

Creating a Smart BadUSB

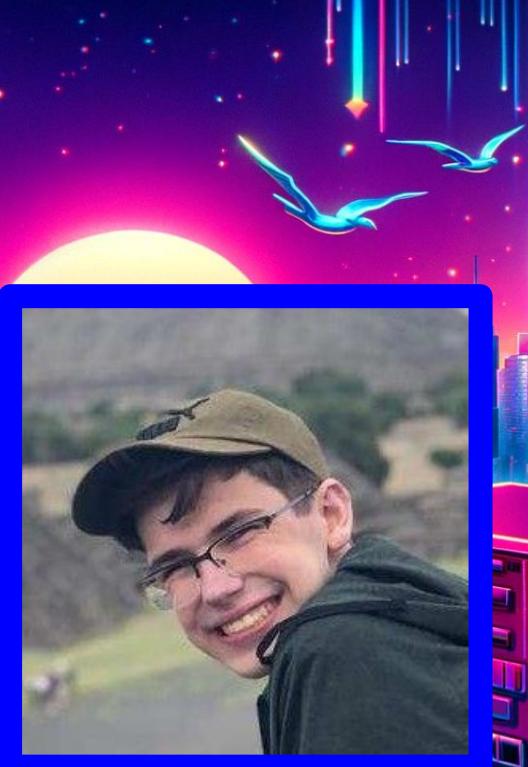


Who am I?

My name is Brandon Hawkins, I am a senior majoring in Computer Science with a focus in Cyber Operations at UTSA.

I am an electronics tinkerer with a deep passion for cybersecurity and innovation.

I enjoy learning and interacting with both the hardware and software side of technology.



BadUSB Overview

- What is a BadUSB?
 - Definition: USB device mimicking a keyboard
 - Created using Raspberry Pi or Arduino
- Execution and Disguise
 - Often disguised as USB thumb drives
 - Executes malicious payload upon connection
 - Takes less than one second to complete
- Payload Execution
 - Utilizes Windows "Run" dialog (Windows Key + R)
 - Enables rapid PowerShell code execution
 - Potential consequences: Remote access, data theft



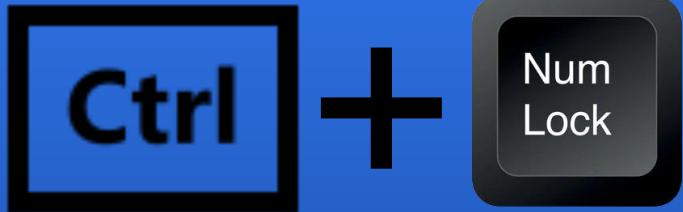
So why is a “smart” BadUSB needed?

- Obviousness of BadUSB
 - Run dialog pops up upon USB insertion
 - Limited time for attacker's actions
 - Risk of shutdown or removal of malicious script
- Execution Challenges
 - BadUSB behavior varies during computer startup, lock screen, or different OS (e.g., Mac or Linux)
 - Premature payload execution may reveal its presence
- "Smart" BadUSB - HID Approach
 - Embedded in a Human Interface Device (HID)
 - Example: Standard USB computer mouse
 - Explanation for choice to follow



What makes it “smart”

- Detection of Windows using the HID Protocol
 - Utilizes built in keyboard LEDs for status checks
 - These leds perform differently depending on OS, lockscreen, etc
- Checking For Mouse Activity
 - Use of a phototransistor to check mouse LED brightness
 - If dim, then mouse isn't being used
- Self Destructs After Successful Payload
 - The arduino disables itself and will not run again



