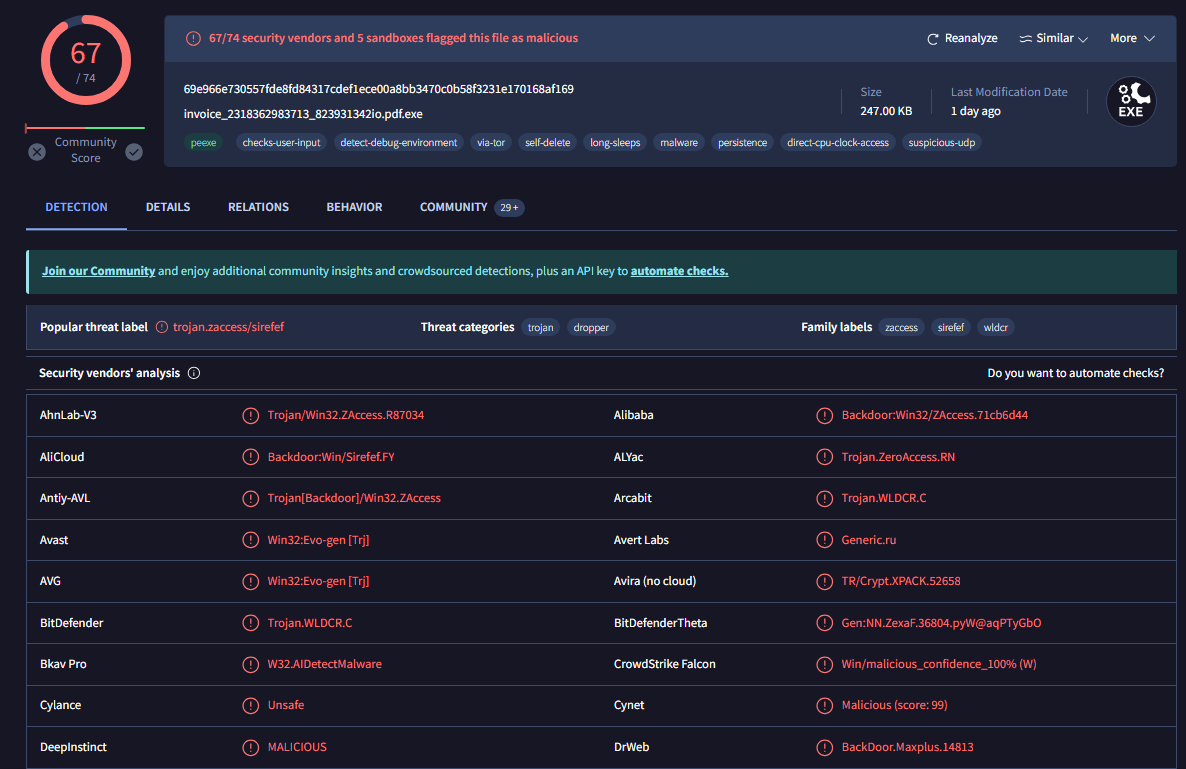
VIRUS TOTAL REPORT OF Zues Trojan:



Hashes:[obtained in pestudio]

MD5

ea039a854d20d7734c5add48f1a51c34

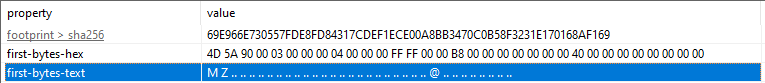
SHA-1

9615dca4c0e46b8a39de5428af7db060399230b2

SHA-256

69e966e730557fde8fd84317cdef1ece00a8bb3470c0b58f3231e170168af169

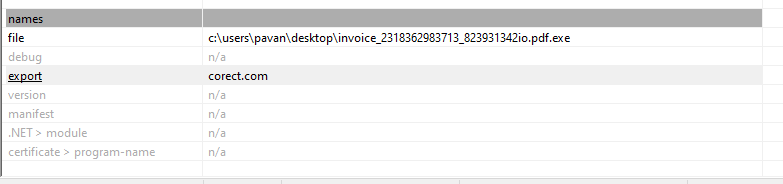
MZ means executable file:

