Autonomous Exploitation Via Malware Injection Using Raspberry PI

Sanjai J [1], Harivikas M [2], Saravanan K [3], Hariharan S [4]
[1,2,3,4]*Bharath Institute of Higher Education and Research, Chennai, India*

Abstract -The Autonomous Exploitation via Malware Injection is an advanced USB attack framework designed for penetration testing and cybersecurity research. It is built for the Raspberry Pi Zero W/2W, transforming it into a malicious HID (Human Interface Device) that can execute automated payloads for exploitation, data exfiltration, and privilege escalation. This project provides a modular and customizable platform for offensive security testing. This framework allows security professionals to simulate real-world attack scenarios, including keystroke injection, remote shell execution, Wi-Fi phishing, and persistence mechanisms. It can bypass security controls such as User Account Control (UAC), antivirus detection, and endpoint security policies by executing obfuscated payloads.

Keywords: Malicious HID, Automated Payloads, Exploitation, Data Exfiltration, Privilege Escalation, Modular Platform, Offensive Security, Keystroke Injection, Remote Shell Execution, Wi-Fi Phishing, Persistence Mechanisms.

I. INTRODUCTION

The Autonomous Exploitation via Malware Injection using Raspberry Pi project is an advanced USB attack platform designed for penetration testing and cybersecurity research. Built for the Raspberry Pi Zero W/2W, it transforms the device into a malicious Human Interface Device (HID) capable of executing automated payloads for system exploitation, privilege escalation, and data exfiltration. The project serves as an open-source alternative to traditional USB Rubber Ducky attacks, offering enhanced functionality and customization.

II. SCOPE OF THE PROJECT

1. USB-Based Security Exploitation & Testing
This project explores USB-based attack techniques, including HID emulation, keystroke injection, and privilege escalation, to test system vulnerabilities. It helps penetration testers, Red Teams, and cybersecurity researchers simulate real-world attack scenarios and evaluate how malicious USB devices can bypass security mechanisms such as antivirus, UAC, and endpoint protection.

2. Multi-Platform Attack Simulation
The project is designed to be compatible with Windows, Linux, and macOS, enabling cybersecurity professionals to analyze, test, and develop defenses against USB-based threats. Its multi-platform functionality allows for comprehensive penetration testing across different system architectures.

3. Cybersecurity Awareness & Defensive Strategies
Beyond offensive security, the project aims to educate organizations about USB security risks. By identifying vulnerabilities, it helps security teams implement stronger endpoint protection policies, restrict unauthorized USB access, and develop better mitigation strategies to prevent cyber threats.

4. Future Advancements & AI-Driven Enhancements
Future enhancements could include AI-powered adaptive payloads, advanced anti-forensic techniques, and wireless attack capabilities. These improvements would further refine the project's ability to bypass security mechanisms, automate attack scenarios, and enhance cybersecurity research while also strengthening detection and defense strategies.

III. SYSTEM ARCHITECTURE

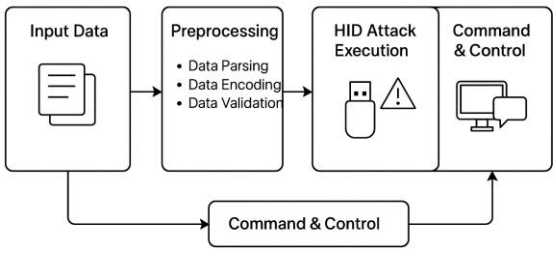

Fig. System Architecture

IV. METHODOLOGY

The proposed system consists of hardware, software, and strategic modules:

Hardware Setup: Raspberry Pi Zero W/2W with USB OTG, powered via portable battery.

Software Tools: Kali Linux (Lite), HID gadget configurations, Python, Bash scripting, Metasploit, and Bettercap.

Modules:

Reconnaissance and vulnerability scanning

Payload deployment (e.g., credential harvesting, reverse shells)

Persistence and evasion (DLL injection, task scheduling)

Command & Control communication (reverse shell using HTTPS/DNS tunnels)

The system auto-executes payloads upon USB connection, simulating real-world keystroke injection or network manipulation attacks.

