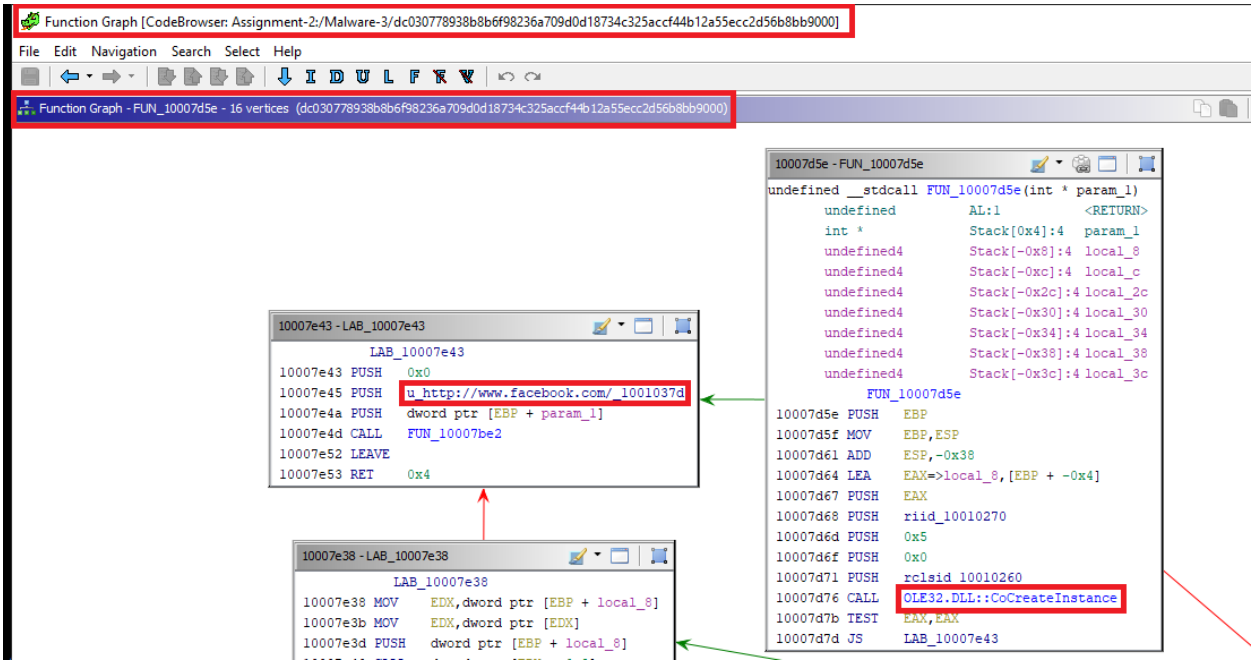


Figure 45: Malware-2 Malicious DLL functions used by malware

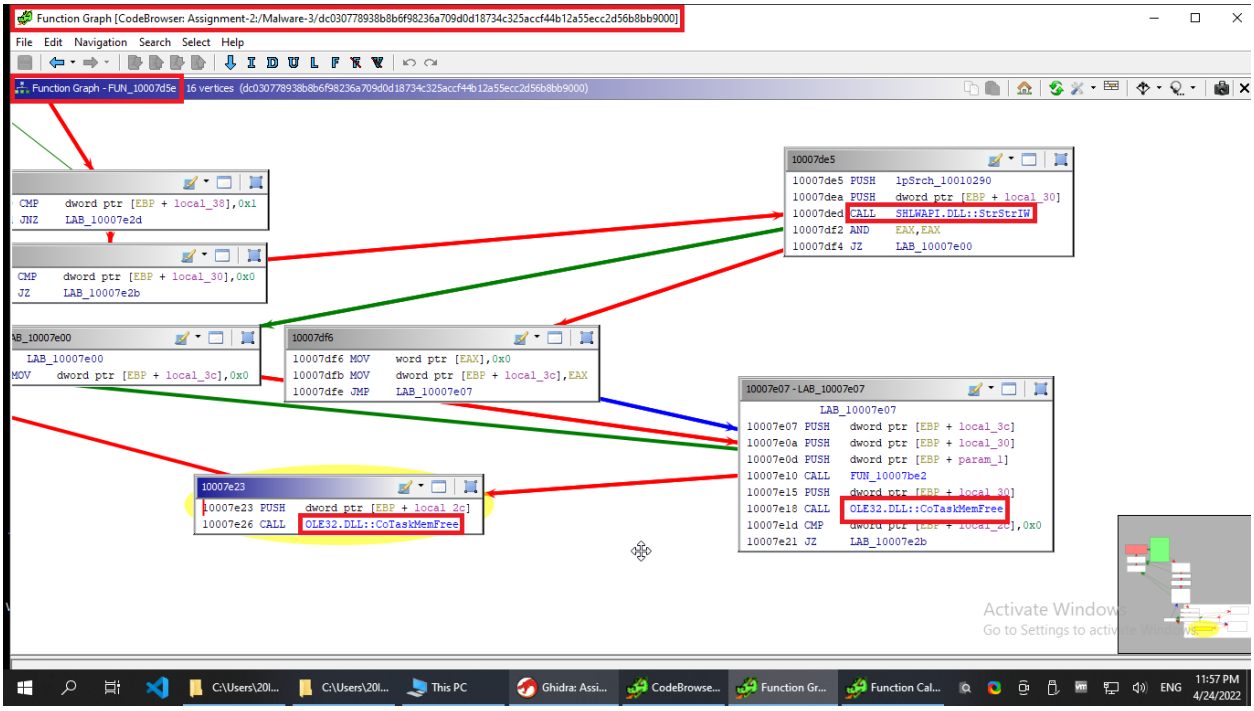


Figure 46: Malware-2 Malicious DLL functions used by malware

Another suspicious functionality called by the DLLs includes the “ADVAPI32.dll” calling its function “RegOepenKeyA”, “RegEnumKeyExA”, and “RegCloseKey” when the malicious function of malware “FUN_10009efe”collects the information of the victim email account including its email addres and password.

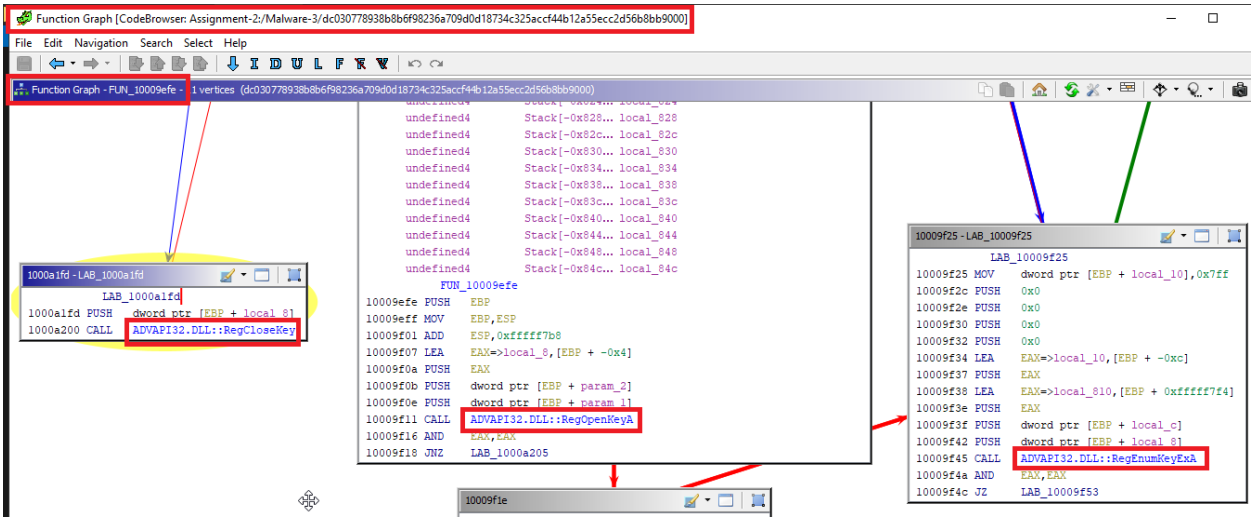


Figure 47: Malware-2 Malicious DLL functions used by malware

Another suspicious functionality called by the DLLs includes the “KERNEL32.dll” calling its function “lstrlenA” and “SHLWAPI.dll” calling its function “StrCmpNIA” when the malicious function of malware “FUN_10008e59”connects to some malicious http and ftp server.

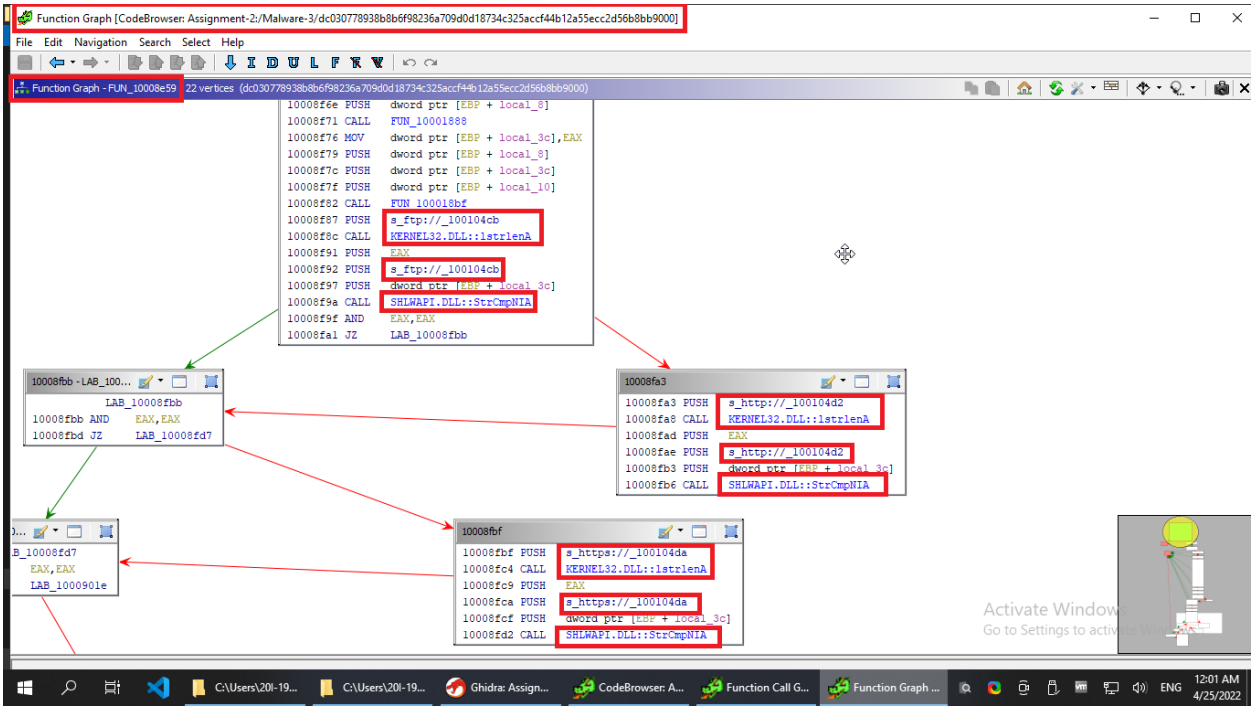


Figure 48: Malware-2 Malicious DLL functions used by malware

Malware-3 in32Tnega.bXRKZUB

This malware belongsto the family of trojans. To analyze malware I open it in Ghidra and then perform auto analysis on the malware sample.

