Advanced Keylogger in Python: Balancing Security and Ethics

Synopsis

"The key to defending against keyloggers lies not only in robust cybersecurity solutions but also in educating individuals about the dangers and empowering them to safeguard their digital lives." - Eugene Kaspersky

Zealand

Author: Szymon Zwara

Supervisor: Homayoon Fayez

Date: May 2023

Table of Contents

1. Introduction

With the increased usage of technology and the internet, the need for security and privacy has become more crucial than ever. One aspect of this is the use of keyloggers, which can be used for legitimate purposes such as monitoring employee activity or for malicious purposes such as stealing passwords. Python is a popular programming language for developing keyloggers due to its ease of use and versatility. However, the use of keyloggers raises ethical concerns about privacy invasion and data theft. Therefore, in this synopsis, we will explore the balance between security and ethics in the development of an advanced keylogger in Python.

1.1 Problem definition

The development of an advanced keylogger in Python raises ethical concerns about privacy and data theft. Therefore, it is essential to consider the implications of such a tool and ensure that it is developed in a responsible and ethical manner. This leads to the following set of questions that will be addressed in this synopsis:

Main question

How can we balance the security benefits of an advanced keylogger in Python with ethical considerations?

Sub-questions

- What are the technical aspects of developing an advanced keylogger in Python?
- How can the use of an advanced keylogger be beneficial for security purposes?
- What are the potential ethical concerns related to the use of keyloggers?
- What are some best practices for using keyloggers in an ethical manner?

1.2 Method

To answer the questions, I have chosen the following 3 activities:

- Researching the topic of keyloggers. The purpose of this activity is to broaden my knowledge and understanding about keyloggers as a whole and their purpose – both legitimate and malicious.
- Developing my own keylogger. In this activity, I will develop a keylogger of my own to see what are the technical aspects of building one.
- Researching the technical aspects of keyloggers and considering the legitimate and malicious uses for this type of software. The purpose of this activity is to gain the necessary insight to answer the questions specified in the problem definition.

1.3 Planning

To ensure that the project is completed in a timely and efficient manner, it is important to plan and organize the work into smaller tasks that can be completed within a given timeframe. With a 4-week deadline, I have planned the following activities:

Week 1 – Research and development of the keylogger

This week will be dedicated to gathering information on the topic of advanced keyloggers in Python and developing one myself. The goal will be to have a functional keylogger that can record keystrokes on a target device by the end of the week. Additional functionalities will be considered, such as: getting system information of the target machine (RAM, OS, Network), hijacking the clipboard contents, and doing screenshots.

Week 2 – Sub-questions

The second week will be focused on addressing the sub-questions related to the development of an advanced keylogger in Python. The goal will be to answer each of these sub-questions in a comprehensive and detailed manner.

Week 3 – Main question

The third week will be dedicated to addressing the main question of balancing security and ethics in the development of an advanced keylogger in Python. This will involve analyzing the technical aspects of developing a keylogger, as well as the potential ethical considerations related to its use. The goal will be to arrive at a balanced and well-reasoned answer to the main question.

Week 4 – Conclusion & Reflection

In the final week, the focus will be on evaluating the answers to all questions, summarizing the findings, and drawing conclusions. Finally, it will involve ensuring that the project adheres to ethical principles and that any potential ethical concerns are fully addressed.

2. Research and Development of the keylogger

2.1 Research

To start off my research, I decided to look for general information about keyloggers. By definition, a keylogger is a form of malware or hardware that keeps track of and records all the keystrokes one might type on the keyboard. The data is then sent to the hacker using a command-and-control server. Afterwards the data may be used for different types of malicious activities.[1]

Since I mentioned that a keylogger can be either in the form of software (malware) or hardware, I will take a few moments to explain how both can be implemented.

Software-based keyloggers are typically designed to infiltrate a target system through various means, such as malicious email attachments, infected websites, or software downloads. Once installed on the victim's computer, these keyloggers operate covertly, capturing and logging every keystroke made by the

[1] Fortinet, *"What is a keylogger? Definition and Types"*, https://www.fortinet.com/resources/cyberglossary/what-is-keyloggers (accessed 12.05.2023 @16:00)

user. They are commonly implemented as executable files that can be unknowingly downloaded through malicious websites, infected email attachments, or disguised as legitimate software. While the exact frequency of infections is challenging to determine, keyloggers pose a significant threat as they can infiltrate systems with varying levels of security, targeting both individuals and organizations.

On the other hand, **hardware-based** keyloggers are physical devices that are connected between the keyboard and the computer or placed inside the keyboard itself. These discreet devices intercept the electrical signals generated by the keystrokes, allowing them to record and store the input. Hardware keyloggers are more challenging to detect as they do not rely on software installations or modifications to the target system. [2]

Hardware keyloggers are physical devices that are physically connected between a computer or device and its keyboard. These devices come in various forms, such as small USB dongles, inline connectors, or even wireless transmitters. Once installed, hardware keyloggers silently capture keystrokes, including passwords, usernames, and sensitive information, without the user's knowledge. Due to their direct connection to the keyboard, hardware keyloggers can be challenging to detect using traditional antivirus or anti-malware software. While less prevalent than software keyloggers, they still pose a significant risk, particularly in scenarios where the attacker has physical access to the targeted device.

One example of such a device is the KeyGrabber USB from Keelog, which according to the manufacturer is equipped with 16GB of memory, which translates to over 8 thousand pages of text, 128-bit encryption, quick and easy installation, and complete transparency to the targeted system. It can be operated in record mode, which logs all the keystrokes on the machine, as well as playback mode, which then allows the user to retrieve the stored data. Currently it can be bought for $45 online and is a great tool especially for monitoring employee productivity at a company.[3]

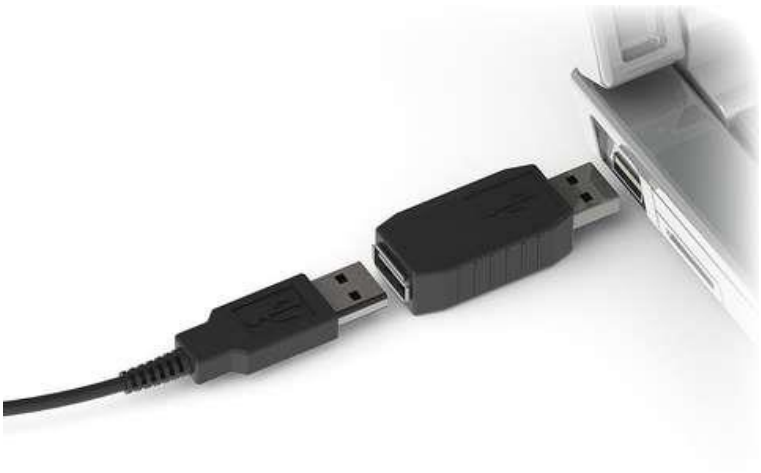

Figure 1 - KeyGrabber USB usage

Having touched upon this, the focus of this synopsis will be based on an implementation of a software keylogger, which will be written in Python.

[2] GeeksEngine, *"What is keylogger and the differences between software and hardware keylogger."*, http://www.geeksengine.com/article/keylogger.html (accessed 13.05.2023 @19:00)
[3] Keelog, *"KeyGrabber USB"*, https://www.keelog.com/usb-keylogger/ (accessed 17.05.2023 @17:00)

2.2 Development

To answer the questions that are mentioned in the problem formulation I had to develop the actual keylogger. This would help me with a greater understanding of the technical aspects of creating such a tool. My choice of programming language was Python, as it is fast, reliable, has a vast collection of available libraries and I have already used it before for one of the school projects.

Unfortunately, the task turned out to be a bit too complicated to complete without any help in the short amount of time that I had, so I decided to follow a tutorial by Grant Collins, where he goes deep into how to develop the software in question.[4] This allowed me to finish it in much less time, which in turn gave me more time to consider the main and sub questions.

In this section I won't go too much into detail about the technical aspects of development, as this will be covered in the next one. Instead, I would like to talk about my thoughts and opinions about the development process and the challenges that I encountered along the way.

To start off, I created a small diagram that illustrates the logic of the application.

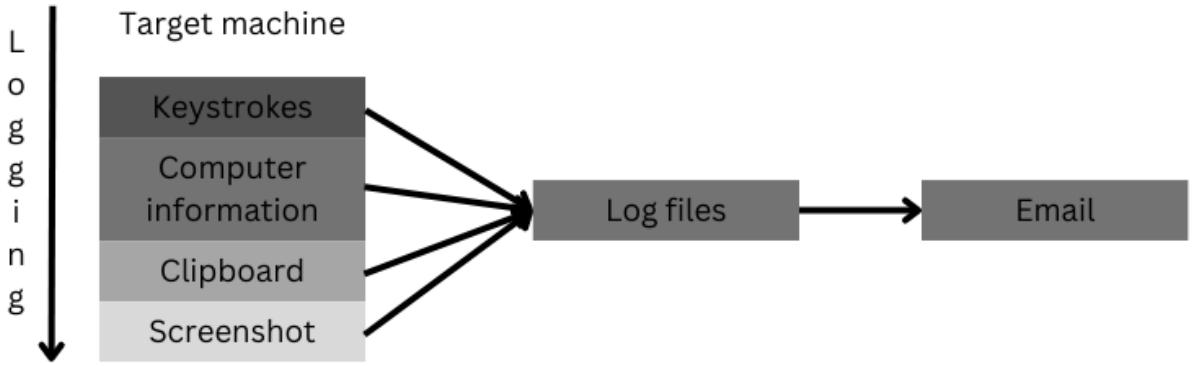

Figure 2 - Logic diagram of the keylogger

The items on the left are the ones that the application gathers during its operation. Later, this information is saved to the respective log files, which are then sent via a disposable email to the recipient. Basing off this diagram and the tutorial I have started the development.

The first obstacle I encountered was installing the necessary libraries. Installing the required dependencies, such as keyboard event handlers, encryption modules, and networking libraries proved to be a complex task. Issues arose due to difficulties in resolving dependencies. Even though everything was installed properly, the compiler was complaining about unresolved references. Luckily, the documentation to some of the libraries helped me to finish the set up. Another hurdle turned out to be the SMTP configuration for the mail server that is used to send the log files to the recipient. This has led me to trying out a few different ports until I finally found one that worked.

After that the development went without any major issues, which eventually left me with a finished product.

[4] Grant Collins, *"Create an Advanced Keylogger in Python - Crash Course"*, https://www.youtube.com/watch?v=25um032xgrw (accessed 17.05.2023 @19:00)

3. What are the technical aspects of developing a keylogger?

In this section I would like to discuss the numerous technical aspects of developing a keylogger that I went through during the process. My focus will be on specific portions of the application, which make up the core functionality. I will also provide code snippets for some of the most interesting ones.

The first component that I would like to mention is the function that is logging all the keystrokes and saving them in a file.

```
keys =[]
    def on_press(key):
        global keys, count, currentTime

        print(key)
        keys.append(key)
        count += 1
        currentTime = time.time()

        if count >= 1:
            count = 0
            write_file(keys)
            keys =[]

    def write_file(keys):
        with open(file_path + extend + keys_information, "a") as f:
            for key in keys:
                k = str(key).replace("'", "")
                if k.find("space") > 0:
                    f.write('\n')
                    f.close()
                elif k.find("Key") == -1:
                    f.write(k)
                    f.close()
```

Figure 3 - Key logging functionality

The on_press method prints all pressed keys to the terminal, as well as appends them to the keys array. After that, it uses the write_file method to write the log file. This makes up the core functionality of the keylogger.

The keylogger also gathers computer information, contents of the clipboard, and periodically takes a screenshot of the target machines desktop, which happens in a similar manner utilizing different python libraries. I will not include these functionalities in this paper, as I think that they don't differ too much from the one I mentioned.

Another functionality worth mentioning is the encryption part, as making the log files confidential is very important when dealing with log files that might contain sensitive information. For that, I have used two extra python scripts – GenerateKey and DecryptFile. They both use the Fernet package, which allows the

use of symmetric encryption to obfuscate the log files. The GenerateKey script generates a unique key which is used in the keylogger by Fernet to provide the encryption. The same key is later used in the DecryptFile script to decrypt the files.

```
files_to_encrypt = [file_merge + system_information, file_merge +
clipboard_information, file_merge + keys_information]
encrypted_file_names = [file_merge + system_information_e, file_merge +
clipboard_information_e, file_merge + keys_information_e]

count = 0

for encrypting_file in files_to_encrypt:

    with open(files_to_encrypt[count], 'rb') as f:
        data = f.read()

    fernet = Fernet(key)
    encrypted = fernet.encrypt(data)

    with open(encrypted_file_names[count], 'wb') as f:
        f.write(encrypted)

    print("Email will be sent soon")
    send_email(encrypted_file_names[count], encrypted_file_names[count], toaddr)
    count += 1
    print("Email has been sent")
```

Figure 4 - Symmetric encryption of log files

The first two lists contain information about the paths and the names of files that are to be encrypted. After that, the for loop opens each file, reads its data, and uses the pre-generated key to encrypt and write the files, which are then sent to an email of our choice by a predefined method. After that, the application makes sure to cover its tracks by removing the log files from the target machine.

4. How can the use of an advanced keylogger be beneficial for security purposes?

The use of an advanced keylogger can have significant benefits for security purposes by enabling organizations and individuals to proactively monitor and protect their digital assets. Keyloggers, when used responsibly and within legal boundaries, can help identify potential security threats, detect unauthorized access attempts, and enhance incident response capabilities. For instance, businesses can utilize keyloggers to monitor employee activity and identify any suspicious behavior or insider threats. In these cases, the employees must be properly notified about the usage of such monitoring technology. Law enforcement agencies can employ keyloggers in investigations to gather evidence against

cybercriminals involved in activities such as hacking, fraud, or harassment. Additionally, individuals can utilize keyloggers to protect their personal information by monitoring their own devices for any unauthorized access attempts or suspicious activities. [5]

In my opinion, keyloggers can be beneficial for security purposes when used within legal boundaries. It Is important to maintain consent practices and ensure that privacy rights are respected when using keylogging technology.

5. What are the potential ethical concerns related to the use of keyloggers?

The use of keyloggers raises significant ethical concerns due to the potential for misuse and invasion of privacy. While I explained that keyloggers can serve legitimate security purposes when used responsibly, they can also be exploited for malicious activities. One major concern is the unauthorized installation of keyloggers on individuals' devices, without their knowledge or consent, which violates their right to privacy. [6] Malicious actors can exploit keyloggers to steal sensitive information such as passwords, credit card details, or personal data, leading to identity theft or financial loss. Moreover, keyloggers can be used for stalking or harassment purposes, enabling individuals to monitor someone's private conversations, emails, or online activities without their consent. Additionally, keyloggers can be employed by cybercriminals to gain unauthorized access to networks or compromise systems, resulting in data breaches or unauthorized surveillance. [7]

It is crucial to raise awareness about these ethical concerns and promote responsible use of keyloggers to ensure privacy rights are respected and individuals are protected from potential abuse. It's also important to educate about ways to notice a keylogger infection and protect yourself from it happening.

6. What are some best practices for using keyloggers in an ethical manner?

When using keyloggers, it is essential to adhere to ethical guidelines to ensure responsible and lawful usage. Firstly, obtaining explicit consent from individuals whose devices will be monitored is crucial. Clear communication and transparency about the purpose and extent of monitoring will help maintain trust and respect privacy boundaries. Secondly, limiting the use of keyloggers to legitimate security purposes is essential, such as protecting against insider threats, detecting unauthorized access attempts, or investigating cybercrimes with proper legal authorization. Thirdly, implementing strict security

---

[5] Daniel Petri, *"What is Advanced Corporate Keylogging? Definition, Benefits and Uses"*, https://www.proofpoint.com/us/blog/insider-threat-management/what-advanced-corporate-keylogging-definition-benefits-and-uses (accessed 18.05.2023 @11:00)

[6] CrazyLeaf, *"Navigating the Legal and Ethical Issues of Using Keylogger Software in the Workplace"*, https://www.crazyleafdesign.com/blog/navigating-legal-ethical-issues-using-keylogger-software-workplace/ (accessed 18.05.2023 @12:00)

[7] CrowdStrike, *"Keyloggers: How do they work and how to detect them"*, https://www.crowdstrike.com/cybersecurity-101/attack-types/keylogger/ (accessed 18.05.2023 @12:30)

measures to protect the collected data from unauthorized access is important. Encryption, secure storage, and access controls should be employed to safeguard the information gathered through keylogging. Lastly, regularly reviewing and assessing the necessity of keylogging activities is recommended to ensure that it remains justified and aligned with legal and ethical obligations. [8]

In my opinion, by following these best practices, keyloggers can be used ethically, with a focus on maintaining privacy, respecting consent, and enhancing overall security measures.

