Security For the C-Suite
Python Keylogger Writeup

Made by: Catherine Burroughs, Casey Marshall, and Garrett Stagner

A keylogger is a spyware program that records the keys as they are struck on a keyboard. They are intended to run covertly, to not disturb the potential target. The main premise behind the keylogger is to get in-between any link in the chain of events from when a key is pressed and when information about that key is displayed on the monitor. Data can then be extracted from the target machine after their keystrokes are recorded. Financial records, personal secrets, and passwords are just a few of the many pieces of data that a keylogger can steal if your computer becomes compromised.

A keyboard contains mechanical switches or push-buttons that are called keys. When the keys are pressed, an electrical circuit is closed, and the computer's keyboard sends a signal to the computer telling it to display the corresponding key on the screen. This key mechanism is what keyloggers exploit.

The first line for the program is the "shebang". This specifies exactly how to run a script and allows it to be portable across different operating systems.

The second line imports the random module, which generates pseudo-random numbers. For the program randint is used, which helps to generate a random integer within a specified range. This range is customizable by the programmer of the keylogger and only serves the purpose of naming the file with a randomized number so the output does not write over itself. A range of (0,100) would print random numbers within the 0-99 range as it is inexclusive at the top.

The fourth line imports the pynput module, which allows the program to control and monitor input devices such as a mouse or keyboard. Pynput is a keyboard listener which interacts directly with the operating system to capture the keystrokes.

Listener allows us to run our program in a non-blocking fashion, meaning it will execute until stopped. It in turn responds to keys being pressed or released. These keys are written to an existing file that will be created.

Line five a value is assigned to a variable (output), this is used for naming our file. The value is composed of a string (pwnd) concatenated with a randomly generated number created by the randint function. This is where randint generates the random integer within the range that is used. As mentioned, this serves the purpose of making sure the keystrokes recorded are not saved over files but instead written to originals.

Line seven is designed to open our output file before the functions within the program begin. The file needs to be opened and given write permissions so the program is able to record the keystrokes to the text file.

Line eleven defines a function that is called from the imported pynput library. The function *on_press* is used to record keystrokes as they are pressed to our output file. It achieves this by opening the file in append mode, and allowing the keylogger to add the captured keystrokes to the output file.

Line seventeen defines the function *on_release* similar to the other above function that was also imported from the pynput library. This function records as the keys are released, in the instance that the keyboard is held down indefinitely, the *on_press* function will simply continue to be called on and the key will not be recorded until it is physically released.

Line twenty-three sets up the listener and includes our previous functions that were imported via the pynput library.