# ASSINGMENT

## Introductions

Malware is common in our daily life, in this assignment my work is to analyze a sample malware that encrypt the file by using ida pro.

## Executive Summary

In this assignment I will show I analysis this program by using IDA pro. IDA pro is the most popular binary static analysis tool for disassembling, decompiling. IDA pro help us to find the strange function code, searching string and exported or imported functions.

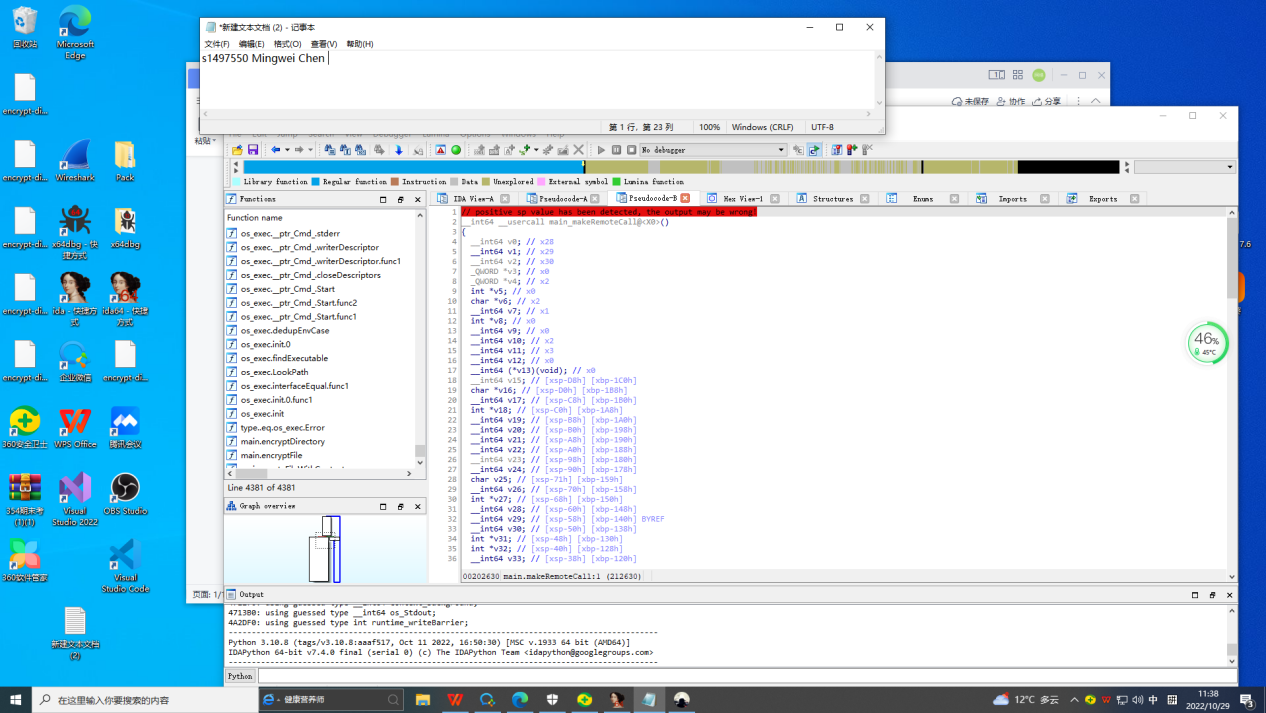
The malware is written in go, which is a new programming language. Comparing to traditional programming language such as c, cpp, java. This kind of malware is more hard to analyse because go provides more complex structure and data types. For example, stings in go has two fields. One is the length of the string and another one is the pointer of the read string, which is quite different from C string.

The malware connect to the attacker using socket programming, and encrypted all the files in the current working directory. After doing encryption, the malware open up the browser and jump the attacker’s website.

## Methods and Techniques

### Load the malware

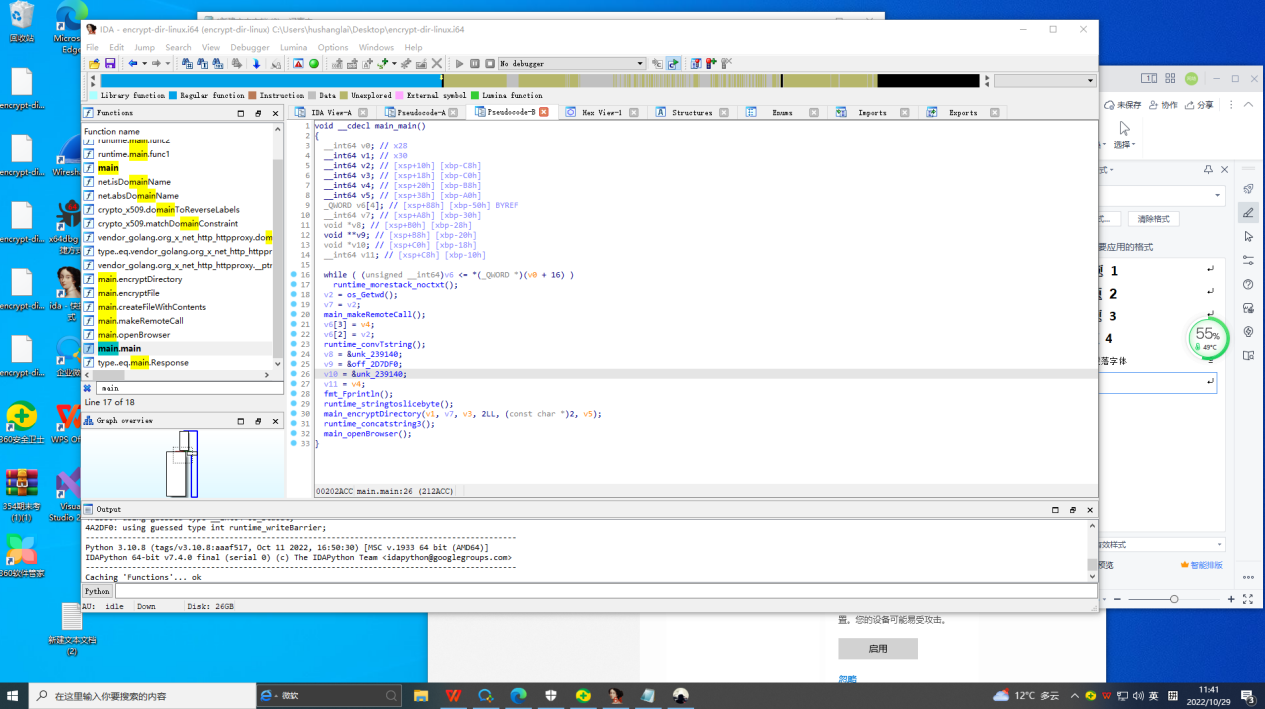
Just drag the malware into the ida pro, note the malware is 64bit, so I should use ida 64 pro



### Find the entry

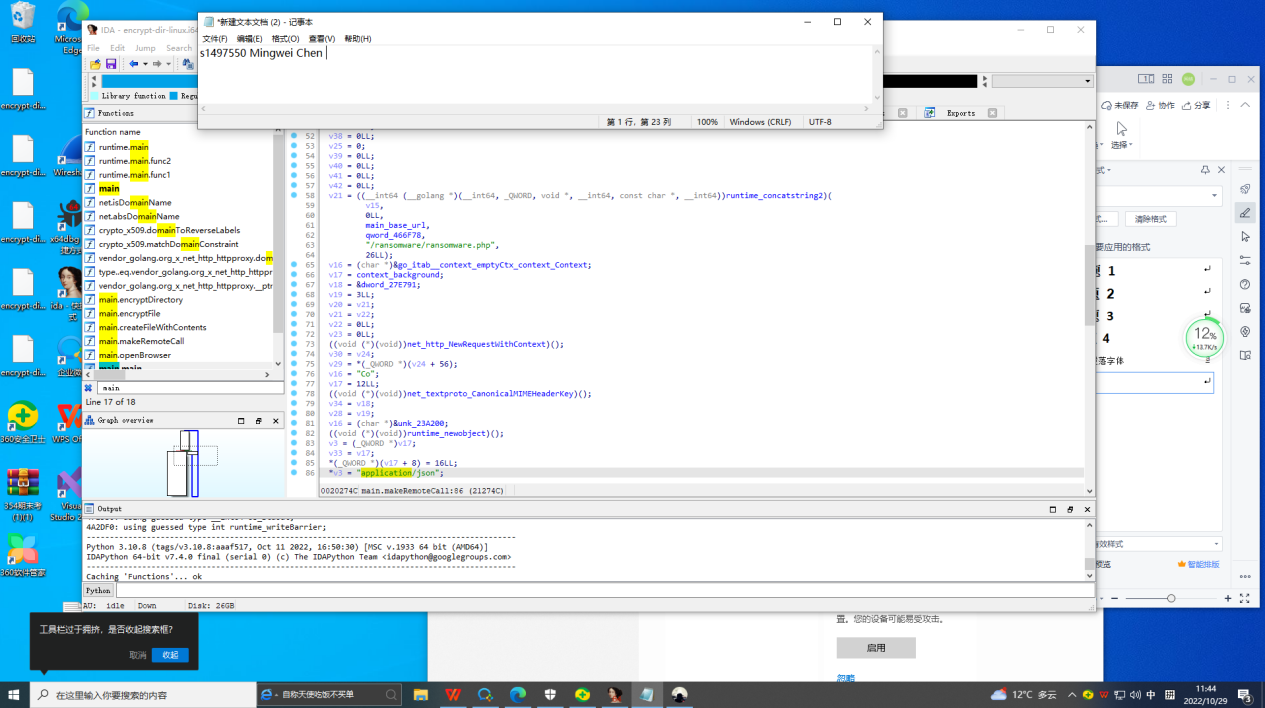
Every program has its entry point, some program is main function, such as C and CPP program.

But this is an Golang binary which is different, google say its main.main

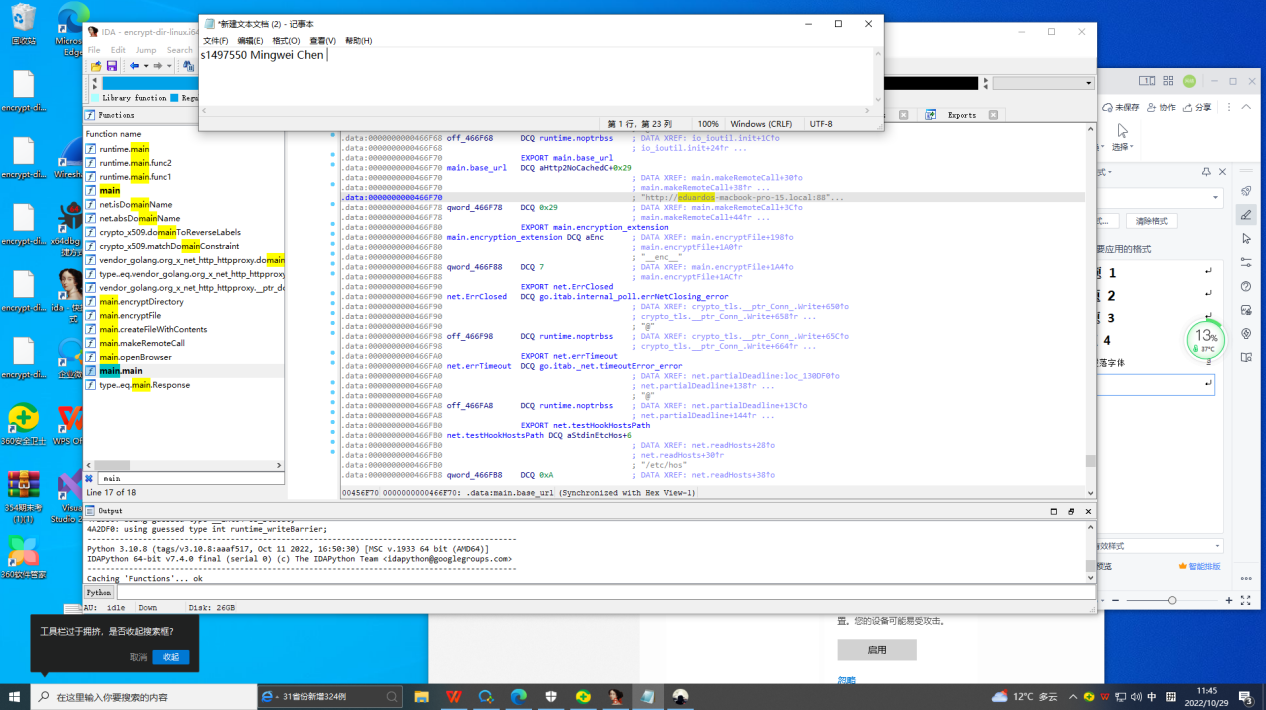


### Remote Connection

Malware usual have the remote connection, we need to find the attacker.



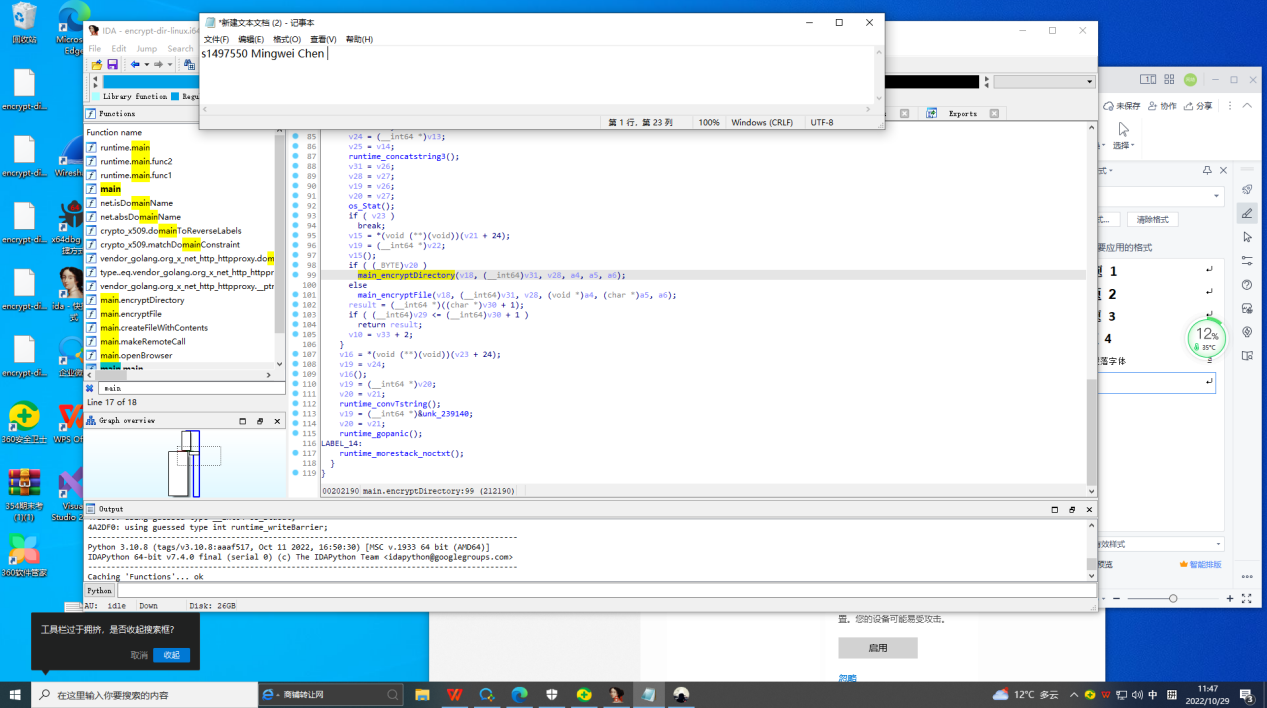
From the code, we see the program tries to make HTTP request.



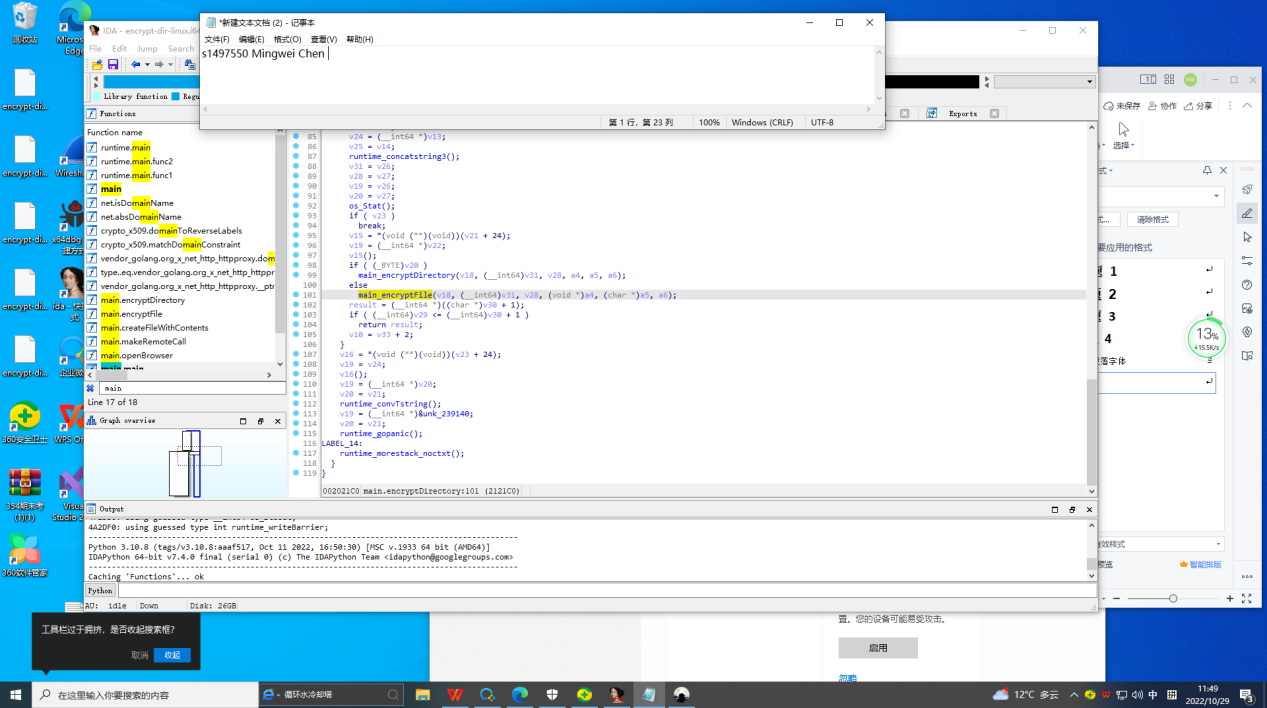
The attacker’s url is easily find. Attacker is hacked.

### Doing Encryprt

This is an encryption function, that encrypt directory



This function iter all the file and encrypt recursively, which means encrypt all the file!



## Conclusion

The malware do these things:

1. Make HTTP request and save public key and unmashal the key
2. The malware use encrypt\_dir function to encrypt all the file
3. The malware ask for money