bad USBs are scary!!

(build one with a Raspberry Pi Pico for ₹ 349)

by Nil K

the demo

the next 30 minutes

1

the demo

- reverse shell,
- prank video

2

working

- HID devices,
- keystroke injections,
- Wi-Fi Duck

3

DIY

- Adafruit Circuit Python,
- HID lib folder,
- automation

4

protect

- how to defend

5

blue team

- HID info detection,
- mass storage quarantine
- news articles

what do you need?

USB Rubber Ducky (Hak5) (₹6,919.58)

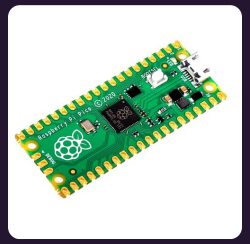
the original Rubber Ducky everyone knows about:

- Ducky Script
- USB A/C connectivity

USB Nova (Spacehuhn) (₹4,149.84)

like USB Rubber Ducky, plus:

- Drag and drop scripts
- Easy attack/setup mode switching
- Supports multiple keyboard layouts



Raspberry Pi Pico (₹349)

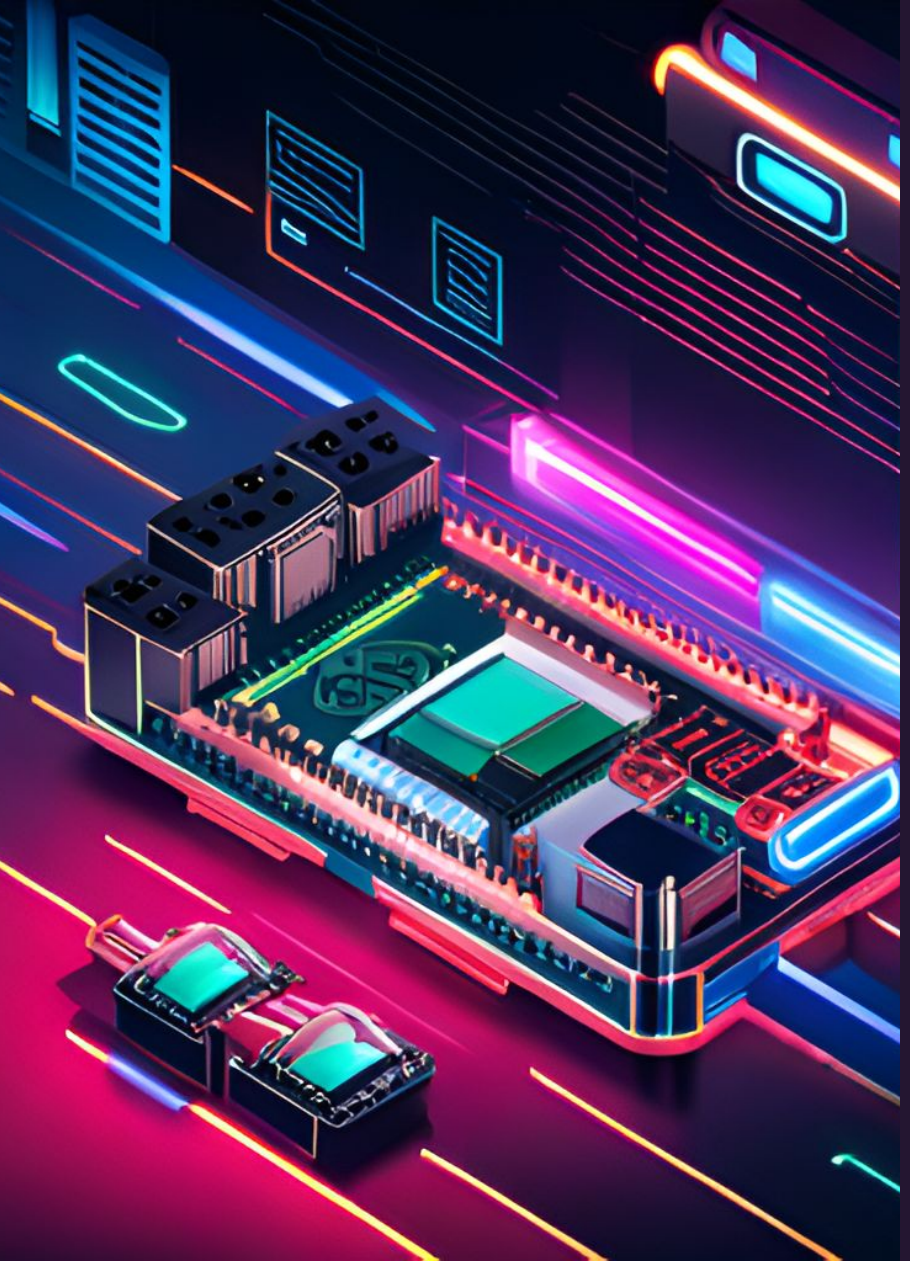
micro controller board by Raspberry Pi:

- RP2040 chip
- 97% cheaper
- drag-drop programming using mass storage over USB

how does it work?

1. it's recognised as an HID device(0×03), which is trusted by default

2. it can type up to 1000 wpm, faster than any human



building it yourself

1 gh clone dbisu/pico-ducky

navigate to github.com/dbisu/pico-ducky and follow README.md,

2 move files around

or, write at a script to automate this part & save time,

3 don't waste time

utilise this newly saved time by reading a book - The Ministry for the Future.

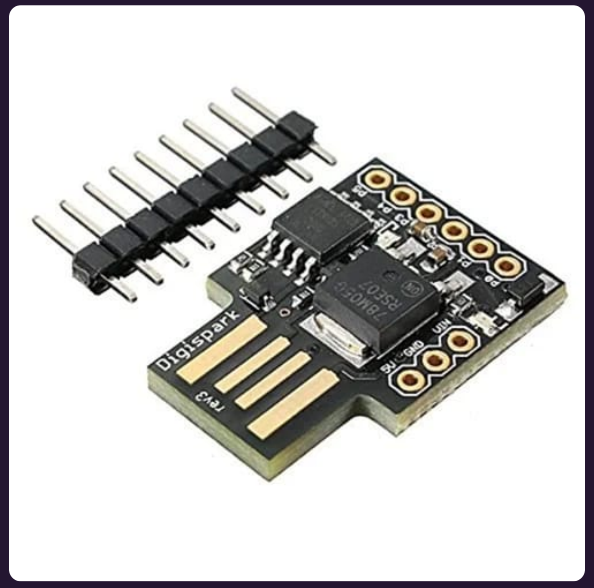
creating attacks

- https://github.com/hak5/usbrubberducky-payloads/tree/master is the official repository for verified payloads, BUT
- you can find scripts from random people on the internet as well, obviously do NOT run as it is.
- ask LLM models like ChatGPT to understand or write Ducky Scripts

Mr Robot (2015)

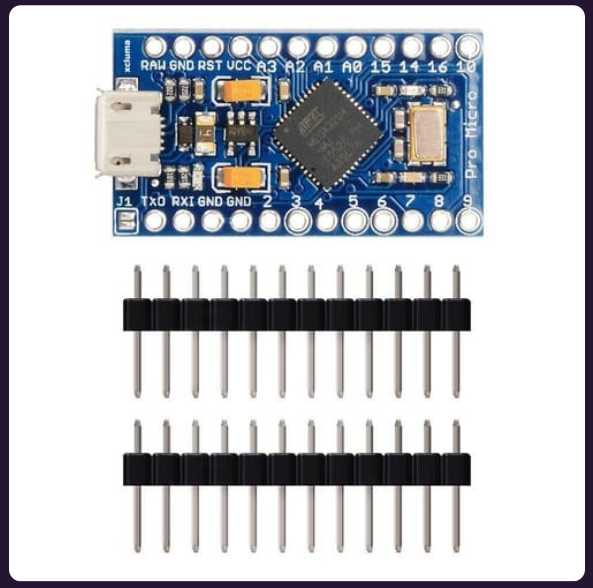
If you're a fan of the TV show Mr Robot, you might remember when Rubber Ducky was featured on the show.

