BadUSB: Rubber Duckies

Amira C

October 2023

1 Introduction

A rubber ducky is when a USB device that allows itself to be disguised as an HID. Once connected to its target computer, it could then executes discreetly harmful commands or injects malicious content.

HID stands for Human Interface Devices such as keyboards, mouses, joysticks....

2 Historical Background

The Rubber Ducky USB drive was first used by the U.S. and Israel intelligence agencies to infiltrate Iranian nuclear facilities. By getting the USB drives into the hands of their nuclear scientists, they would use them inside the facilities to distribute malware on the network systems. The malware would overwrite the nuclear centrifuge systems to damage their equipment while modifying their control systems to show everything was normal. This secret project was called Stuxnet, a malicious computer worm first uncovered in 2010 and thought to have been in development since at least 2005.

3 References

https://www.manageengine.com/device-control/badusb.html: :text=BadUSB
https://orlantech.com/beware-of-the-rubber-ducky/: :text=A
https://en.wikipedia.org/wiki/Stuxnet