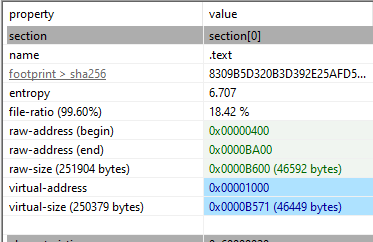


Zues Trojan File Name:

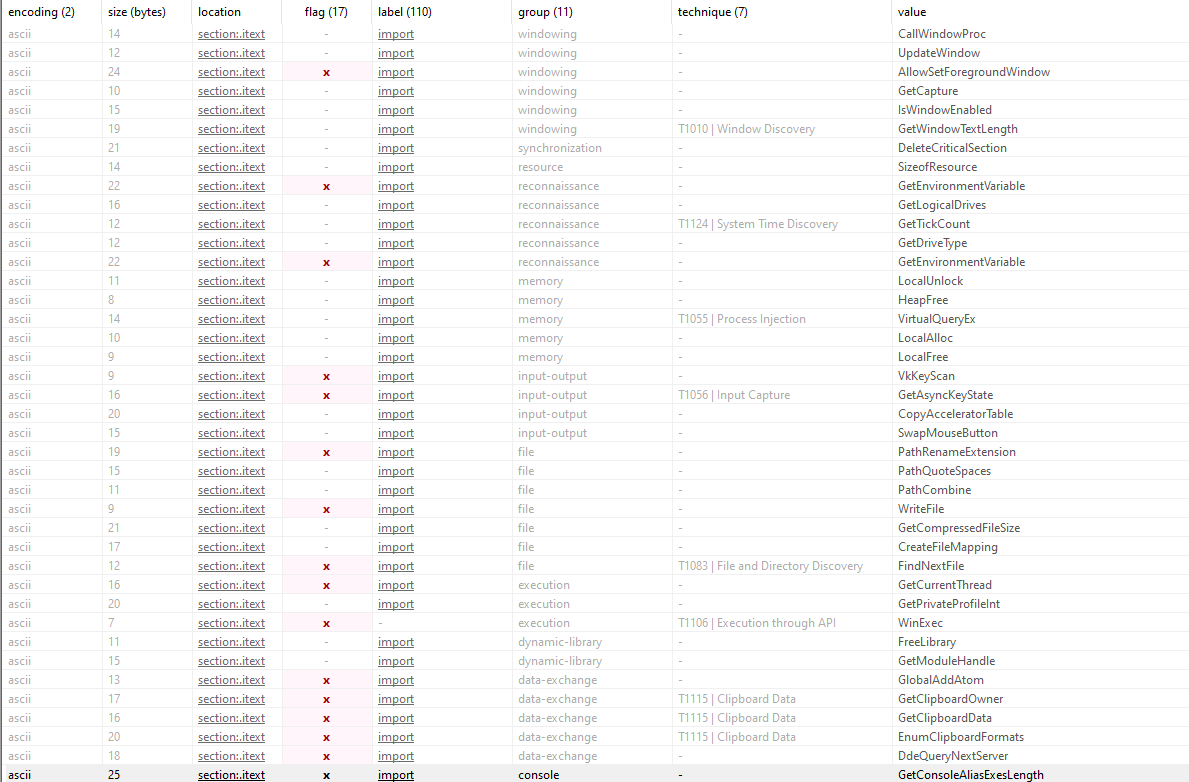
invoice\_2318362983713\_823931342io.pdf.exe

advanced static Analysis:





Pe studio initial report:



Api calls.

Libraries:

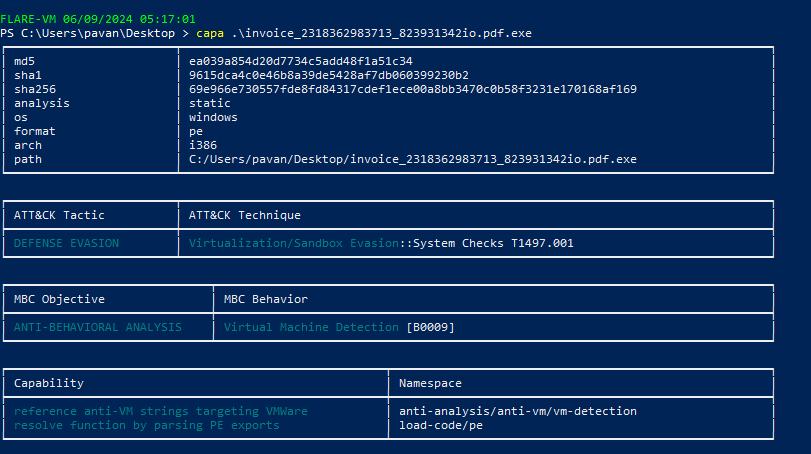
SHLWAPI.dll,-,-,0x00020208,0x00020078,implicit,21,-,Shell Light-weight Utility Library

