Rubber Duckies/BadUSBs

Ash Brown

September 2023

1 Introduction

A BadUSB (sometimes known as a Rubber Ducky), is an HID device that is disguised as a regular USB and can be used to quickly configure the system, run scripts, or deliver malware to a computer system.

2 Background

A Rubber Ducky refers to a brand of BadUSBs made by Hak5. However, there are many other types of BadUSBs available, such as Digisparks, Flipper Zeros, or even regular USBs.

3 Uses

BadUSBs were originally used to automate tedious tasks in the workplace by IT professionals, but they have evolved into a common hacking tool. In the world of pentesting, BadUSBs are typically used to test the human actors in a company. If a pentester is able to insert a BadUSB into a company computer, or if an employee inserts a gifted or planted USB into a computer, then that demonstrates a vulnerability in the company's security, and the company should consider briefing their employees on BadUSBs. BadUSBs are also used maliciously by hackers in order to covertly/remotely deliver malicious payloads.

4 Hardware

A Human Interface Device (HID) is a device that can be connected to a computer to allow a user to interact with the system. HID devices include monitors, keyboards, mice, BadUSBs, and more. BadUSBs act like a keyboard, but can be preprogrammed to inject a series of keystrokes quickly and covertly. Because HID devices are inherently trusted by computer systems, there is not much one can do to protect their system from a BadUSB attack. Some BadUSBs have storage on them either to exfiltrate data, or for storing larger payloads.

5 Software

Hak 5 Rubber Duckies are programmed with Ducky Script, a simple scripting language written specifically for Duckies. Other BadUSBs can be programmed with nearly any language, such as Python, Javascript, or even C. For example, Digispark BadUSBs are programmed with C++.

6 References

"Everything I Can Remember About Rubber Duckies". *My big fat brain.* Retrieved 2023-09-24.