# WRITEUP – Into to Reversing Final Assignment

Submitted by:

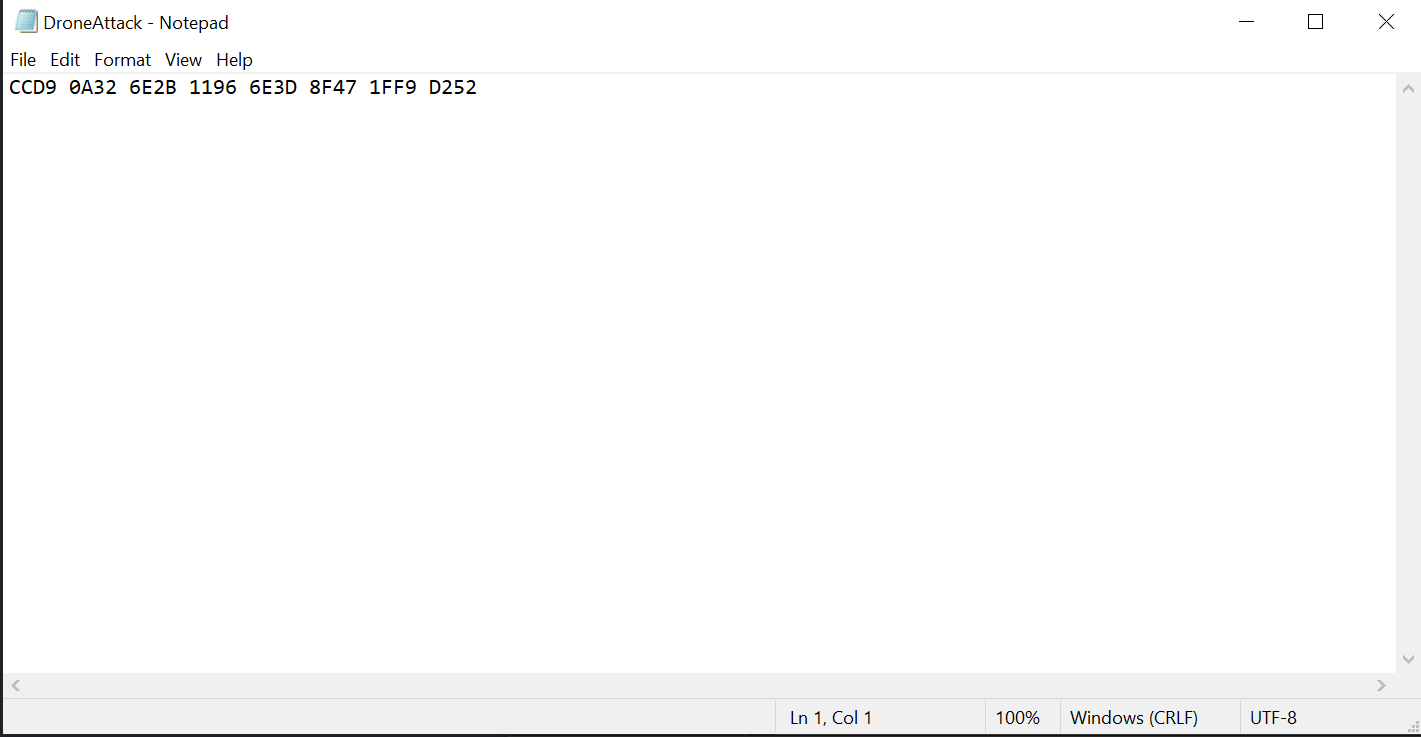
* Daniel Attali 328780879

## Stage 1:

The first part was just to run the .exe we were given and we saw printed an image and we were presented with a scenario, the second thing we did was to open the file using IDA and try to find anti debug behaviors in the tls\_callback since we didn’t find anything (yet) we went and found the \_\_main function and try to find and rename basic functions, like the function who takes a string and print it to the screen using a typewriter effect.

After Identify those basic functions we started working on the functions we found in the main, the first function seems to be taking a string has input and for each byte XORing it with 0x2A and then again XORing it with 0x2A again meaning this function didn’t modify the string in any way, so we looked into the next call in the main function and found another function and with in it a call to what we called stage\_1\_main, in the stage\_1\_main we found the following, first the function create a string “C:\ReversingCTF” and another string “DroneAttack.txt” and from our understanding of this function it tried to open the file and if not found printed an error message, so we created the file and when we ran the program again we saw the program had done 2 things:

1. Written into the .txt file
2. Added a AttackIRGC.dll file into the directory



After this it is had printed to the screen the success message and we are done with stage 1.

Stage 1: You are a special operations expert.

Your mission is to protect our pilots. Disable the anti aircraft system

Oh, intelligence report says the enemy spread decoys, find the real target, fast!

Anti aircraft system located

Intiating disable sequence

Great job. Anti aircraft system is disabled

Stage 2: You are a jet fighter pilot. The sky is clear. Your mission: release bombs on IRGC headquarters.

To find them, use the cyber intelligence unit

## Stage 2: