kb-keylogger
Malware & Forensics Project

Berat Kocak

April 2026

Contents

1. Project Overview

This project demonstrates a two-phased attack and detection scenario. In the first phase, a hardware keylogger intercepts keyboard input on a target machine and periodically exfiltrates the captured data to a remote server every 10 minutes. In the second stage, forensic analysis is conducted on the target system to reconstruct the attack timeline and identify evidence of the data exfiltration.

1.1. Motivation & Learning Objectives

The primary objective of this project is to explore and understand the technical lifecycle of credential exfiltration. By developing and analyzing the tool, I aim to address the following questions:

1. Technical Implementation
   - **Input Hooking:** Understanding the architectural differences in how various Operating Systems process keyboard interrupts.
   - **Stealth:** Developing methods to capture inputs without disrupting the user experience or triggering system alerts.
2. Data Management & Exfiltration
   - **Storage:** Determining efficient and secure structures for local log storage.
   - **Exfiltration:** Defining protocols for remote C2 transmission.
   - **Noise Reduction:** Implementing techniques to minimize the digital footprint of data transmission to evade detection.
3. Critical Evaluation
   - **Iterative Development:** Identifying weaknesses in the initial design and implementing structural improvements.
   - **Infection Vectors**: Moving away from a hardware to a software-only solution.
   - **Gap Analysis:** Documenting persistent technical challenges and areas for further research.

1.2. Scope

The technical scope of this project is confined to the development of the kb-keylogger and its subsequent forensic analysis within a controlled environment. Malware characteristics such as boot-level persistence, EDR or Antivirus evasion and the weaponization of the tool are explicitly excluded.

1.3. Disclaimer

The goal of this project is exclusively to educate myself on this topic and learn new technologies and their security implications. The author assumes no responsibility for any misuse or damages arising from the application of the information contained within this report.

2. Phase A: Keylogger Development

2.1. Hardware

I am using a WaveShare ESP32-S3 Mini Microcontroller, which will connect to the target machine via USB-C port. The keylogger is going to be uploaded to this device and monitor the keypoard inputs on the target machine.

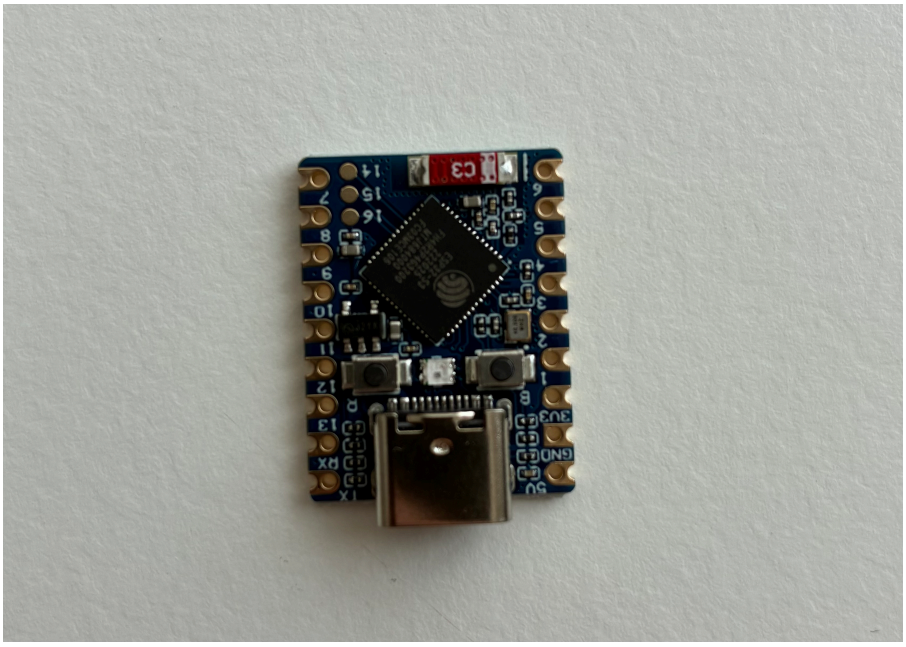

Figure 1: The WaveShare ESP32-S3 Mini and its built-in USB-C Port

2.2. Design & Architecture

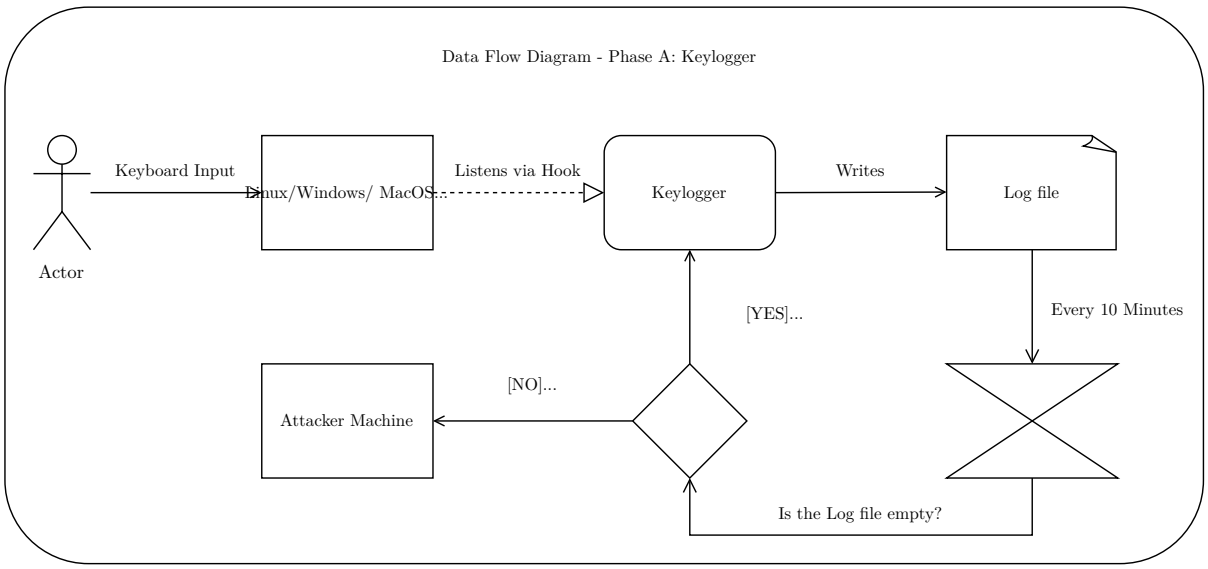

Figure 2: First draft of the Data Flow Diagram

2.3. Implementation Details

2.3.1. Keyboard Capture Linux

2.3.2. Keyboard Capture Windows

2.3.3. Keyboard Capture MacOS

2.3.4. Data Logging

2.3.5. Exfiltration

2.4. Challenges & Solutions

3. Phase B: Forensic Analysis

3.1. Methodology and Tools

3.2. Evidence Collection

3.2.1. Traffic Capture

3.2.2. System artifacts

3.3. Analysis

3.3.1. Networt traffic

3.3.2. Behavior

4. Results & Observations

4.1. Reflection on Initial Goals

5. Future Improvements

5.1. Keylogging

5.2. Defensive Implications

6. Appendix

6.1. Source Codes

6.2. Screenshots

6.3. Timeline tables