KERNEL32.dll,-,-,0x00020190,0x00020000,implicit,29,-,Windows NT BASE API Client

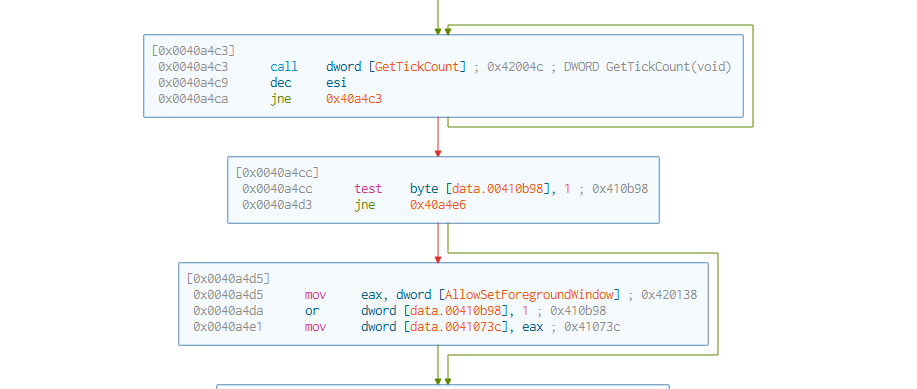
USER32.dll,-,-,0x00020260,0x000200D0,implicit,27,-,Multi-User Windows USER API Client Library

Floss is used to get the String only output.