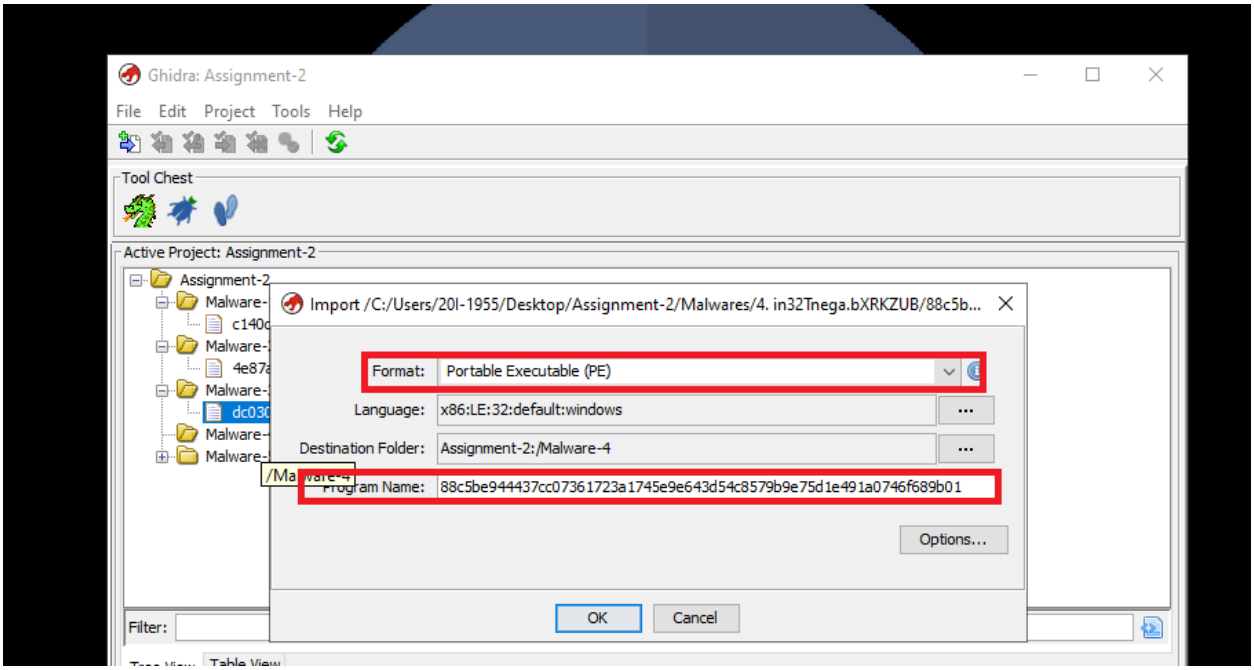


Figure 49: Malware-3: Opening malware in Ghidra

On opening the malware sample in the Ghidra I found that the malware is PE executable.

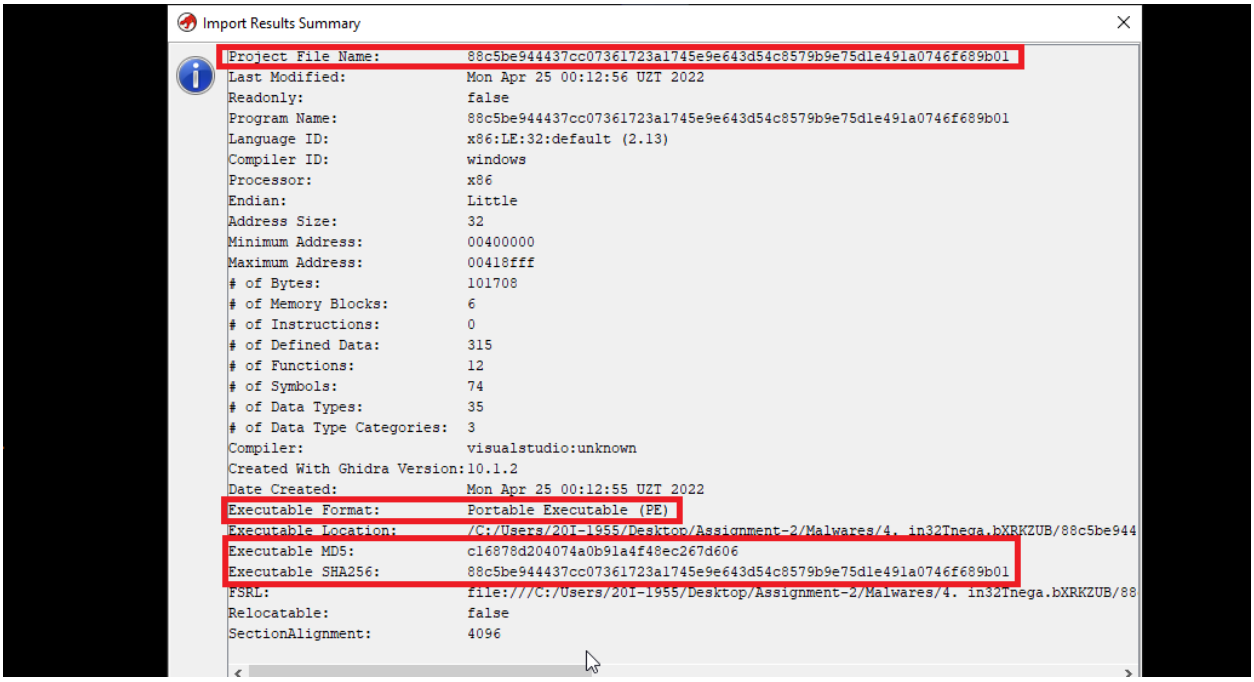


Figure 50: Malware-3: Basic details exreacted by Ghidra about the malware sample

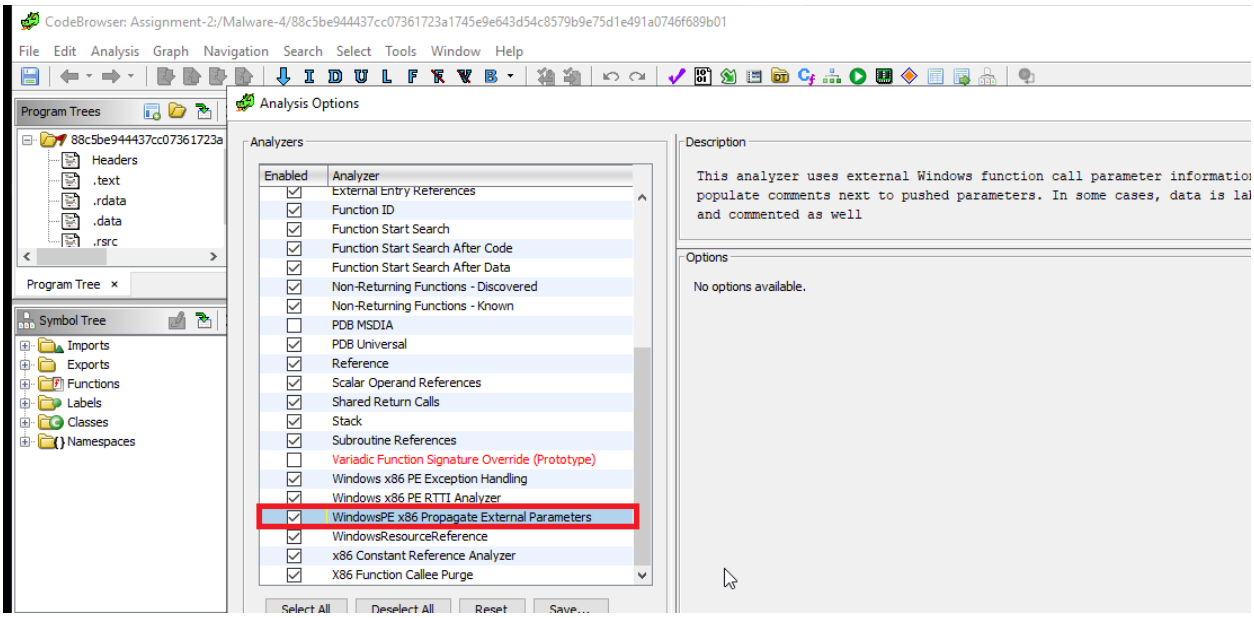


Figure 51: Malware-3: Ghidra auto analyze the malware

Task-1 What are the different segments or sections in case of each malware?

After Ghidra complete the auto analysis I found that the magic byte oif the malware which is MZ, moreover I found the details of different sections used by malware that includes ".text", ".rdata", ".data", ".rsrc".

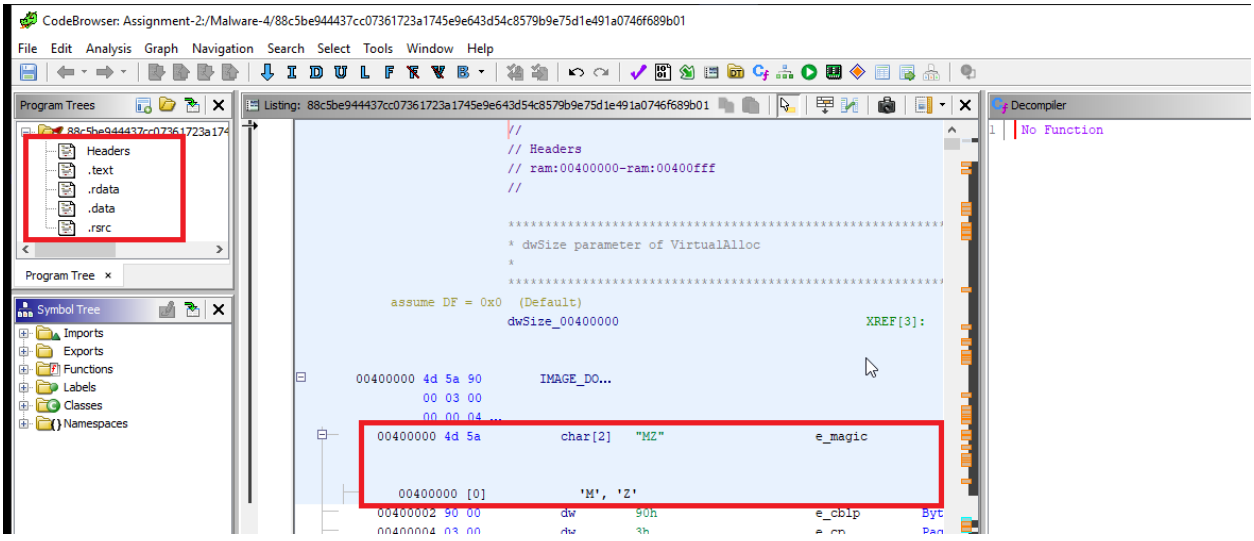


Figure 52: Malware-3: Magic byte and details of the sections used by malware

Task-2 What are different functions, imports and exports of each Malware?

To perform its functionality malware imports different DLL's that includes "KERNEL32.dll", "SHELL32.dll" and "USER32.dll". Moreover it also use different funcitons to perform it functionality.

