Cyber Security Project 1: Keylogger

So I have made a key logger malware that have the following features:

1. It can log all the letters and special characters along with the other keys.
2. To turn it of and clean the changes made by the keylogger we can just write “quit”
3. It can add it self to the startup registry of the user so that it run on it’s own when the laptop is reopened after shutting it down and when it sees “quit” in the log it removes itself from the registry.
4. At mid-night it sends an email along with the keylog file using the smtplib of the python.
5. It can cleanup the changes it made like deleting the keylog file and removing itsef from the windows registry

Why I did these things

1. I have used the path “C:\Users\Public\Keylogs.txt” to store the file of keylogs cause this directory is present for everyone and can be accessed by anyone
2. I have added the malware to registry so that it will run again when the laptop is shutdown and reopened

References:

1. David Bombal keylogger file for the basic handling of the keys and I have modified them to a certain extent

Initial codes

<https://github.com/davidbombal/CompTIA-Security-Plus/blob/main/python-keylogger>

better version

<https://github.com/davidbombal/python-keylogger/blob/main/keylogger.py>

1. For writing the email script: <https://youtu.be/QJobMzcmoMo?si=3zRTsyvmSqeA6C-z>
2. Took help of ChatGPT, Perplexity, Claude.ai

Window registry path to check if the file path was added and removed properly

* Click win+r > search regedit > click yes
* The file we are looking for is in a path like this:

“Computer\HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run“

To stop the keylogger manually if we have removed the quit code part

* To turn of the malware you can open task manager and search for mal.exe and end task

**keyloggerdevlopedversion**

DISCLAIMER  
I am not going TO USE THIS CODE TO DO malicious activity, NOR AM I GOING TO encourage anyone to DO SO. WARNING  
YOU SHOULD NOT DOWNLOAD ANYTHING FROM AN UNTRUSTED WEBSITE AND EXECUTE IT

SOFTWARE TO DOWNLOAD

i. VM Ware:<https://www.vmware.com/info/workstation-player/evaluation>

ii.Windows 11 iso :<https://www.microsoft.com/software-download/windows11>

python package

i. pip install pynput

ii. pip install pyinstaller

iii. pyinstaller --onefile yourscript.py -w so that it won't have a terminal open when being executed

iv. $env:PATH += ";C:\Users\user\AppData\Roaming\Python\Python312\Scripts"

Features

* prints the timestamps after one hour and logs the text along with special characters and keys that are used. DONE
* sends the file via email at midnight every day or posts the file to a web server. the video I took reference for writing the email script: <https://youtu.be/QJobMzcmoMo?si=3zRTsyvmSqeA6C-z>
* After converting it into an executable file the Windows Defender doesn't see it as malware. # NOT CONFIRMED WILL TRY TO SEE IF IT DOES WORK THAT WAY
* run on its own when downloaded and when the laptop opens after being shut down.