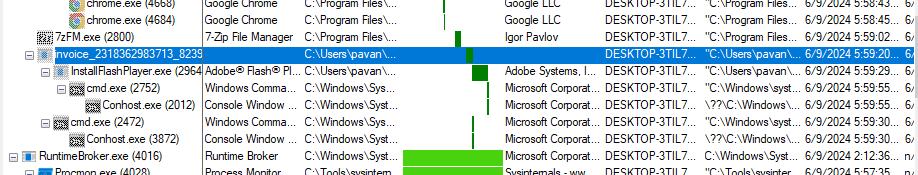
Capa-



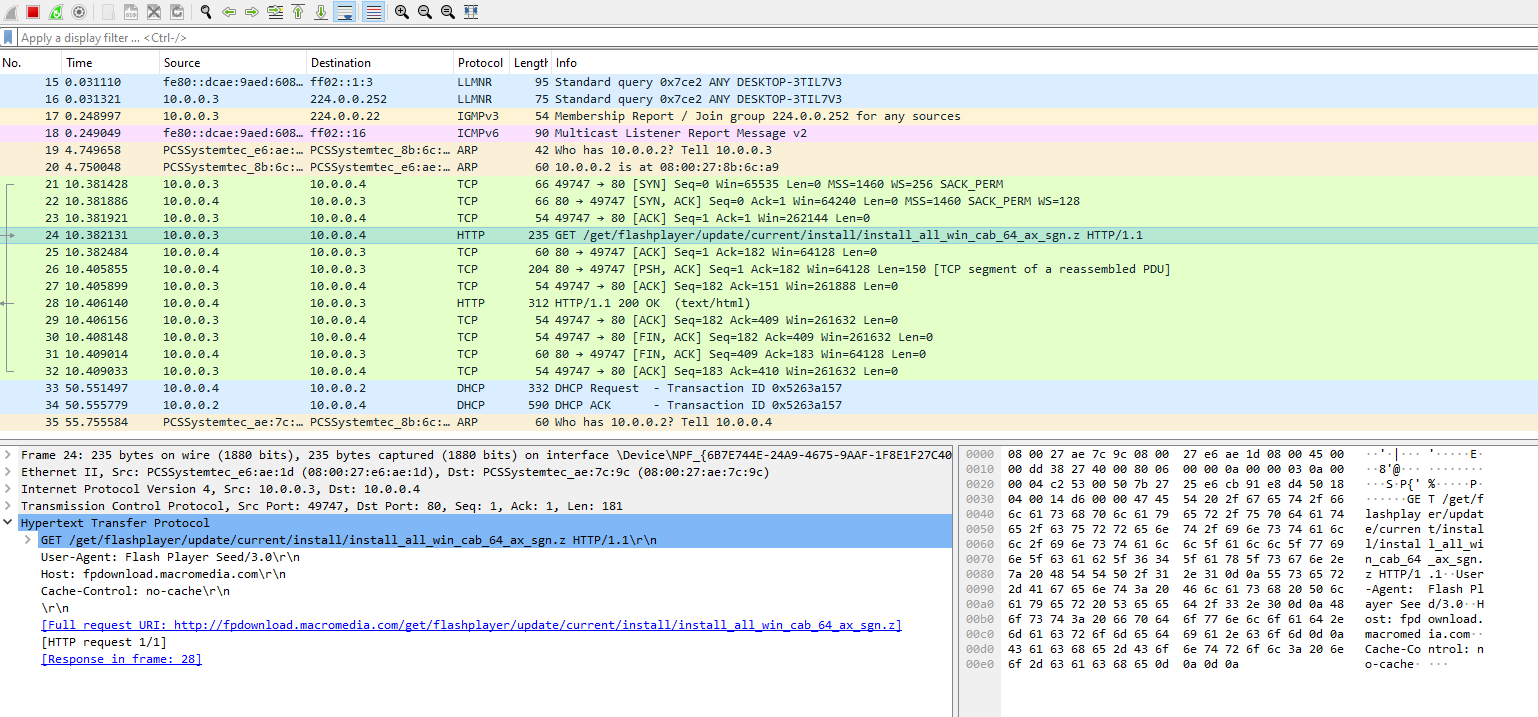
Cutter is a free and open reverse engineering platform:

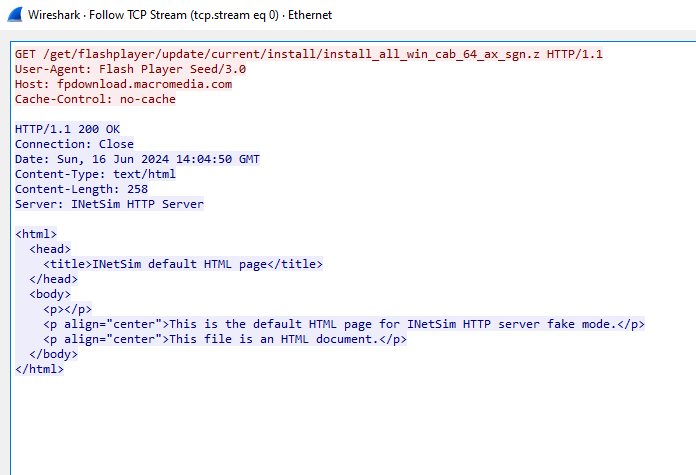


Dynamic Analysis:



Wireshark report after detonating the malware:

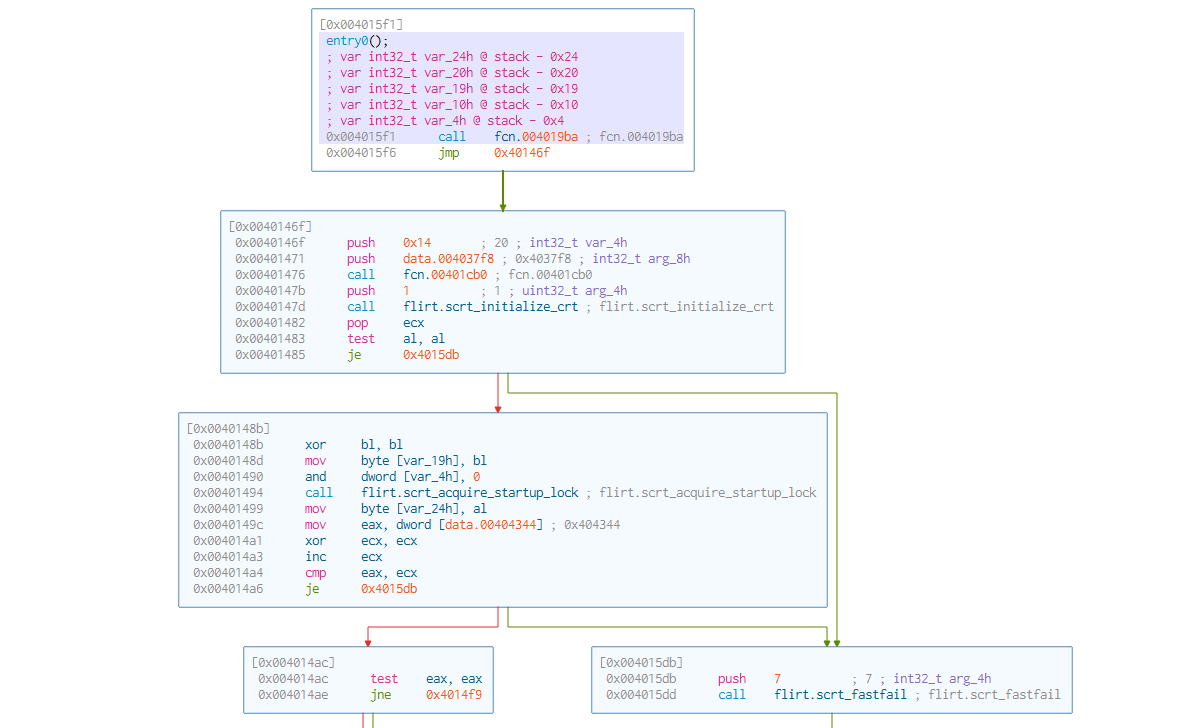
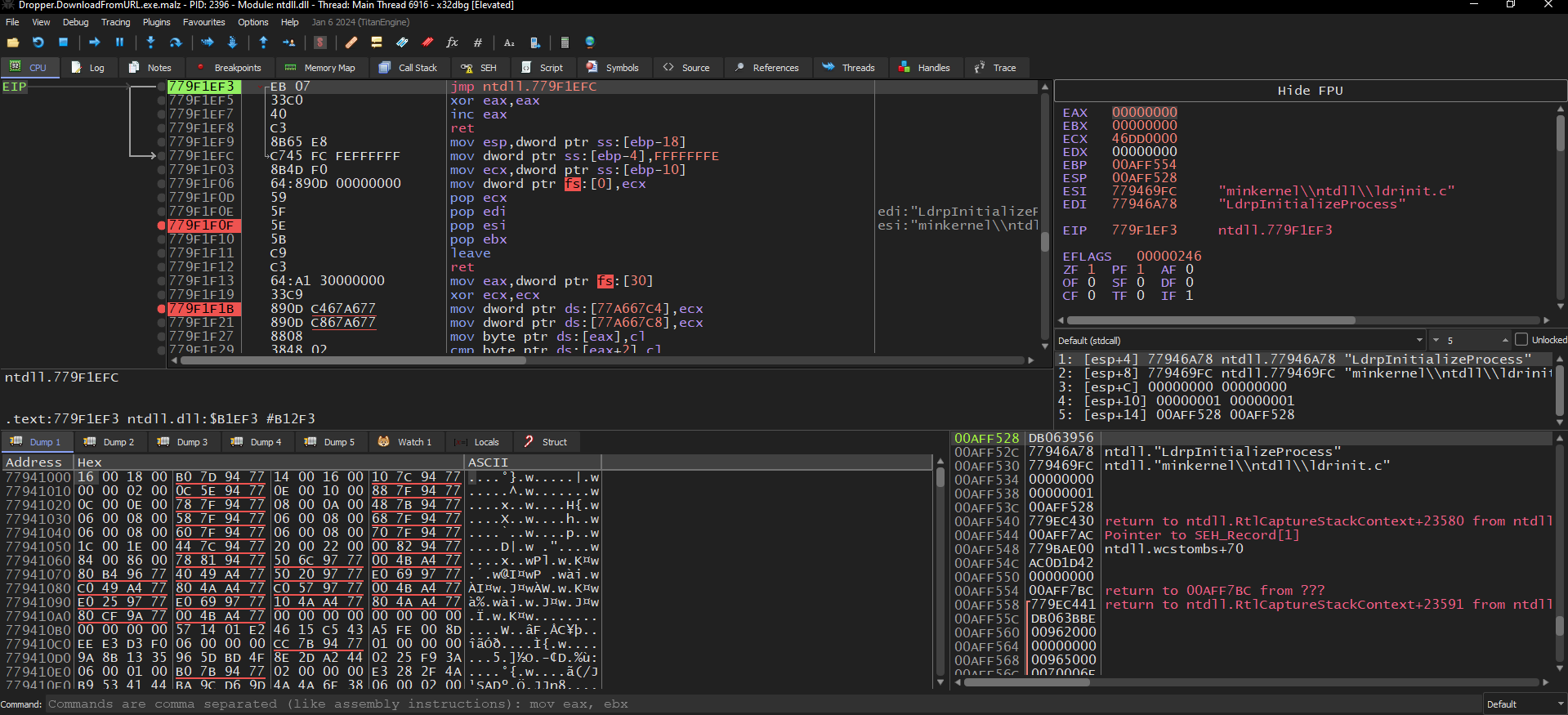