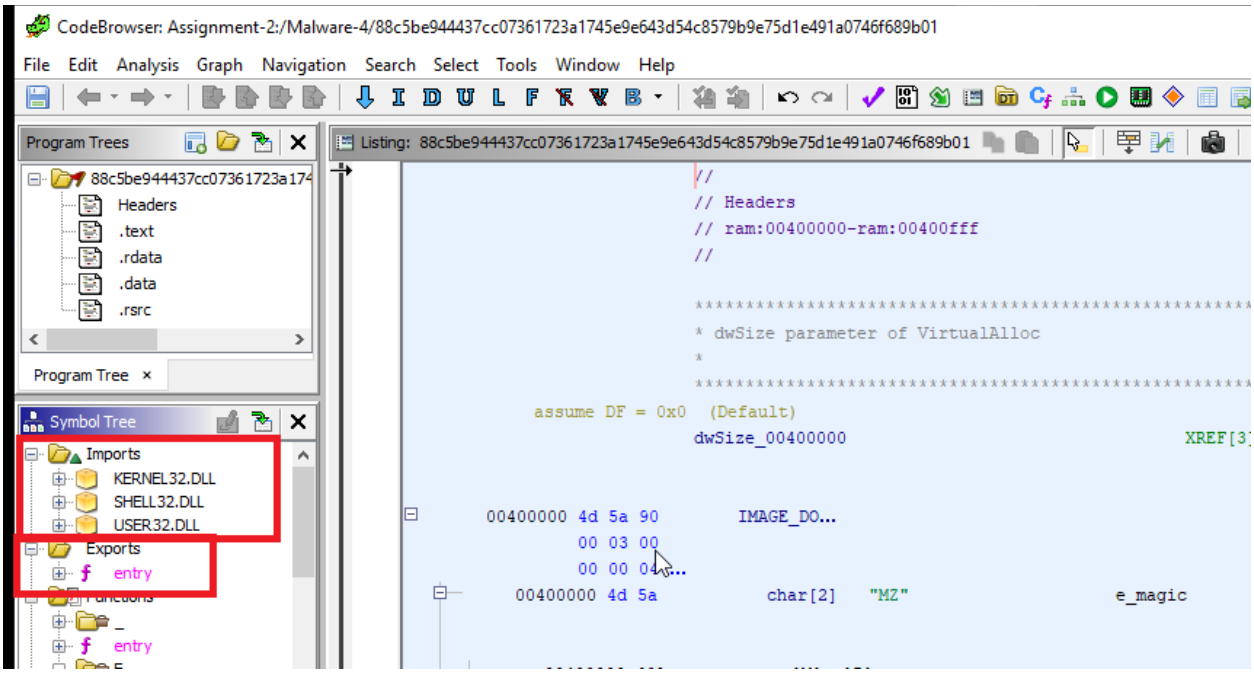


Figure 53: Malware-3: Details of the functions, imports and exports used by malware

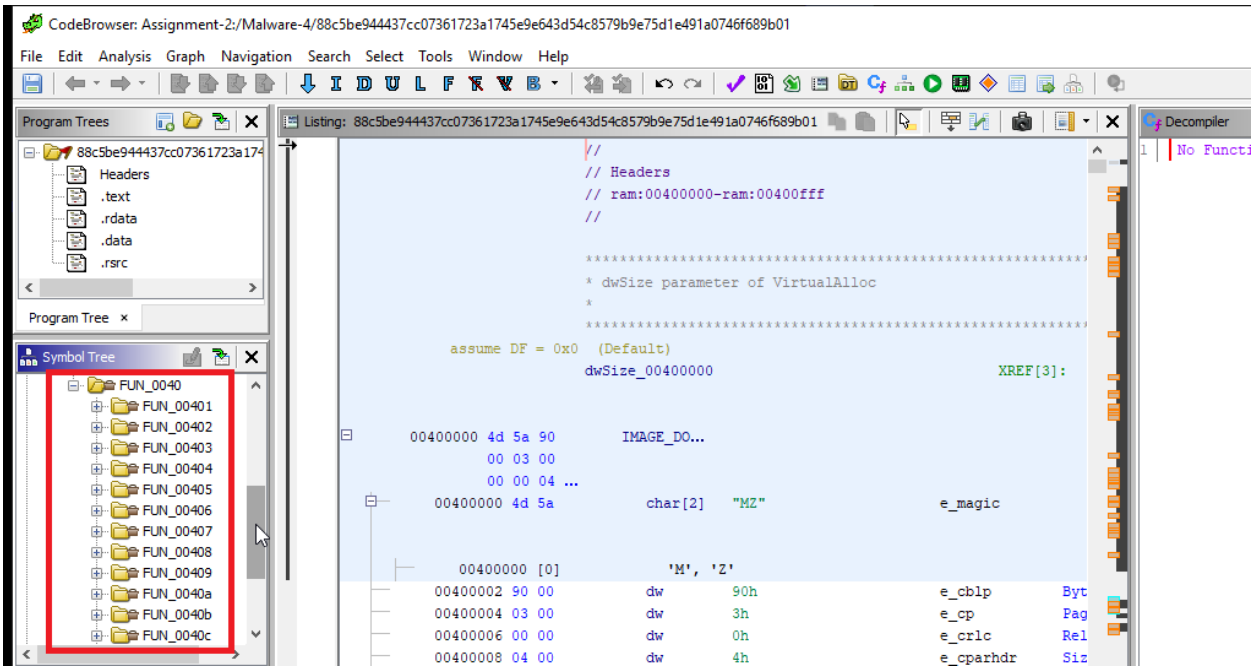


Figure 54: Malware-3: Different functions used by malware

Task-3 What is flow of functions in case of each malware? Is there any suspicious function? Give detail (name, arguments, call mechanism) of suspicious functions?

The flow of the funcitons of this malware is that it installs some malicious software on the victim machine without notifying him/her.

Task-3.1 FUN_00401550

In this function malware collects information of the running processes and then install some malicious software on the victim machine.

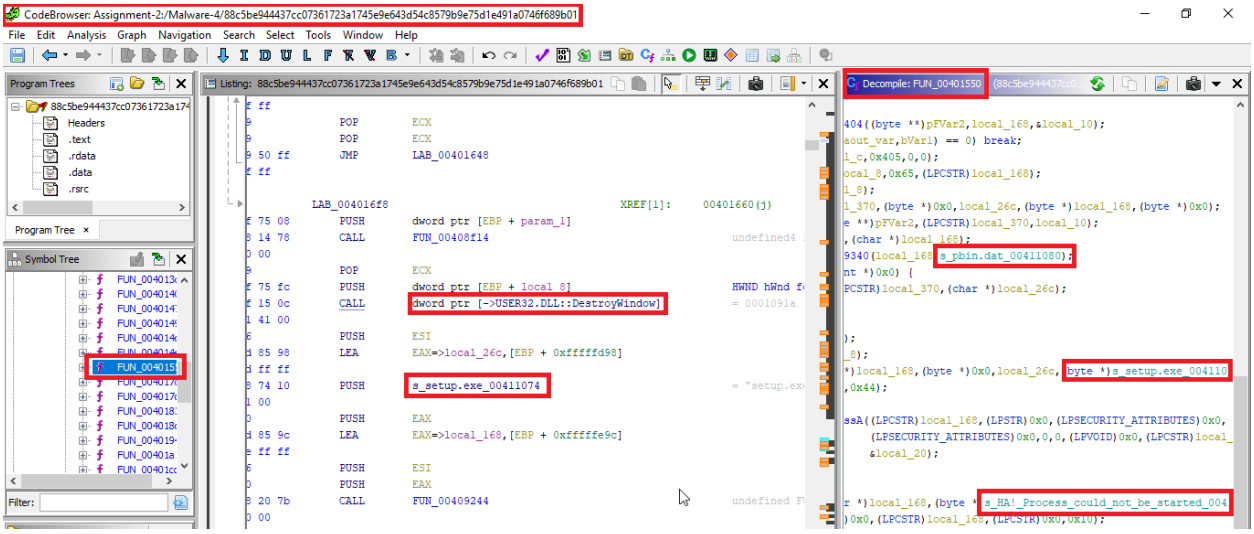


Figure 55: Malware-3: Malware collects the information of the running process and instlling some malicious software

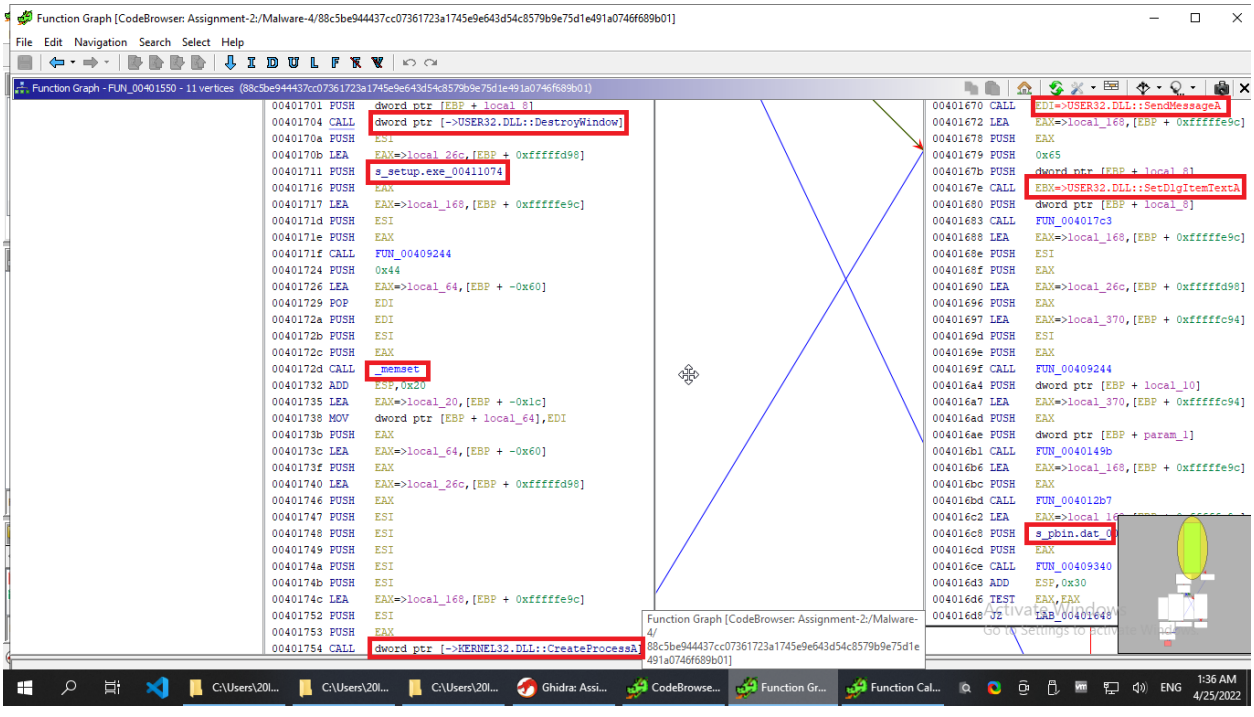


Figure 56: Malware-3: Malware installing some malicious softeare on victim mahcine

