University of Wah

Department of Computer Science

BS Cyber Security

Malware Analysis

Project Report

Title: Remote HID-Based Malware Injection Framework

BLE Rubber Ducky–Style Attack Simulation

Submitted to: Sir Inzmamul Haq

Group Members:

Muhammad Azfar Waqas (UW-23-CY-BS-013)

Ibrar Ul Hassan Shami (UW-23-CY-BS-018)

Hassan Iftikhar (UW-23-CY-BS-002)

Section: BS-CYS-5N

Table of Contents

1 Introduction:

Malware attacks increasingly rely on **social engineering and trusted input channels** rather than traditional exploits. One such vector is **Human Interface Device (HID) injection**, where malicious commands are executed by impersonating a legitimate keyboard or input device.

This project focuses on the **analysis of HID-based malware attacks** using a **Bluetooth Low Energy (BLE)–enabled ESP32 platform**. The system remotely emulates a trusted BLE keyboard and injects pre-defined command payloads into a target system, allowing students to analyze how malware can be delivered **without dropping files or exploiting vulnerabilities**.

The project is designed strictly for **malware analysis education**, emphasizing **behavioral analysis, execution flow, and attack vectors**, rather than real-world exploitation.

---

2 Problem Statement:

Traditional malware detection mechanisms focus on **file-based signatures and exploits**, while modern attacks increasingly abuse **trusted peripherals** such as keyboards and Bluetooth devices. HID-based attacks bypass antivirus software because the system interprets malicious input as **legitimate user activity**.

Students often study malware theoretically but lack practical exposure to:

- Non-file-based malware delivery
- Input-device impersonation attacks
- Command-based malware execution

There is a need for a **controlled framework** that demonstrates how such malware behaves **after execution**, enabling proper malware analysis and defensive understanding.

---

3 Project Objectives:

The objectives of this project are to:

- Analyze **HID-based malware delivery techniques**
- Demonstrate **BLE keyboard impersonation attacks**
- Study command-based malware execution behavior
- Analyze how malware bypasses traditional security controls
- Observe system behavior during HID-based attacks
- Promote ethical malware research and analysis

---

4 Scope of the Project:

This project includes:

- BLE HID keyboard emulation using ESP32
- Remote execution of predefined payloads
- Malware behavior analysis (post-execution)
- Observation of system response and user interaction
- Testing in isolated and authorized environments only

The project does **not**:

- Spread malware autonomously
- Target real users or networks
- Bypass authentication mechanisms

---

5 Tools & Technologies:

Tools & Technologies	Purpose
ESP32 DevKit (WROOM-32)	BLE HID emulation
Arduino IDE	Firmware development
Bluetooth Low Energy (BLE)	Remote HID communication
Windows Test VM	Malware behavior analysis
PowerShell / CMD	Command-based payload execution
SPIFFS	Payload storage

---

6 Methodology:

Threat Identification:

The following malware techniques are analyzed:

- HID-based command injection
- Trusted device impersonation
- Fileless malware execution
- User-initiated attack simulation

Asset Identification:

- System integrity
- User trust
- Input device authenticity

---

7 Malware Attack Implementation:

- ESP32 is configured as a **BLE keyboard**
- Predefined payloads are stored in SPIFFS
- Upon trigger, the device injects:
  - ✓ System commands
  - ✓ Script execution commands
- Payloads are executed as **legitimate keyboard input**

This simulates a **Rubber Ducky–style malware attack**, executed remotely via BLE.

---

8 Controlled Testing & Analysis:

- All tests are performed on:
  - ✓ Virtual machines
  - ✓ Authorized test systems
- Observations include:
  - ✓ Execution flow
  - ✓ System logs
  - ✓ User interface response

---

9 Expected Outcomes:

- Successful demonstration of HID-based malware attacks
- Understanding of fileless malware execution
- Insight into how trusted devices can be abused
- Improved malware behavior analysis skills
- Stronger understanding of defensive countermeasures

---

10 Significance of the Project

This project bridges the gap between **theoretical malware concepts** and **real-world attack behavior**. By demonstrating how malware can be delivered through trusted HID channels, students gain practical insight into modern attack techniques that bypass traditional security controls.

The project is highly relevant for cybersecurity education, particularly in **malware analysis, red teaming, and defensive security research**.

---

11 Conclusion:

The project successfully demonstrates a **remote HID-based malware injection framework** using an ESP32 BLE platform. It highlights how malware can be executed without exploiting vulnerabilities, relying instead on trusted device impersonation.

The system serves as an effective educational tool for understanding modern malware delivery techniques and reinforces the importance of behavior-based detection and defensive security strategies.

---

12 References:

1. Hak5. (2022). *USB Rubber Ducky: Keystroke Injection Attacks*. Hak5 Official Documentation.
2. Bluetooth Special Interest Group (SIG). (2022). *Bluetooth Low Energy (BLE) Security Overview*.
3. Espressif Systems. (2023). *ESP32 Technical Reference Manual*.
4. MITRE Corporation. (2023). *MITRE ATT&CK® Framework – Input Injection (T1056 / T1204)*.
5. National Institute of Standards and Technology (NIST). (2014). *Guide to Malware Incident Prevention and Handling (Special Publication 800-83 Rev. 1)*.