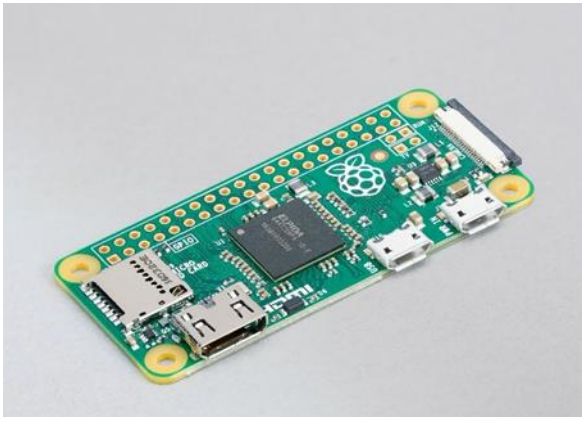

Fig. Raspberry pi

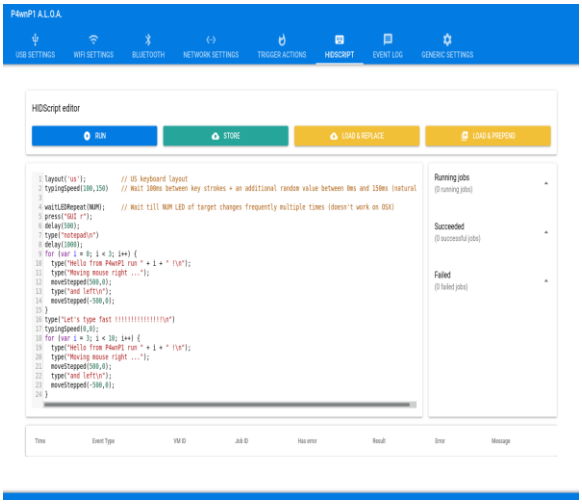

Fig. HID script

V. CONCLUSION

This project successfully demonstrated the capabilities of USB-based HID attacks using a Raspberry Pi device. By emulating a trusted USB keyboard/mouse, it was able to execute automated keystroke injections, deploy payloads, and establish remote access on target systems. The results highlighted how default system configurations often fail to detect or prevent such attacks, making them a serious cybersecurity threat. Additionally, the project showcased various attack techniques, including credential harvesting, privilege escalation, data exfiltration, and network interception. The success of these attacks emphasizes the need for stronger endpoint security measures, such as USB whitelisting, disabling autorun scripts, and deploying advanced endpoint detection and response (EDR) solutions. In conclusion, this project serves as a valuable tool for penetration testing and cybersecurity research, helping security professionals understand, detect, and mitigate USB-based attacks. It reinforces the importance of security awareness and policy enforcement to protect against real-world threats.

V. ACKNOWLEDGEMENT

We express our sincere gratitude to Dr. L. Godlin Atlas, our project guide, for his continuous support and guidance throughout the course of this research. We also thank Dr. S. Maruthuperumal, Head of the Department, and all faculty members of the Department of Computer Science and Engineering (Cyber Security) at Bharath Institute of Higher Education and Research for providing us the resources and motivation to complete this project successfully.

REFERENCE

[1] Mayuri Khadpe, Pranita Binnar, Dr. Faruk Kazi, "Malware Injection in Operational Technology Networks," IEEE, 2018.

[2] Maryna Yevdokymenko, Elsayed Mohamed, Paul Onwuakpa Arinze, "Ethical Hacking and Penetration Testing Using Raspberry PI," IJCSIT, 2019.

[3] Dimitrios Tychalas, Anastasis Keliris, Michail Maniatakos, "Stealthy Information Leakage Through Peripheral Exploitation in Modern Embedded Systems," IEEE Transactions, 2020.

[4] S. Kim, "Anatomy on Malware Distribution Networks," in IEEE Access, vol. 8, 2020.
[5] O. A. Aslan and R. Samet, "A Comprehensive Review on Malware Detection Approaches," IEEE Access, 2020.