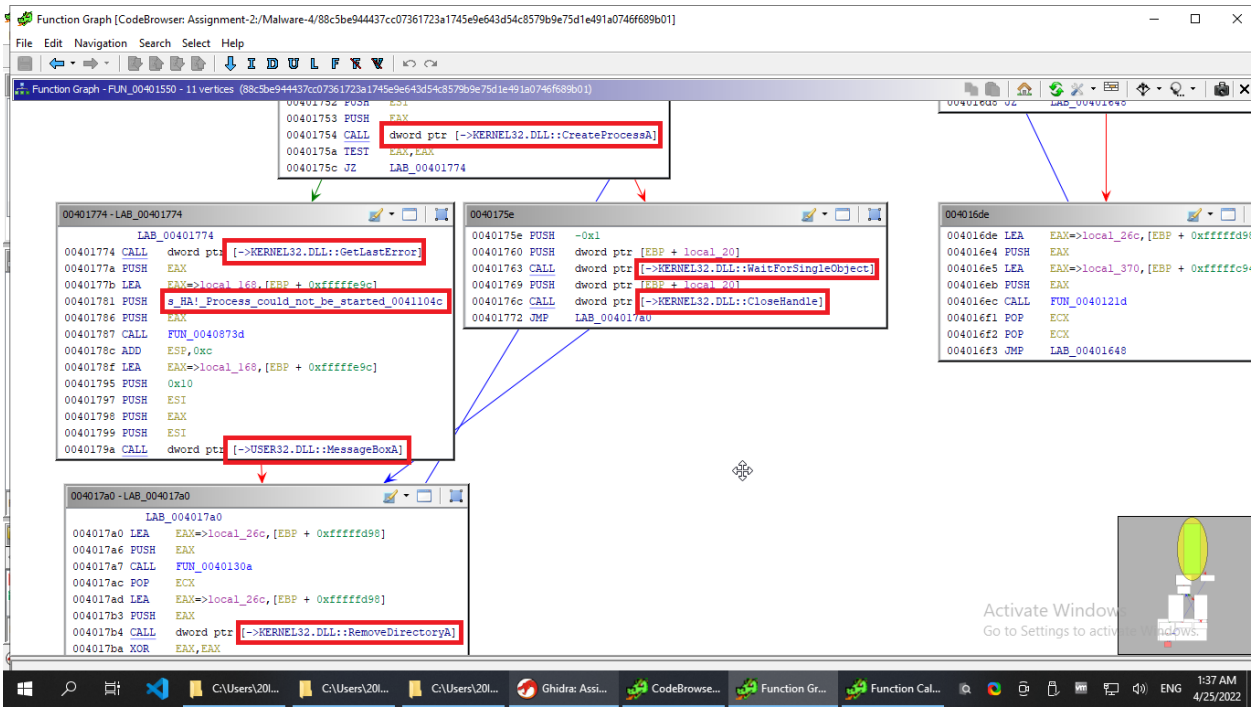


Figure 57: Malware-3: Malicious DLL fuctions used by malware

Task-4 What DLL's any malware includes? Are there any suspicious functionality called by these DLL's?

The DLL's used by this malware includes "KERNEL32.dll", "SHELL32.dll" and "USER32.dll".

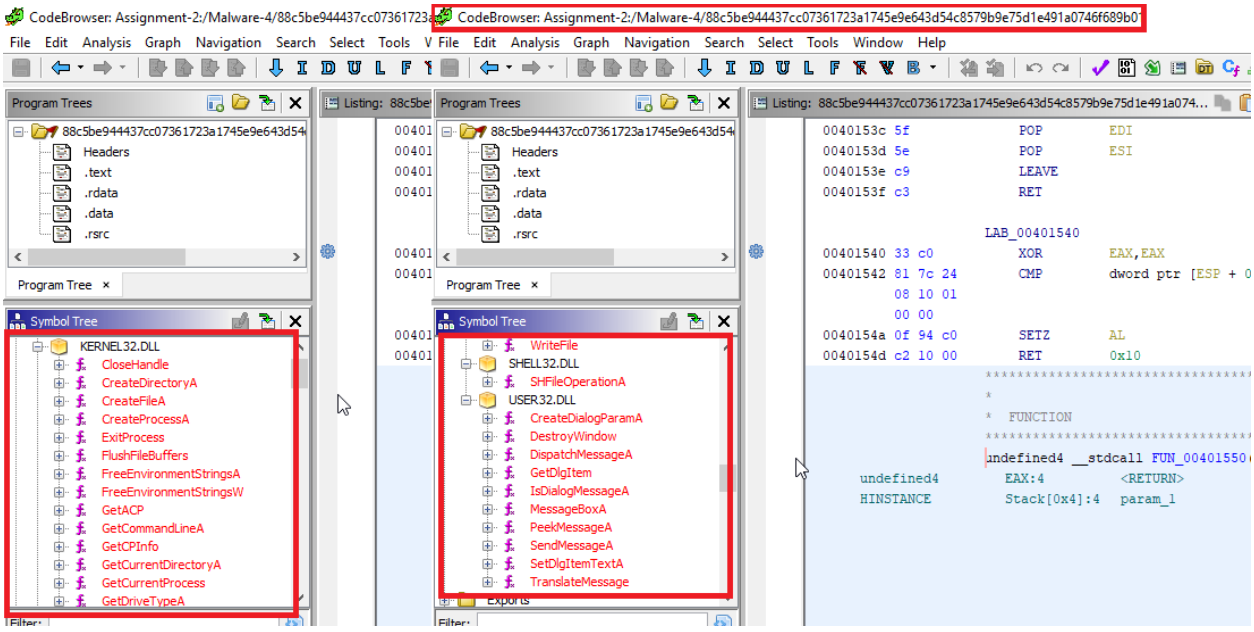


Figure 58: List of DLLs used by the malware with their functions

The suspicious functionality called by the DLLs includes the "User32.Dll" calling its function "SendMessageA", "SetGlgItemTextA", "DestroyWindow" and "MessageBoxA" and "KERNEL32.dll" calling

its funcitons “CreateProcessA”, “RemoveDirectoryA”, “Wait ForSingleObject” and “CloseHandle” when the malicious function of malware “FUN_00401550”installs some malicious software on victims machine.

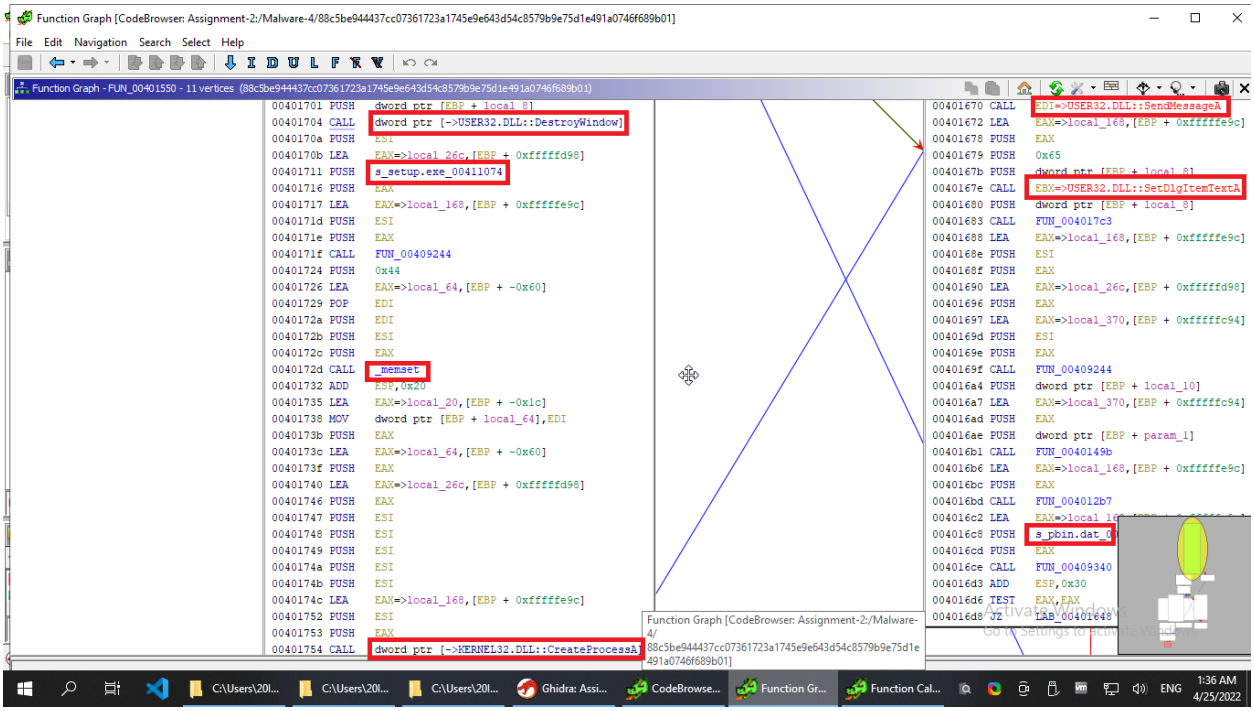


Figure 59: Malware-3 Malicious DLL functions used by malware

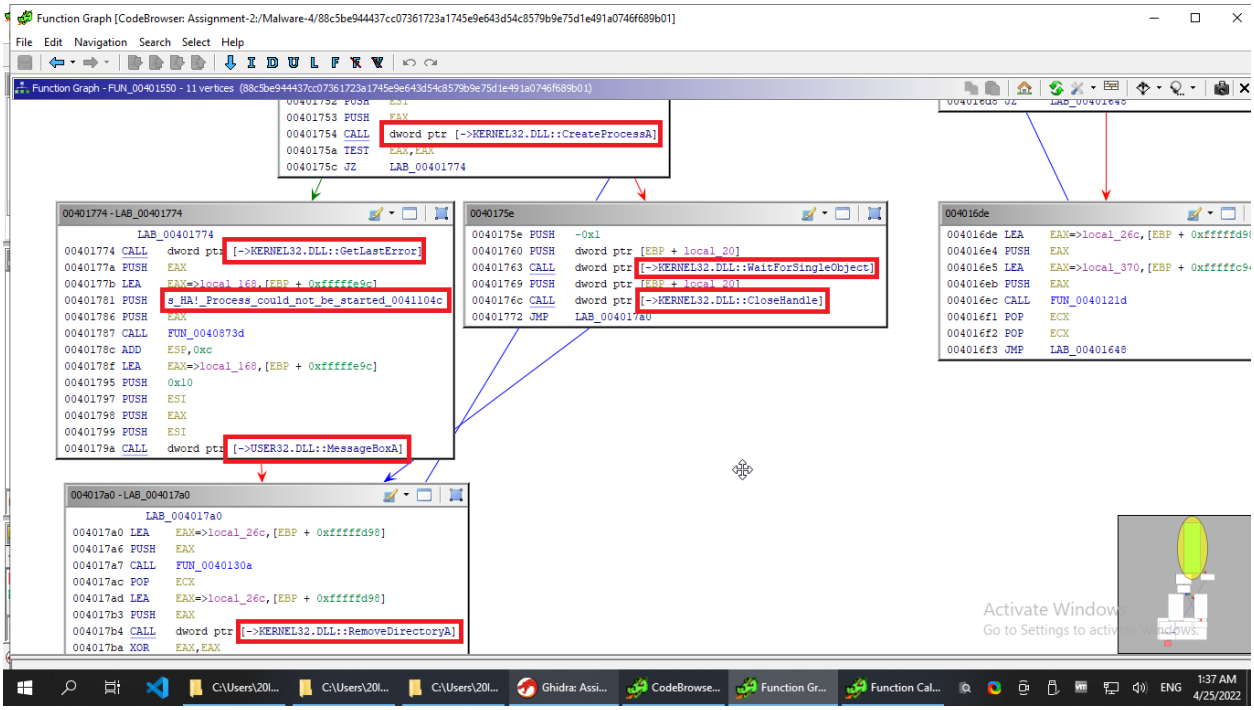


Figure 60: Malware-3 Malicious DLL functions used by malware

Malware-4 Trojan.GenericKD.3652107

This malware belongsto the family of trojans. To analyze malware I open it in Ghidra and then perform auto analysis on the malware sample.