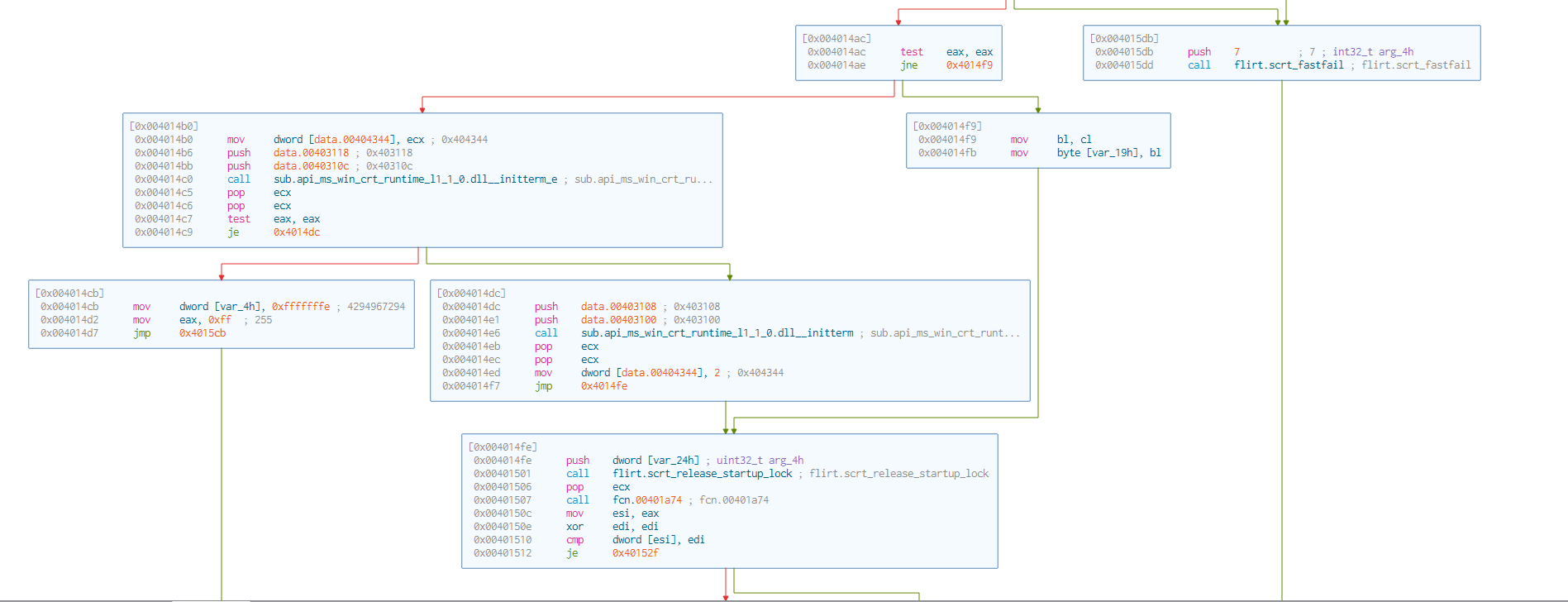


Advanced dynamic Analysis:

Detonating malware inside a program.[debugger]

Debugger acts as a mediator between the user and the program.





Inetsim:

