REPORT ASSIGNMENT

**Subject: Malware operation**

**Assignment: Project Lab**

**Topic: Ransomware**

*Instructor: Nghi Hoàng Khoa*

*Report Date: 7/6/2021*

***Team***

1. **General Information:**

Class: NT230.L21.ANTN

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Name** | **Student ID** | **Email** |
| 1 | Nguyễn Xuân Hà | 18520042 | 18520042@gm.uit.edu.vn |
| 2 | Huỳnh Hoàng Hải | 18520697 | 18520697@gm.uit.edu.vn |

1. **Working stage:**

|  |  |  |
| --- | --- | --- |
| **STT** | **Work** | **Self-assessment** |
| 1 | Check Internet | Done |
| 2 | Setup Discord as C&C server | Done |
| 3 | Destroy file by random byte | Done |

***Below is our team’s report detail.***

Ransomware

# **Technique and Behaviour**

In this demo, we will use C# as program language, Visual studio 2019 to build.

## Main technique:

* Pretend to be a Discord’s bot to trick Antivirus.
* Take command from Discord and execute on Victim machine.
* Using 256bit – keysize AES encrypt
* Using random byte to overwrite files and destroy completely.

## Behaviour:

**Step 1**: By some reason, victim trigger our ransomware. Our malicious program will connect to a Discord server as a bot.

**Step 2**:

* If internet on: Attacker can interact with ransomware through out Discord server. We can make ransomware to encrypt/decrypt/destroy file on victim with key from attacker (in our scope of demo, of course, you can custom your ransomware as your wish).
* If internet down: Ransomware will destroy files on victim machine by using random bytes.

*In our demo, ransomware will only affect to files stay on Download folder and Desktop. Windows defender realtime monitor and Firewall alway turn on.*

# Setup Discord as C&C server

The main reason that I chose C# for my demo because it is supported with powerful library. If you want to setup step by step, I refer to read this document:

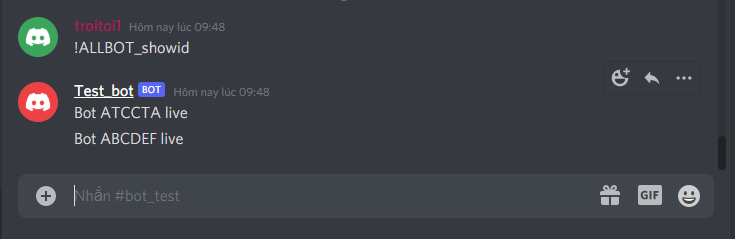
<https://docs.stillu.cc/guides/introduction/intro.html>

We will create a Bot and add him to our Discord server. We have a bot Token too, our ransomware will use this token to connect to Discord server.



Our bot token, ransomware will use this

To handler multi ransomware, each of them will generate an individual ID. In our demo, we fix a specific ID for them.

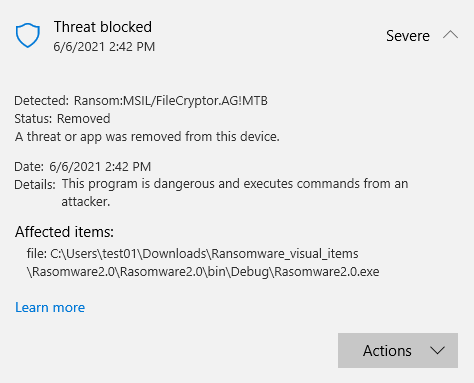


A demo multi ransomware

To compare, I test ransomware of this man with Windows defender:

<https://www.youtube.com/watch?v=UfHgALGjtJs&list=PLCBJ_FgcvQFkT4Wja8sEnNZ30fLi8hZql&index=12>

His ransomware mainly enrypt/decrypt file with local key and not connect outside, but he immediately catch by Window derfender.



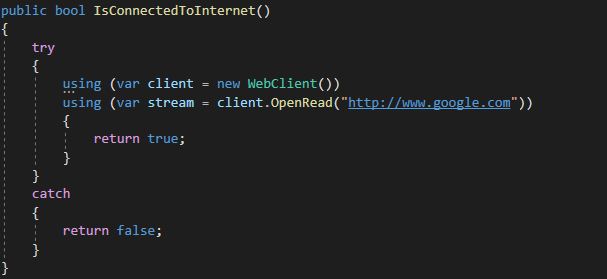
We guess that our AV has mistake our ransomware with true Discord bot.

# **Ransomware function**

## Main function

You can custom your function as your wish. In this demo, we only demo a basic destructive ransomware with main function:

**Check internet connection:**



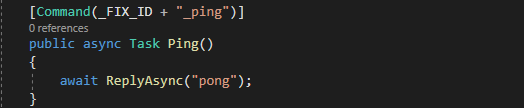
We open a web client stream to google.com. There are some other way that you can ask teacher google.

**Receive and Execute command from Attacker through out Discord server:**

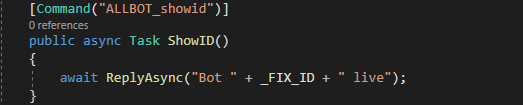
Most of our command will have format: *!****<ransomwareID>\_<command>***

We introduce some basic command:

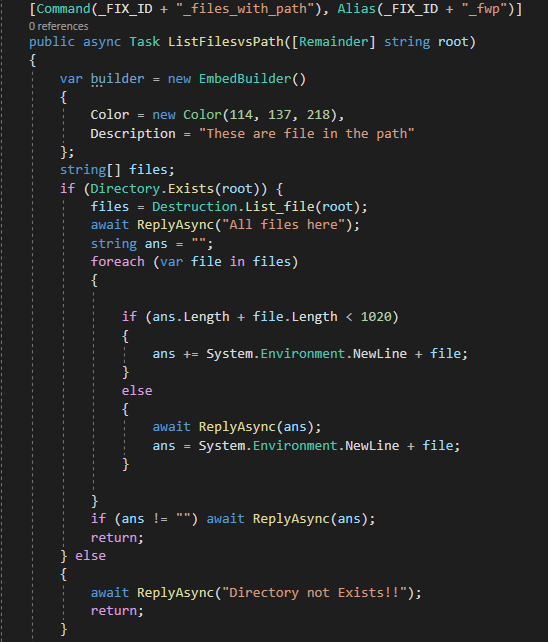
* ***“\_ping”:*** check status of ransomware.



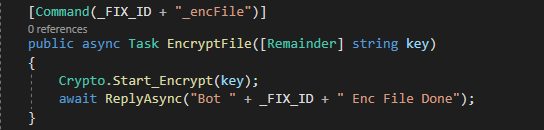
* ***“ALLBOT\_showid”:*** sent ID to server.



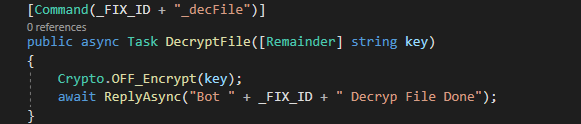
* ***“\_files\_with\_path”:*** list all files in a directory (demo purpose)



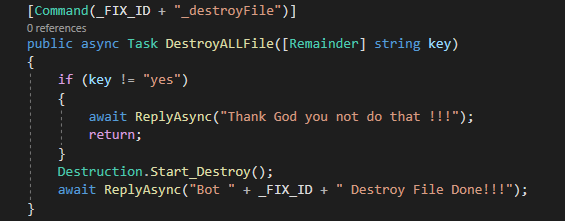
* ***"\_encFile":*** Encrypt files with key from attacker.



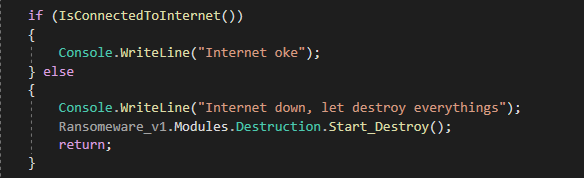
* ***"\_decFile":*** Decrypt files with key from attacker.



* ***"\_destroyFile":*** Destroy files.



**If internet down, then destroy files:**

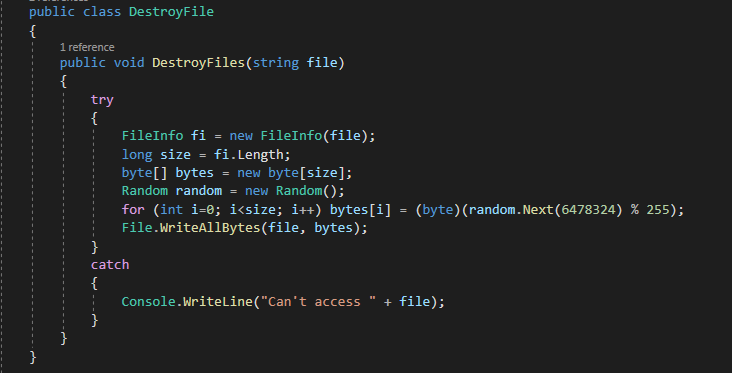
****

## Support function

There are logic functions to handler main command.

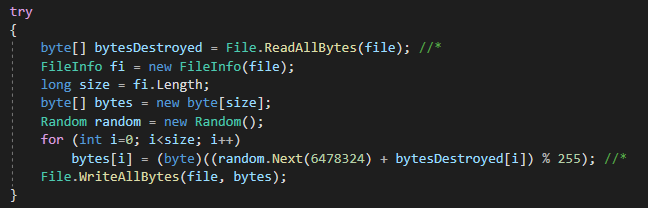
**Destruction class**

At first, I use the simplest way

****

* Take responsible to overwrite file with random byte. We don’t need use Time as seed for Random function because in C#, in default, Random function use machine time as seed.
* Of course, this is not the most efficiency way because administrator can trace log a guess the start time of ransomware and recover files, although it extremely hard to do that.
* One trick that, ransomware should destroy itself to erase any vestige.

To improve algorithm with target that no one can recover old files. I use an extra variable.



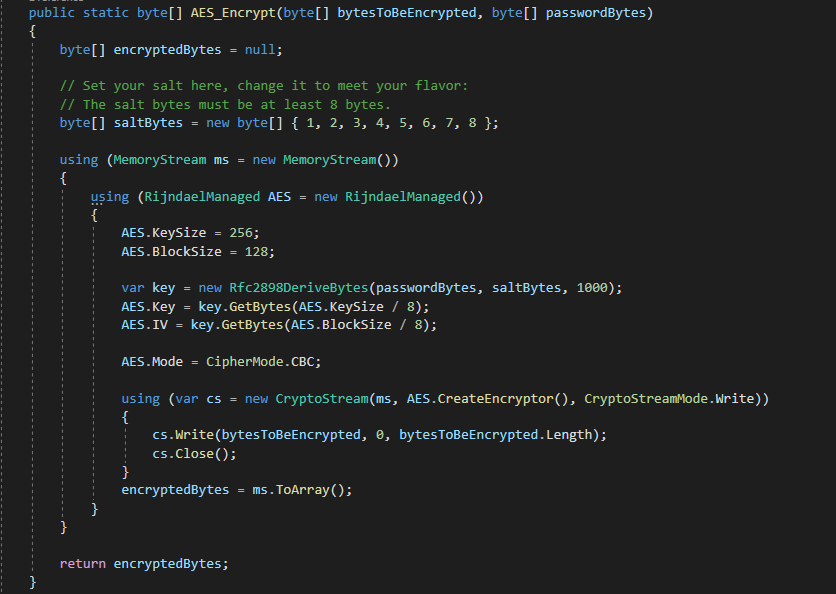
* It mainly bases on mathematics with modulo division. Take a simple expression as example:

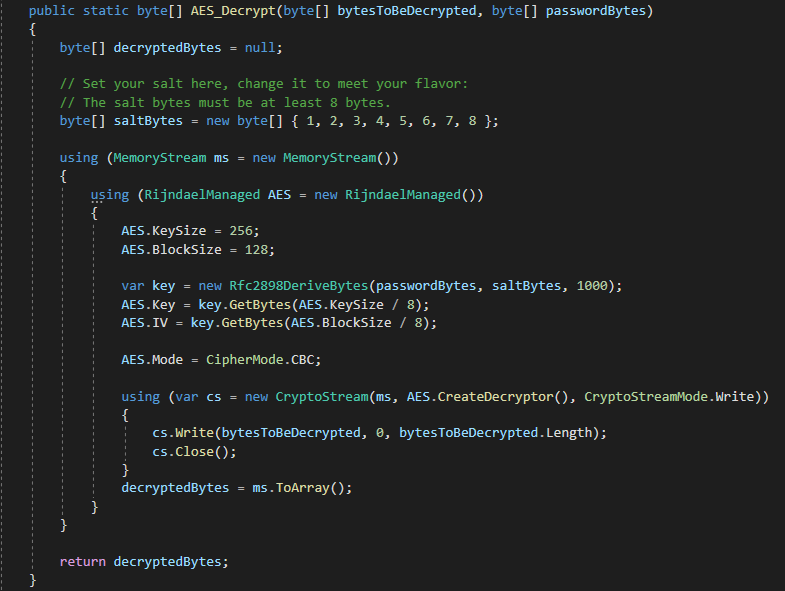
(20 + x) mod 4 = 1

* It clearly that x will have more than 1 value (5, 9, …). And in our case, you will never know exactly what value of *“bytesDestroyed[i]”* because you are finding it too!!!
* Pray God save you now (￣y▽￣)╭ Ohohoho…..

**Cryptographic class**

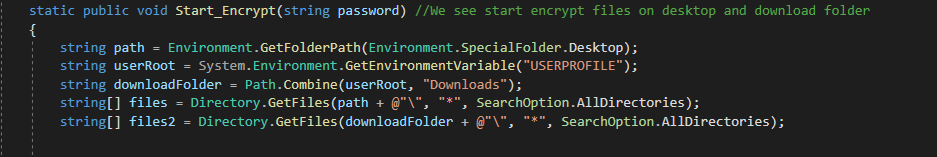
This class is a simple implementation of AES algorithm. No need to dig deep into it.





Ransomware will get password form attacker, then concat with extra string to enhance security and finally hash with SHA256 function.

In this demo, we just forcus on files which stay on Desktop and Download folder.

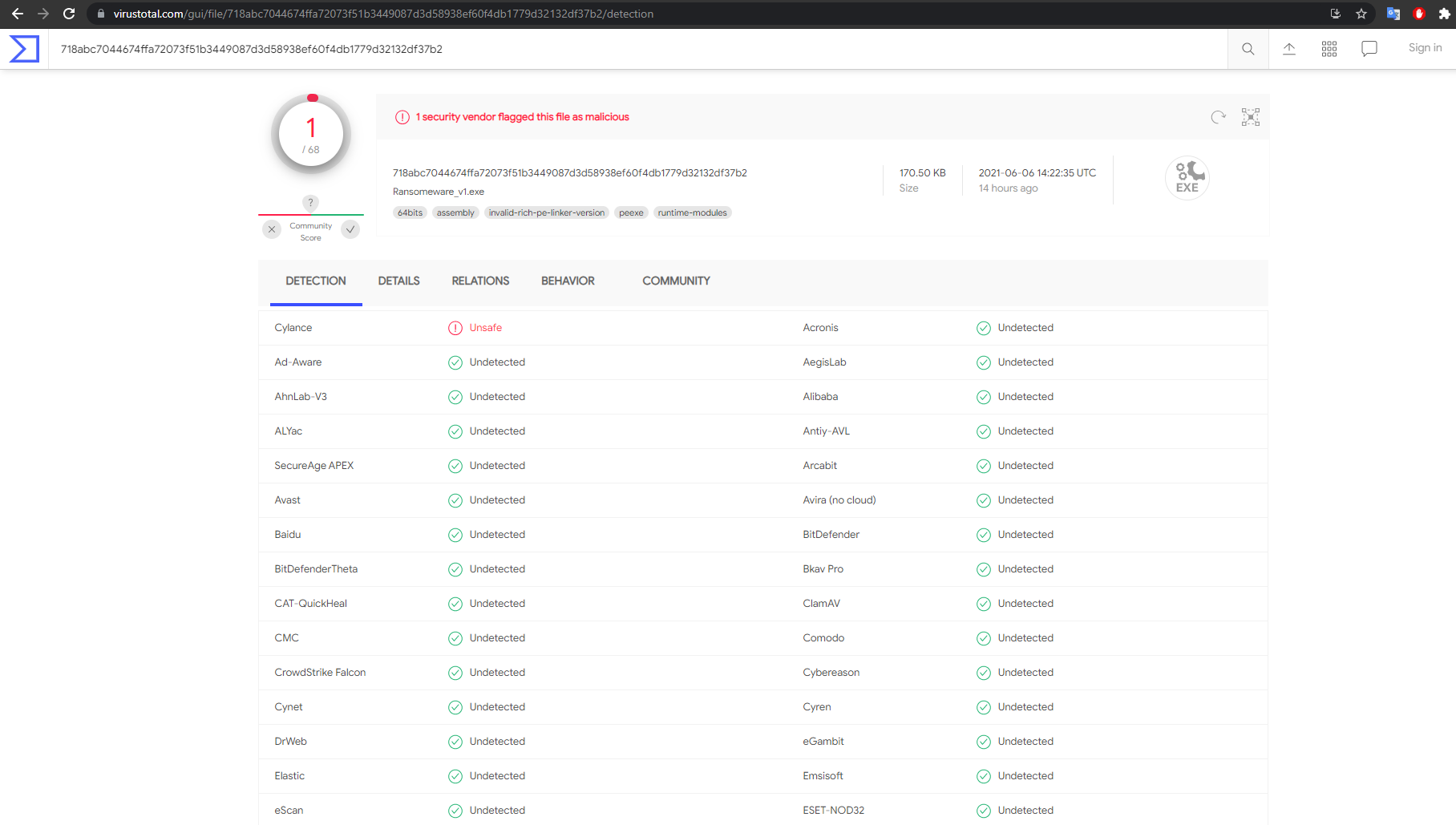


# **Demo**

Video demo at:

<https://youtu.be/t5Ra9WgXpwM>

Test with virus total:



***This is only demo technique report so that this code is not practical for use in real context. This report is only for education purpose.***

**Attach file**

[1] Source code: <https://github.com/troisang1/ransomware_C->

[2] Video demo: <https://youtu.be/t5Ra9WgXpwM>

[3] Source code: Source.zip

**END**