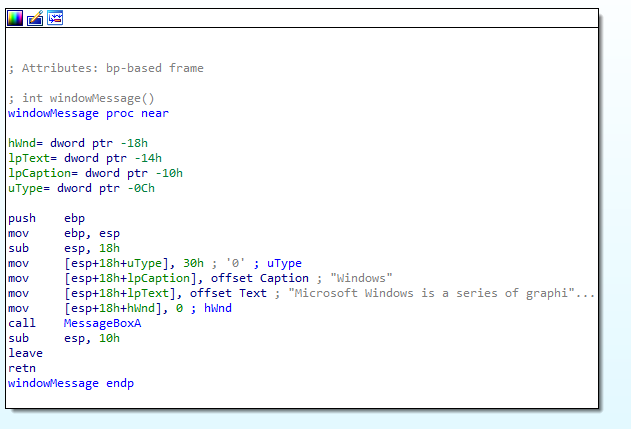
We get an x86 PE file

Run it, it pop out a window with some message NO FLAGGGGGGG

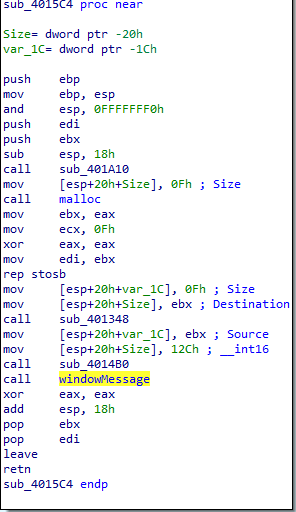
Throw it into IDA

—---------------------------------------------------------------------

- I find the rubbish message in the popped out window above



It was called there

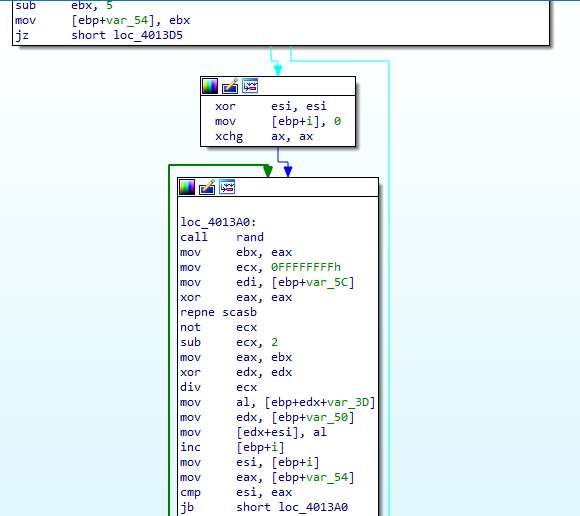


Above this function, i found 2 interesting function - sub\_401348 and sub\_4014B0

in the first one, at first it generates a random string with length is 5

then add to the end ‘.dll’

then store it to a variable in memory called Destination

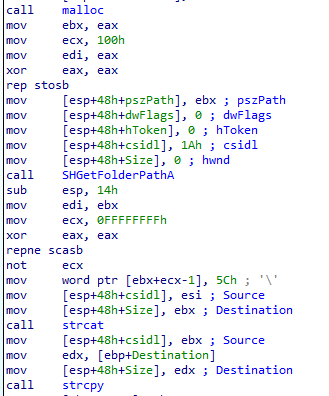


-In the second function: First it call bunch of API to create a file, which called by the name that create before

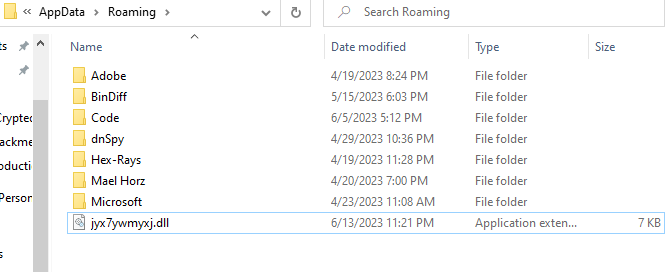


and now the questions are where is the file and what it contain

* where is the file: you can find it in sub\_40141C



Debug it, i found that it will create file at C:\Users\<user>\AppData\Roaming\

* What it contain ??
* 

you have 2 choice: debug it and you will find DisplayMessage function, Run dll 🙂

i run it, then it get

(Open cmd at the folder, then run RUNDLL32.EXE dllname, entrypoint) (in my case dllname: jyx7ywmyxj.dll, entrypoint: DisplayMessage)