7. How can we balance the security benefits of an advanced keylogger in Python with ethical considerations?

Balancing the security benefits of an advanced keylogger in Python with ethical considerations requires a responsible and conscientious approach. When considering the security benefits of an advanced keylogger in Python, it is crucial to address the ethical considerations discussed earlier. This includes obtaining explicit consent from individuals, as mentioned in the previous paragraph, and maintaining transparency in the monitoring process. Additionally, implementing strict security measures to protect the collected data, as highlighted before, is vital to safeguard sensitive information from unauthorized access. Furthermore, limiting the use of the keylogger to legitimate security purposes, as previously mentioned, ensures that it is not misused for unethical activities. Regularly reviewing the necessity of keylogging activities helps maintain compliance with legal and ethical obligations.

I think that by integrating these practices, the security benefits of an advanced keylogger in Python can be balanced with ethical considerations, promoting responsible and lawful usage while respecting privacy rights and maintaining ethical standards.

8. Conclusion

In conclusion, the use of an advanced keylogger in Python for security purposes requires careful consideration of ethical principles. While keyloggers can provide significant security benefits, it is imperative to prioritize consent, transparency, and privacy protection. By obtaining explicit consent, implementing robust security measures, limiting usage to legitimate security purposes, and regularly reviewing the necessity of keylogging activities, a balance can be achieved between enhancing security measures and respecting ethical considerations. Responsible and ethical use of advanced keyloggers ensures that individuals' privacy rights are upheld while effectively addressing security concerns. Striking this balance is essential in maintaining trust, safeguarding sensitive information, and adhering to legal and ethical obligations.

[8] Alonzo Martinez, *"From Keylogging To Spyware: What Should Employers Consider When Monitoring Remote Workers?"*, https://www.forbes.com/sites/alonzomartinez/2020/05/15/from-keylogging-to-spyware-what-should-employers-consider-when-monitoring-remote-workers/?sh=240d6e893981 (accessed 18.05.2023 @13:00)

9. Reflection

While reflecting on the questions that I have answered in previous sections I have noticed areas where improvements could have been made. Now that I have more knowledge and understanding, I can ask more insightful questions that would have led to a more thorough exploration of the topic. The method I used to address each question individually was suitable, but I could have improved by conducting additional research and analysis. This would have allowed me to provide a more comprehensive understanding of the subject. In terms of planning, I could have been more organized by outlining specific points to cover and creating a clearer structure. By doing so, the ideas would have flowed more smoothly, resulting in a better final product. In retrospect, I would also have started the development of the keylogger earlier, which would probably make me refrain from using an external tutorial.

10. References

Alonzo Martinez, *"From Keylogging To Spyware: What Should Employers Consider When Monitoring Remote Workers?"*, https://www.forbes.com/sites/alonzomartinez/2020/05/15/from-keylogging-to-spyware-what-should-employers-consider-when-monitoring-remote-workers/?sh=240d6e893981

CrazyLeaf, *"Navigating the Legal and Ethical Issues of Using Keylogger Software in the Workplace"*, https://www.crazyleafdesign.com/blog/navigating-legal-ethical-issues-using-keylogger-software-workplace/

CrowdStrike, *"Keyloggers: How do they work and how to detect them",* https://www.crowdstrike.com/cybersecurity-101/attack-types/keylogger/

Daniel Petri, *"What is Advanced Corporate Keylogging? Definition, Benefits and Uses",* https://www.proofpoint.com/us/blog/insider-threat-management/what-advanced-corporate-keylogging-definition-benefits-and-uses

Fortinet*, "What is a keylogger? Definition and Types",* https://www.fortinet.com/resources/cyberglossary/what-is-keyloggers

GeeksEngine, *"What is keylogger and the differences between software and hardware keylogger",* http://www.geeksengine.com/article/keylogger.html

Grant Collins, *"Create an Advanced Keylogger in Python - Crash Course",* https://www.youtube.com/watch?v=25um032xgrw

Keelog, *"KeyGrabber USB",* https://www.keelog.com/usb-keylogger/