Things you'll need



Any USB Mouse



Soldering Iron & Solder



Arduino IDE



USB 2.0 Expansion Module



Arduino Pro Micro



26 awg (or similar)
wire



120 Ohm Resistor
(or similar resistance)



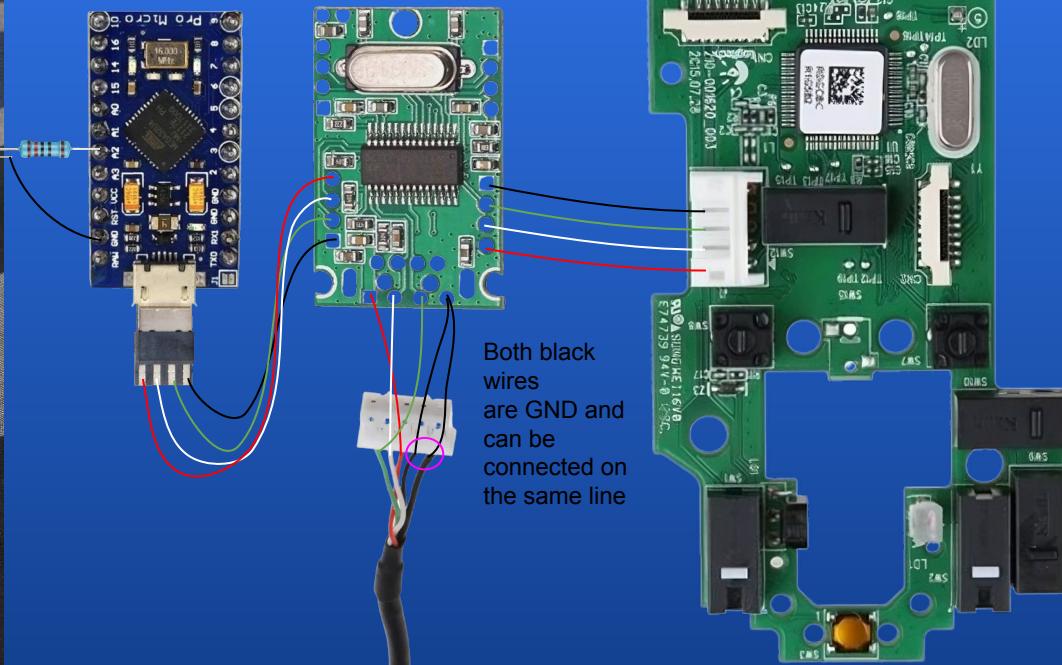
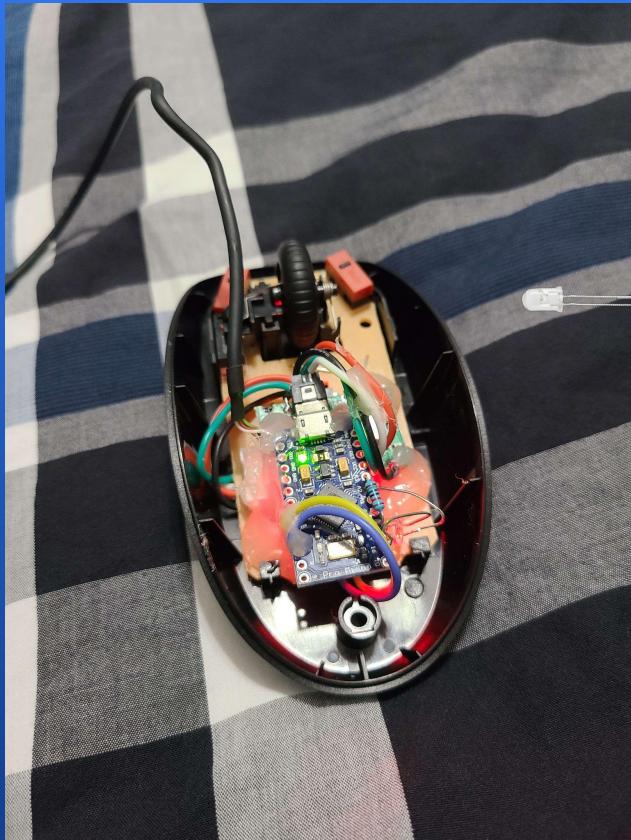
5mm Phototransistor



Micro USB
Solderable Plug
(or spliced
phone cable)

Along with basic soldering skills and some patience!

Wiring



Want to try it yourself? Check it out
on my Github!



<https://github.com/BhawksGit/Smart-BadUSB>

Thanks for listening!