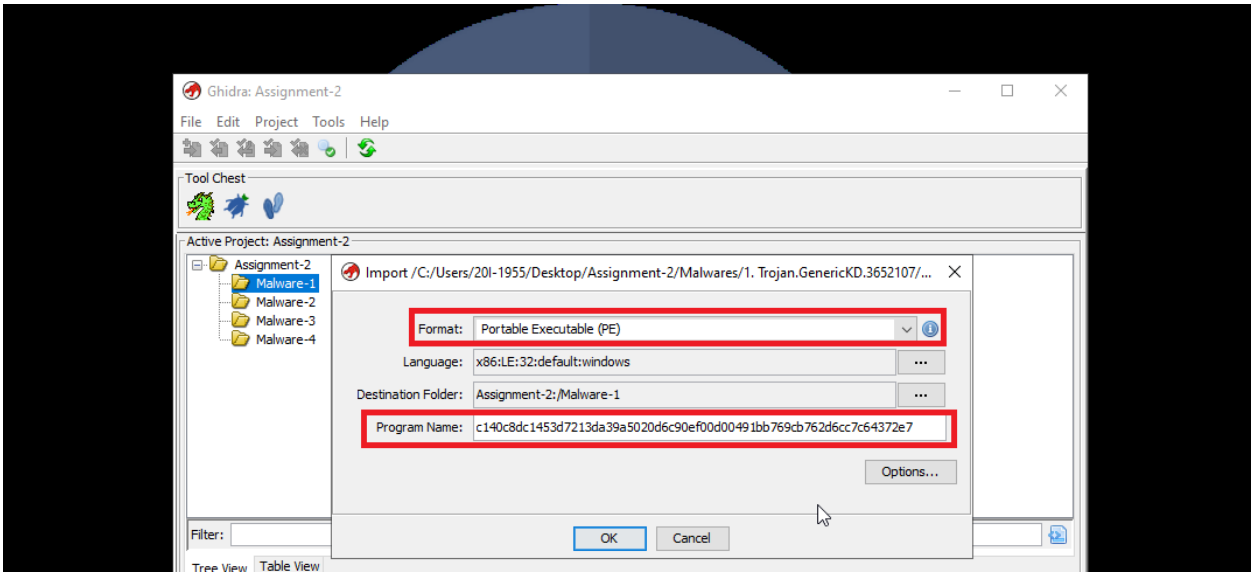


Figure 61: Malware-4: Opening malware in Ghidra

On opening the malware sample in the Ghidra I found that the malware is PE executable.

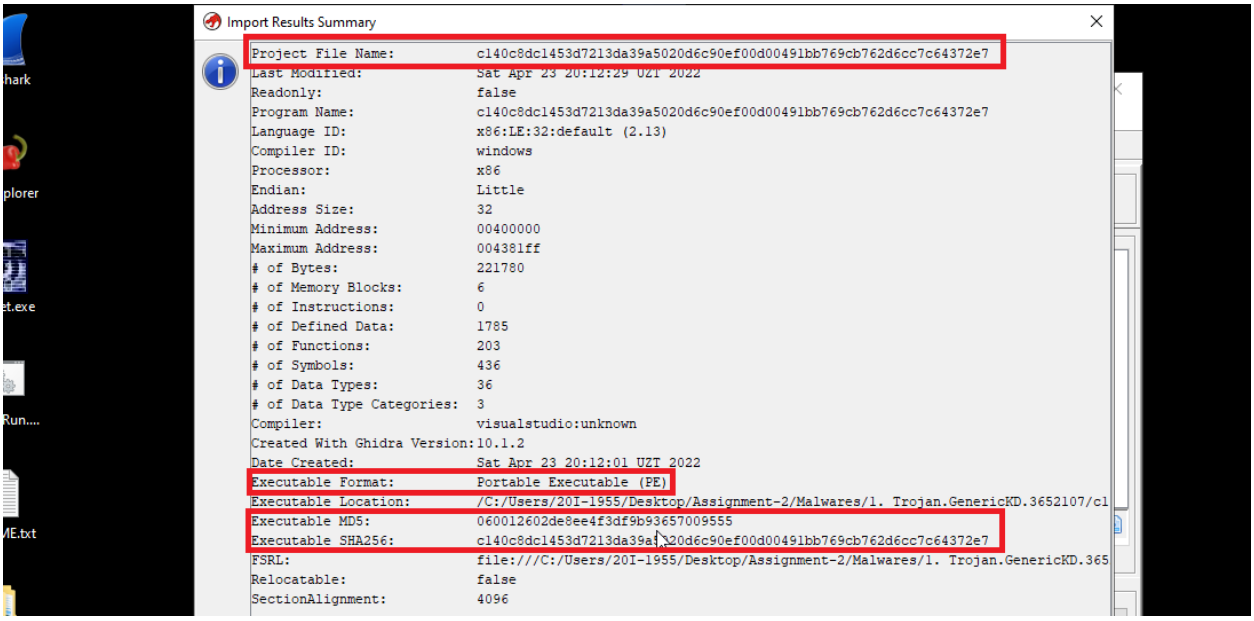


Figure 62: Malware-4: Basic details exreacted by Ghidra about the malware sample

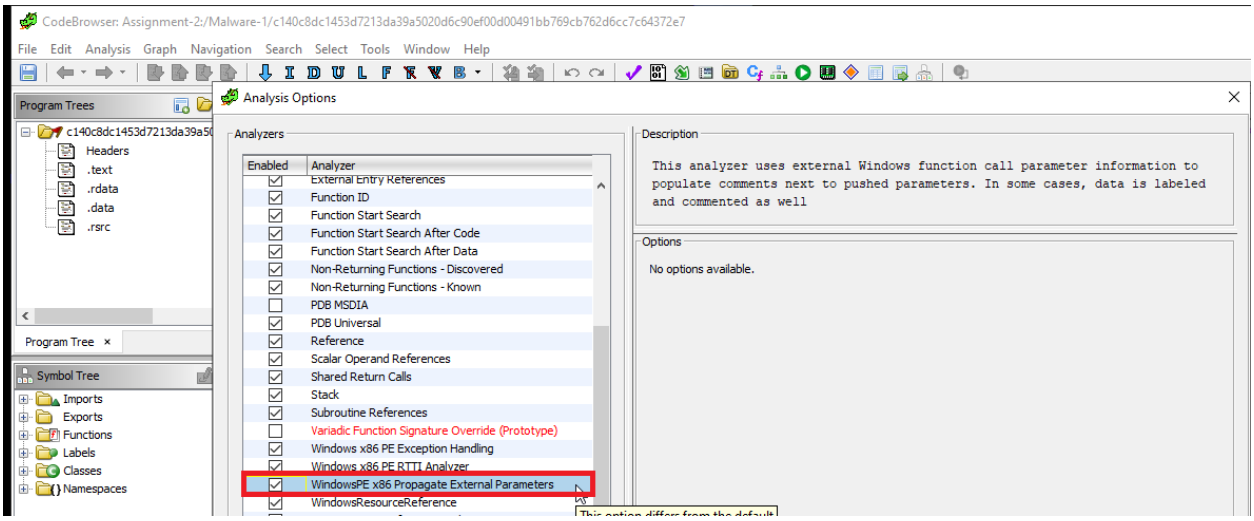


Figure 63: Malware-4: Ghidra auto analyze the malware

Task-1 What are the different segments or sections in case of each malware?

After Ghidra complete the auto analysis I found that the magic byte oif the malware which is MZ, moreover I found the details of different sections used by malware that includes ".text", ".rdata", ".data", ".rsrc".

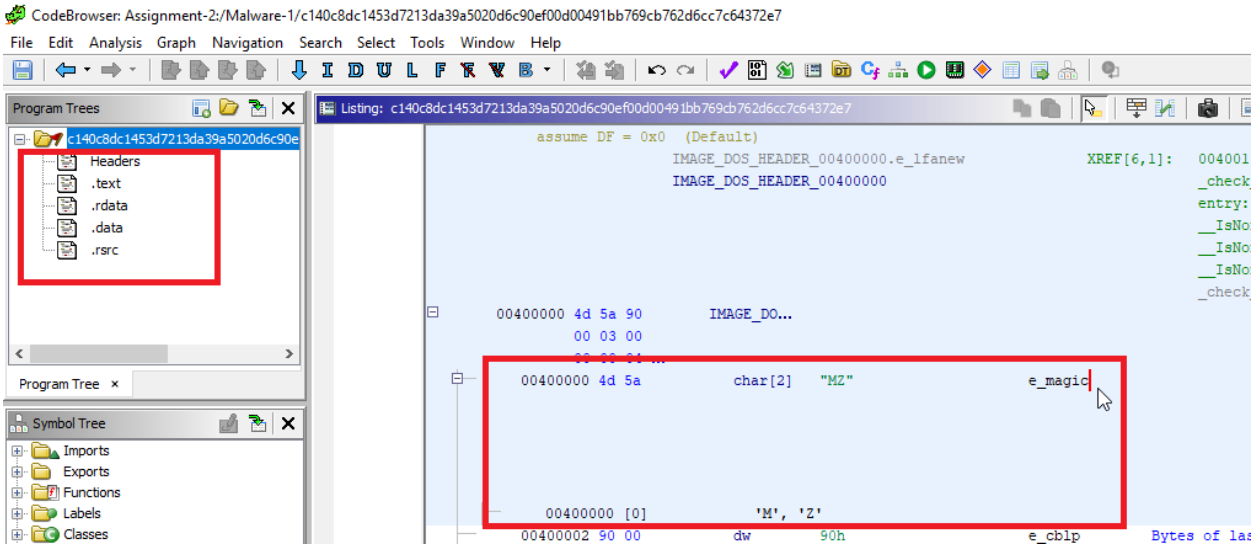


Figure 64: Malware-4: Magic byte and details of the sections used by malware

Task-2 What are different functions, imports and exports of each Malware?

To perform its functionality malware imports different DLL's that includes "ADVAPI32.dll", "COMCTL32.dll", "GDI32.dll", "KERNEL32.DLL", "OLE32.DLL", "SHELL32.dll", "SHLWAPI.dll","USER32.dll" and "VERSION.dll". Moreover it also use different funcitons to perform it functionality.

