Phishing+keylogger

Date :2023

Technology used: Python ,Tkinter , PHP

My Goal in this project was to be able to grab the windows password of the victim.

For doing I began to implement a keylogger using the python ‘keyboard’ library, every keystroke is stored in a array every x seconds the array is save in a file,

and then send the file via protocol chosen (email, https, sftp I personally https because it doesn’t requires password for your account).

If the files hasn’t been sent the file stay In memory till next sending time (multiple can be sent together), if the files has successfully been sent the local file is being deleted.

Now this is not enough because the keylogging is not active when the user logging, so what I had to find a solution.

My solution is to create a fake windows user elevation query which asks user for his password but even here I need to be sure the user will tempt to put in password in it.

For this I chose to ask the user to allow OneDrive Update to make changes in the computer, I even implemented the switch between PIN/password, the ‘/a’ bell sound when the window appeared .

But this is still not enough because I need the user to install at the first place so for this, I took an open-source python Typing game.

When the user plays the nothing happened (for the user thinking the prompt come from the game,

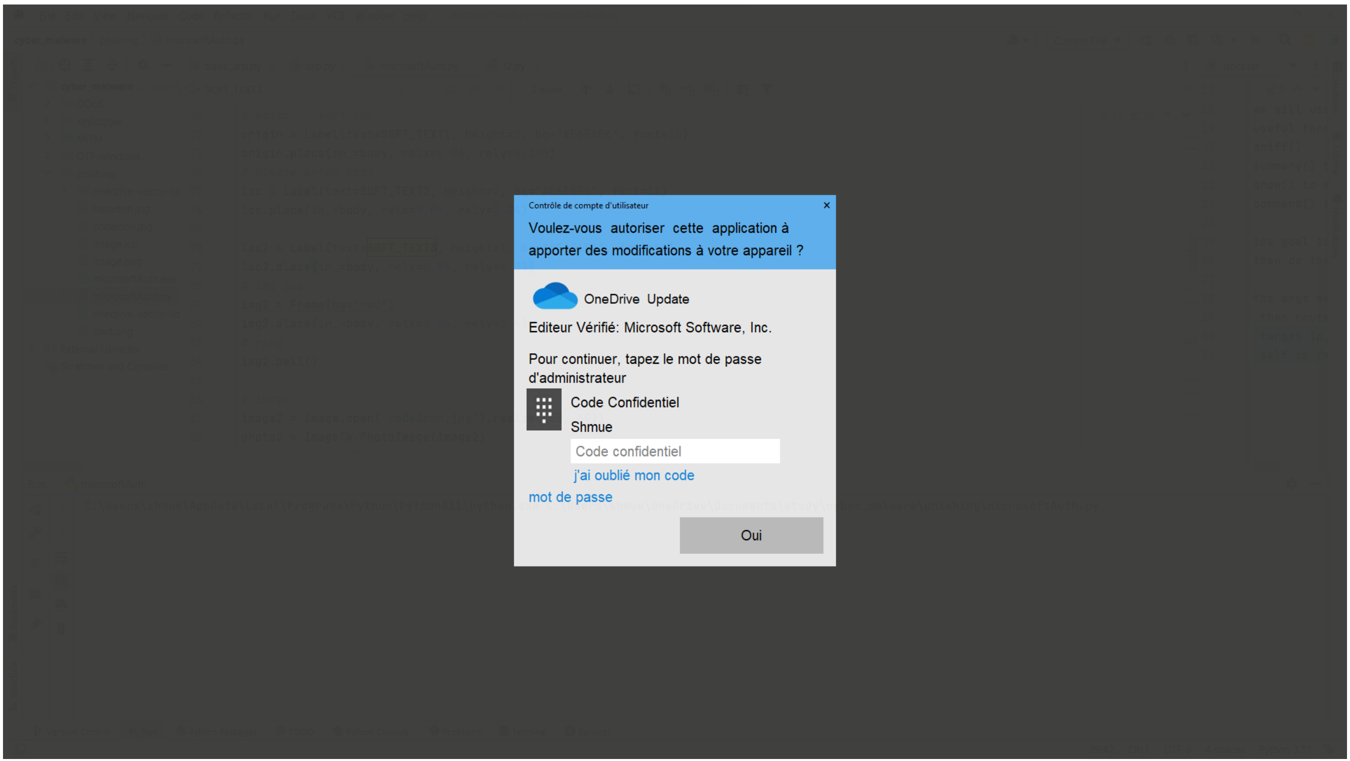
But when the user close the game it wait some time (1 min or more) and only then activates the keylogger and the fake windows prompt .