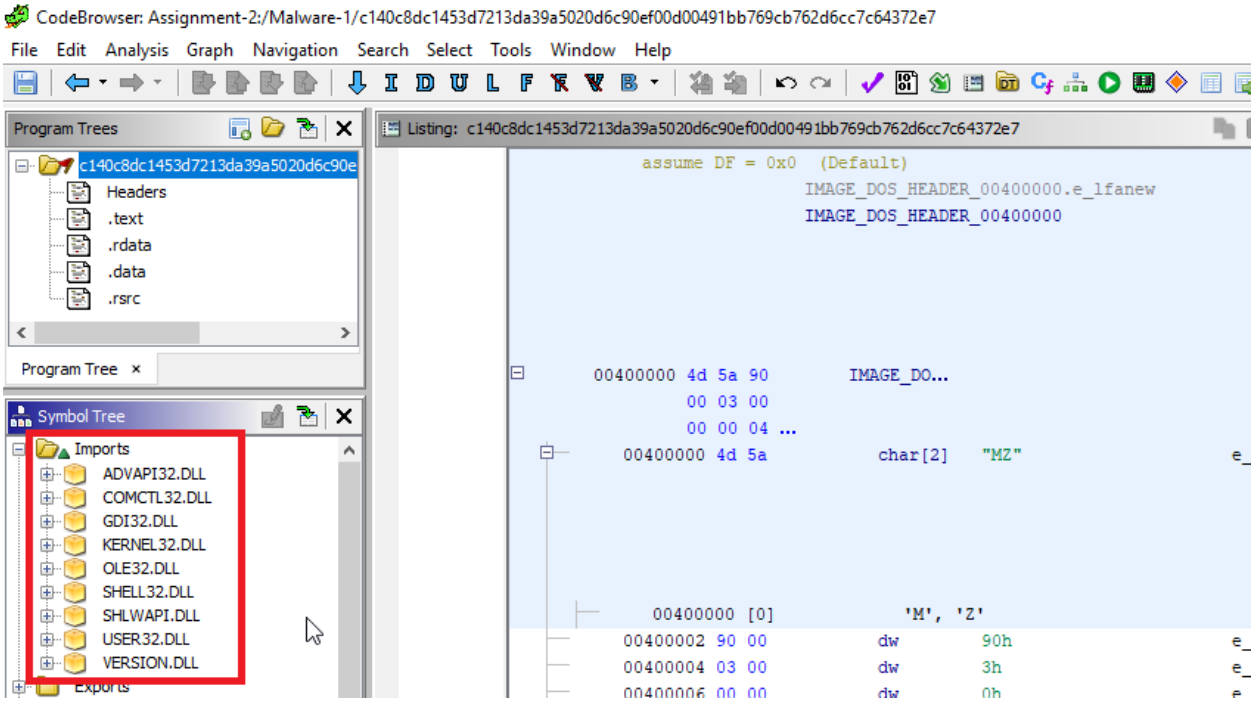


Figure 65: Malware-4: Details of the functions, imports and exports used by malware

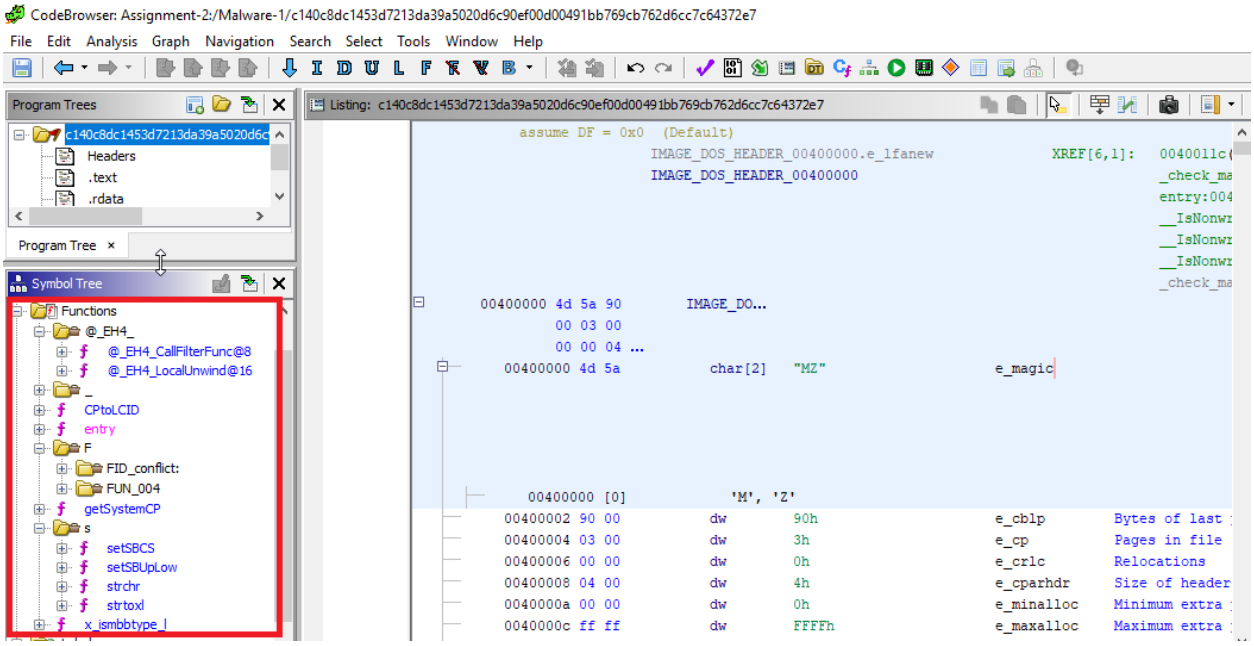


Figure 66: Malware-4: Different functions used by malware

Task-3 What is flow of functions in case of each malware? Is there any suspicious function? Give detail (name, arguments, call mechanism) of suspicious functions?

The flow of the funcitons of this malware is that it initialize the critical section, enter into the critical section perform sme malicious actions there and then deletes that critical section.

Task-3.1 FUN_crtInitCritSecNoSpinCount

In this function malware initialize the critical section to access it to perform malicious action.

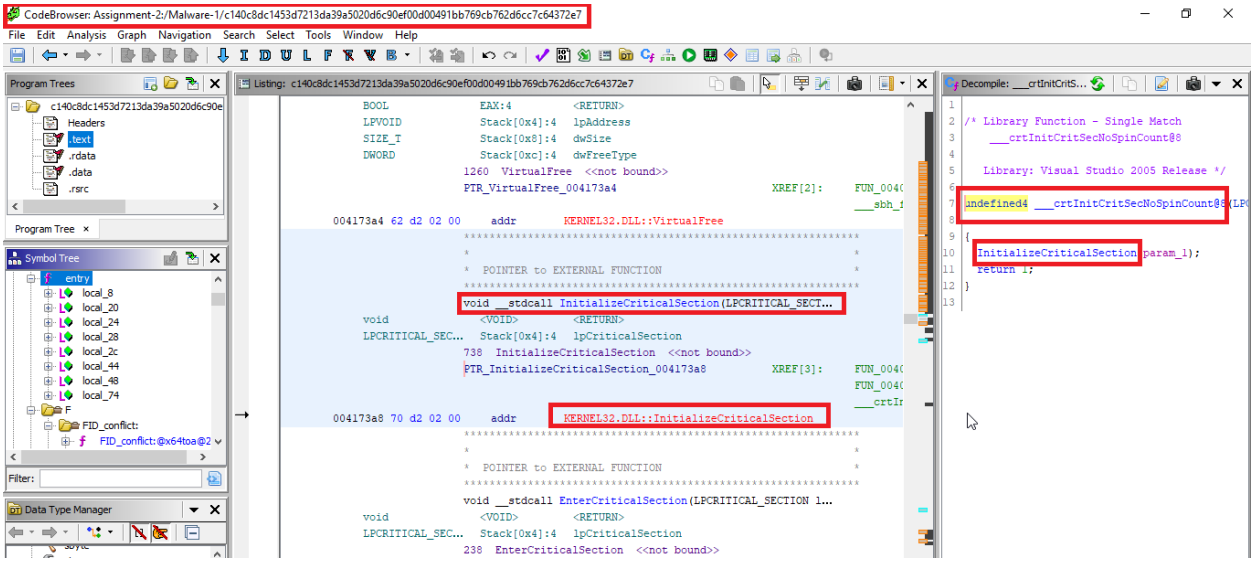
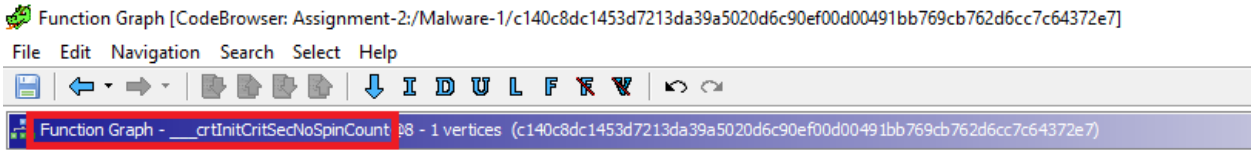


Figure 67: Malware-4: Malware initialize the critical section



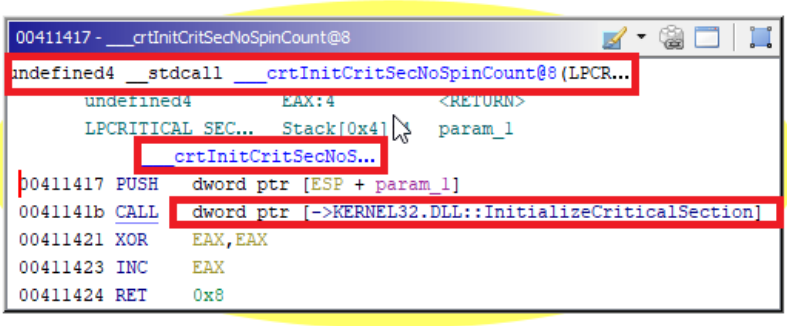


Figure 68: Malware-4: Malicious DLL fuctions used by malware

Task-3.2 FUN_lock_file2

In this function malware enter to the critical section to access it to perform malicious action.

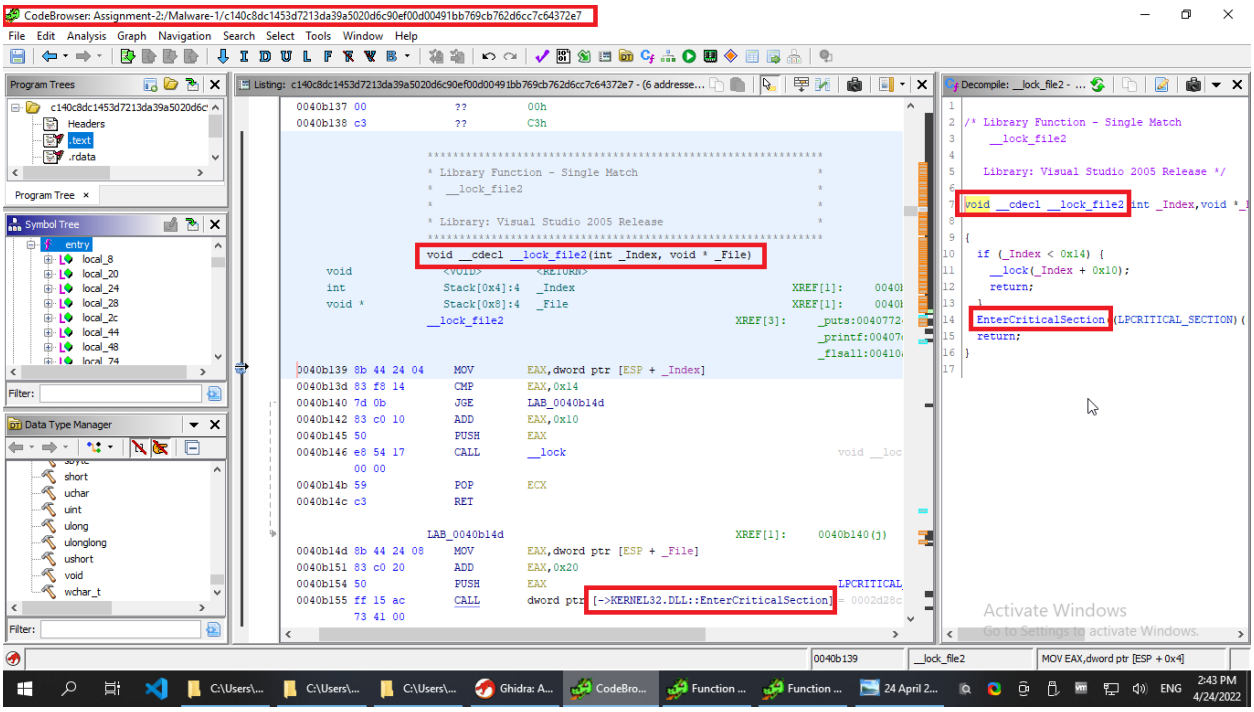


Figure 69: Malware-4: Malware enters into the critical section to perform malicious action

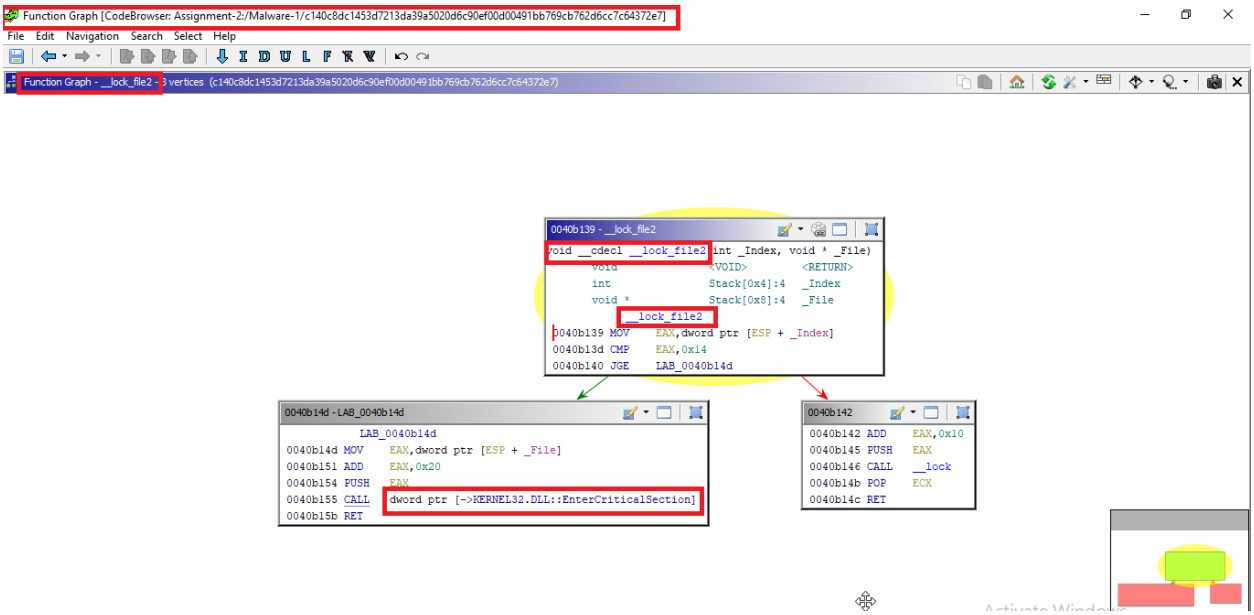


Figure 70: Malware-4: Malicious DLL fuctions used by malware

Task-3.3 FUN_0040bae8

In this function malware delets to the critical section to after performing its malicious action.

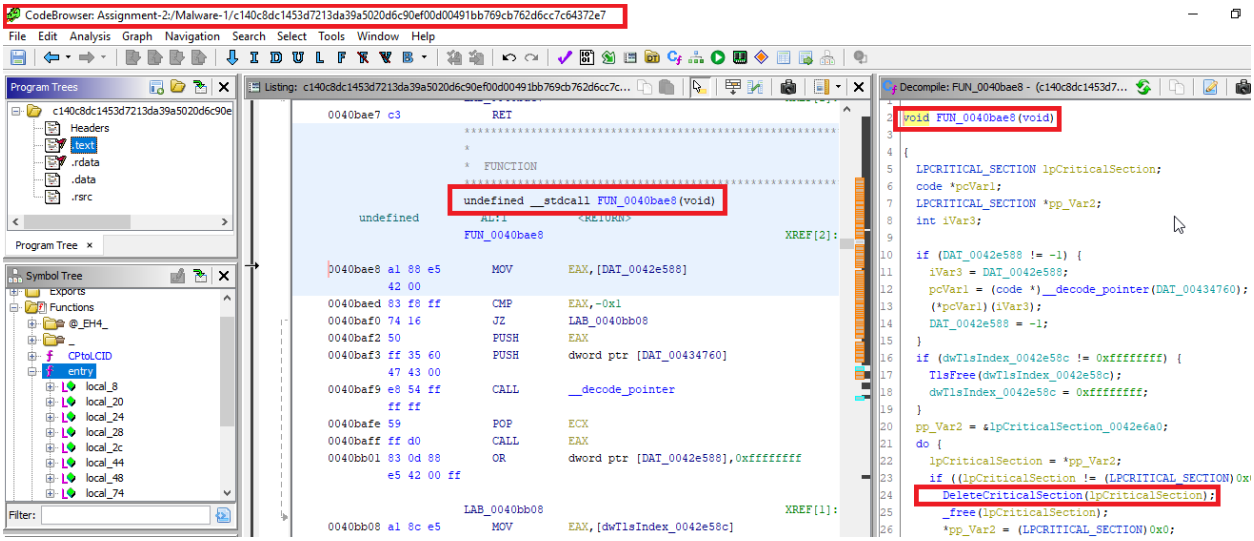


Figure 71: Malware-4: Malware deletes the critical section after performing its malicious actions

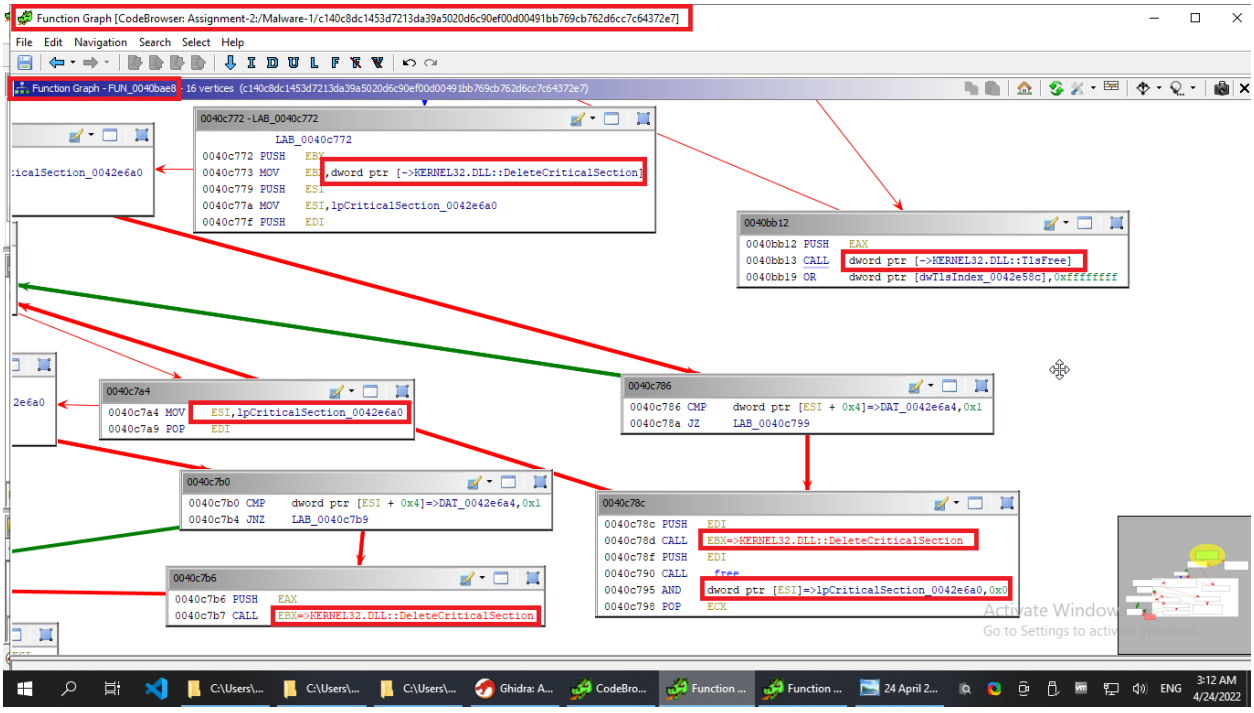


Figure 72: Malware-4: Malicious DLL fuctions used by malware

Task-4 What DLL's any malware includes? Are there any suspicious functionality called by these DLL's?

The DLL's used by this malware includes includes "ADVAPI32.dll", "COMCTL32.dll", "GDI32.dll", "KERNEL32.DLL", "OLE32.DLL", "SHELL32.dll", "SHLWAPI.dll","USER32.dll" and "VERSION.dll