My only problems are that when the user launch it for the first time the blue SmartScreen pops out making the user suspicious (that is also one of the reason why I launch only some time after they closed the game), and that after few scan the keylogger get detected , I tried using an UPX packer but still … my next step will be to learn obfuscation technics.

But for the windows password I can implement a script which returns me what has been written in the input.

Pictures below

| | |
VVV



Contrôle de compte d'utilisateur ×

Voulez-vous autoriser cette application à apporter des modifications à votre appareil ?

OneDrive Update

Editeur Vérifié: Microsoft Software, Inc.

Pour continuer, tapez le mot de passe d'administrateur

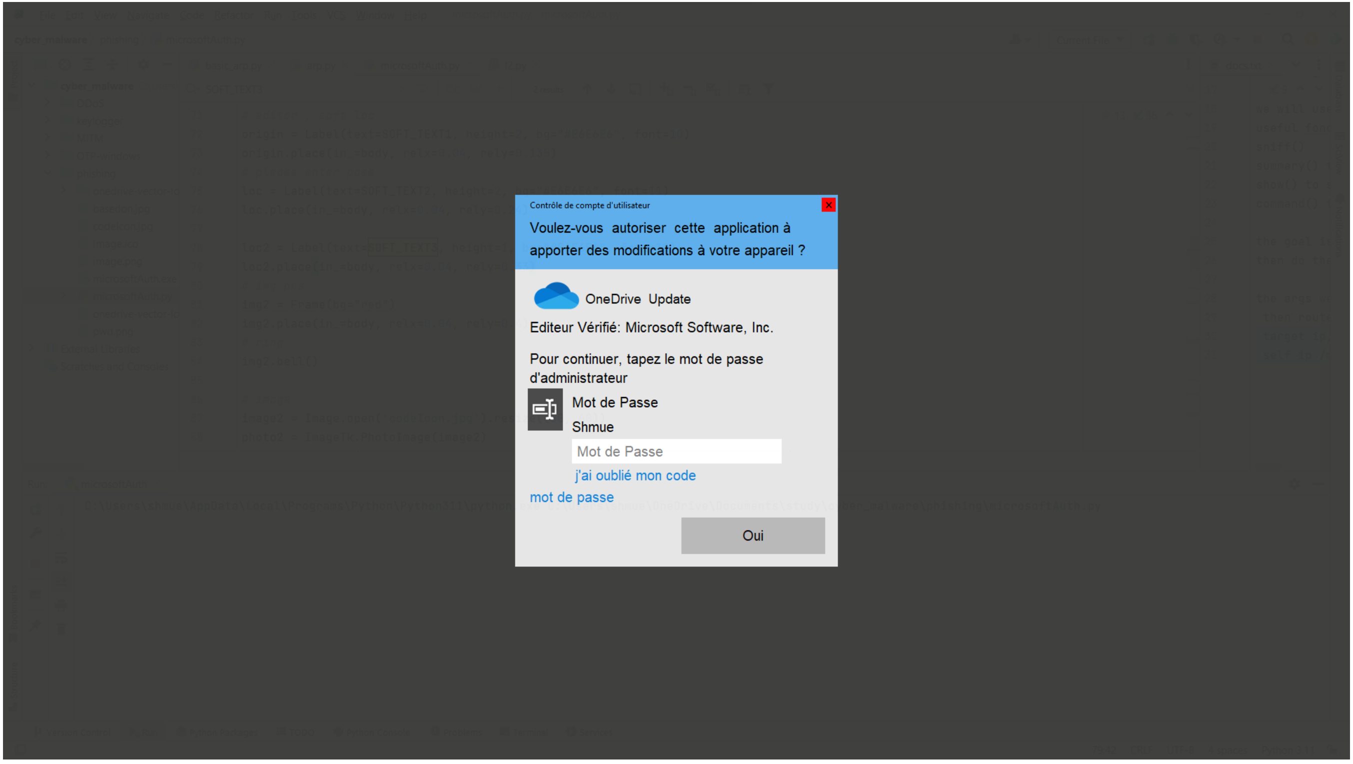
Code Confidentiel

Shmue

Code confidentiel

j'ai oublié mon code

mot de passe



Contrôle de compte d'utilisateur ×

Voulez-vous autoriser cette application à apporter des modifications à votre appareil ?

OneDrive Update

Editeur Vérifié: Microsoft Software, Inc.

Pour continuer, tapez le mot de passe d'administrateur

Mot de Passe

Shmue

Mot de Passe

j'ai oublié mon code

mot de passe