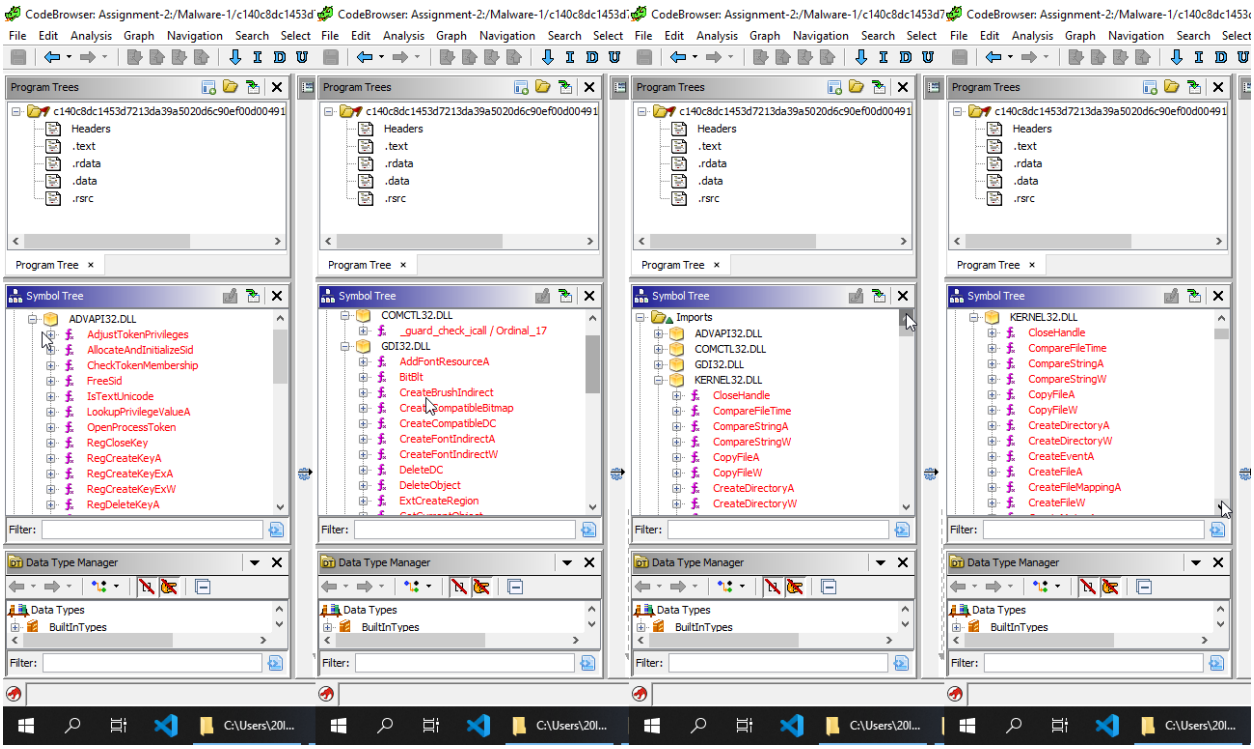


Figure 73: Malware-4: List of DLLs used by the malware with their functions

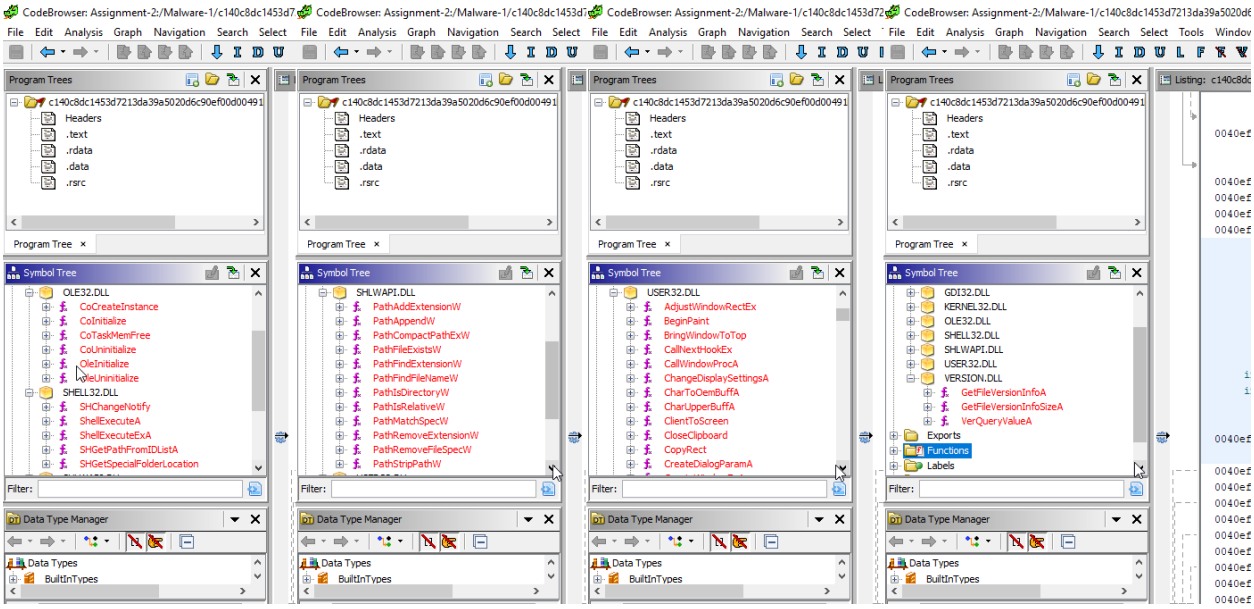


Figure 74: Malware-4: List of DLLs used by the malware with their functions

The suspicious functionality called by the DLLs includes the “KERNEL32.dll” calling its function “InitializeCriticalSection” when the malicious function of malware “FUN_crtInitCritSecNoSpinCount ” initialize the critical seciton.

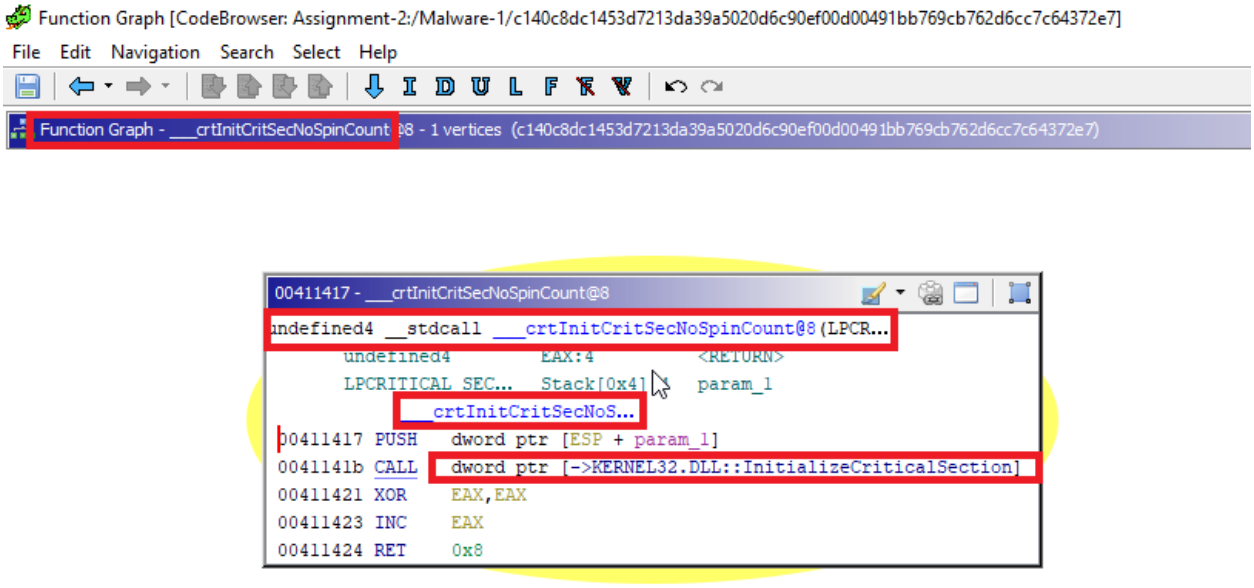


Figure 75: Malware-4 Malicious DLL functions used by malware

The suspicious functionality called by the DLLs includes the “KERNEL32.dll” calling its function “EnterCriticalSection” when the malicious function of malware “FUN_lock_file2 ” enters the critical seciton.

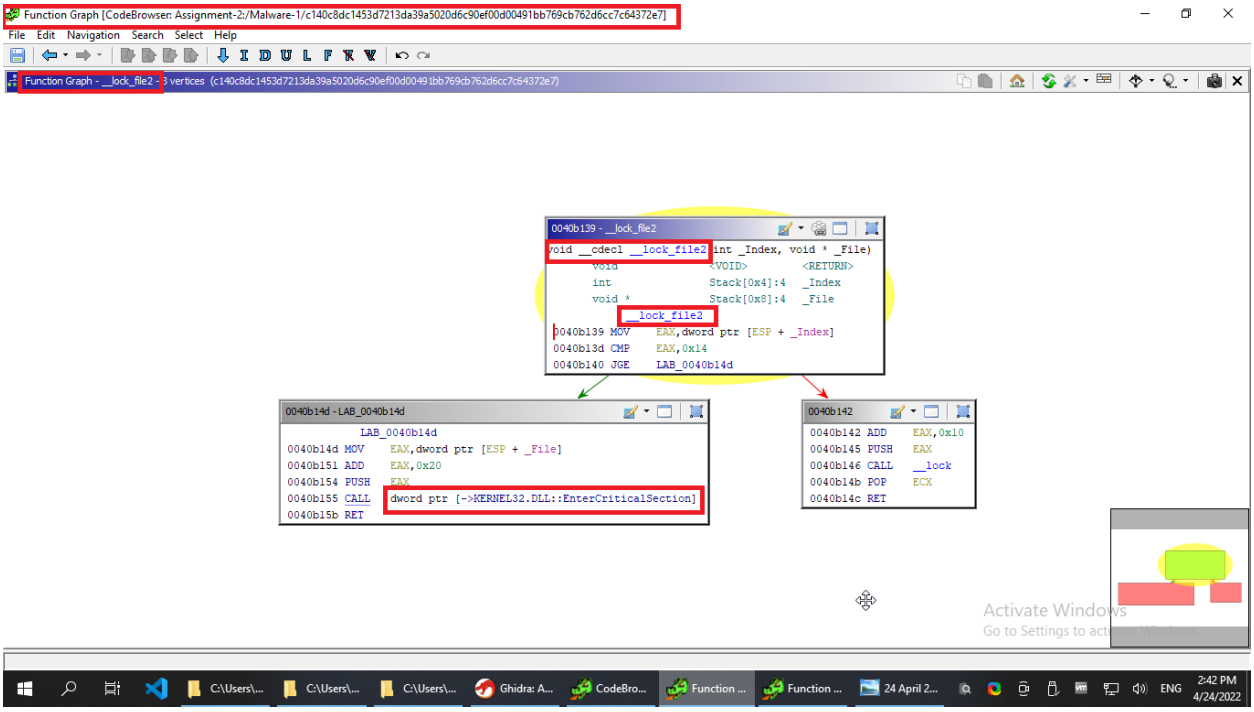


Figure 76: Malware-4 Malicious DLL functions used by malware

The suspicious functionality called by the DLLs includes the “KERNEL32.dll” calling its function “DeleteCriticalSection” and “TlsFree” when the malicious function of malware “FUN_0040bae8 ” deletes the critical section after performing the malicious actions..

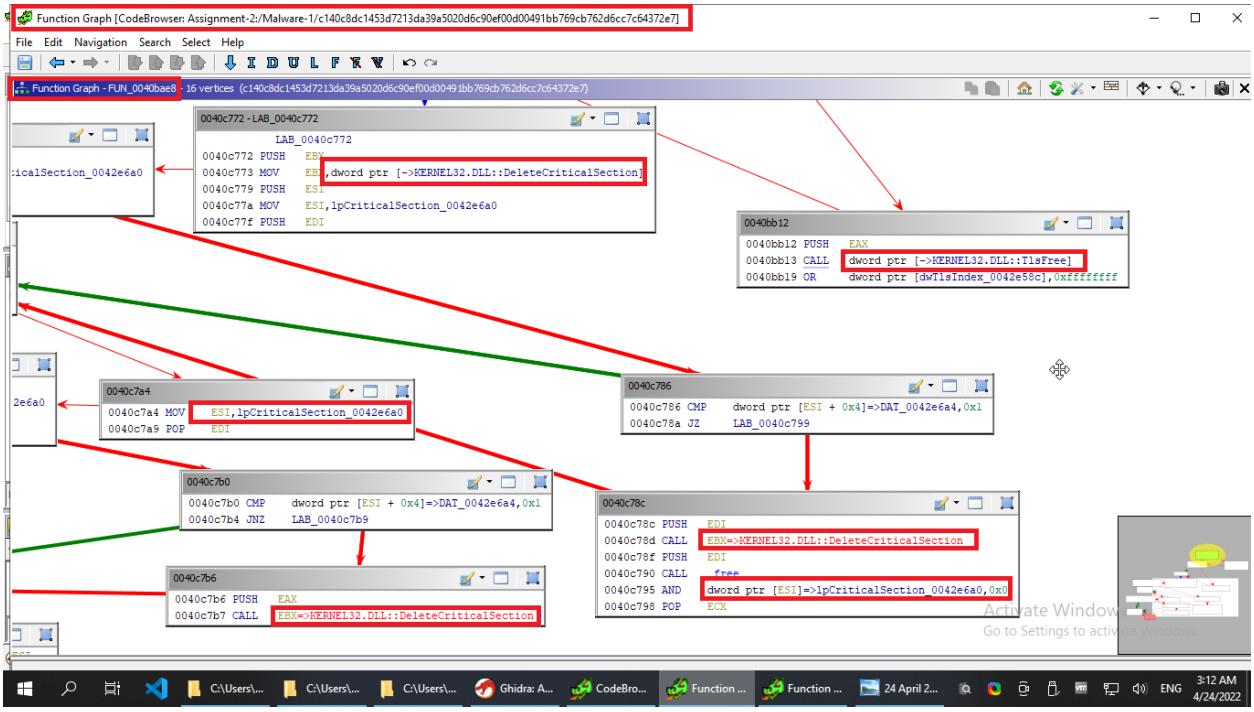


Figure 77: Malware-4 Malicious DLL functions used by malware