alternative micro-controllers



Attiny85

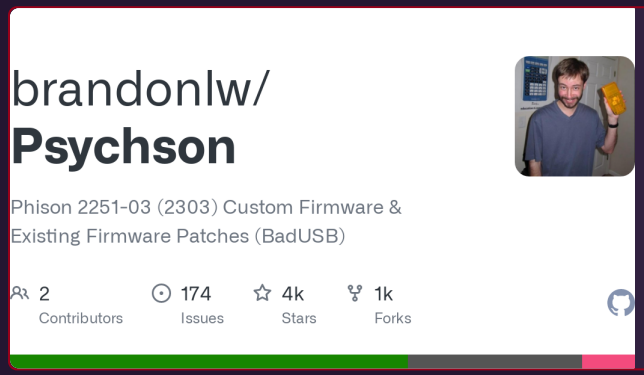
stealing Wi-Fi passwords in seconds - link



Atmega 32u4

brute-forcing the android/iPhone PIN - link

reprogramming a USB flash drive



GitHub

GitHub - brandonlw/Psychson: Phison 2251-03 (2303)...

Phison 2251-03 (2303) Custom Firmware & Existing Firmware Patches (BadUSB) - GitHub - brandonlw/Psychson: Phison 2251...

how do you protect yourself?

don't plugin unknown hardware

NEVER plug in an unknown device. ALWAYS use an isolated environment.

Win + L always!

NEVER step away from your computer without locking it first.

ZDNET

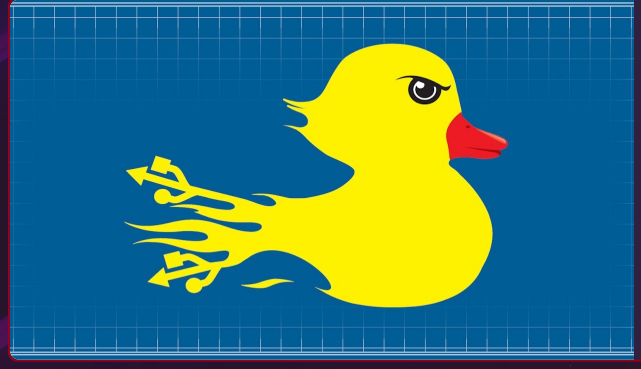
Criminals push malware by 'losing' USB sticks in parkin...

Here's a case of corporate espionage you've probably never heard before: infiltrating a corporation by "losing" malware-infected US...

Super User

How do I safely investigate a USB stick found in the...

I work at an embedded software company. This morning I found a USB stick in the parking lot in front of the building. With all the...



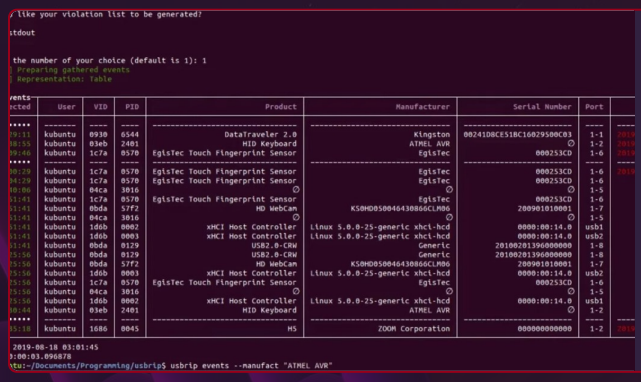
Digital Guardian

Detecting a Rubber Ducky USB Attack with Digital...

Our latest video demonstrates how Digital Guardian Advanced Threat Protection can detect and block a Rubber Ducky USB...

Explorer. Hacker. Nerd.

Blocking USB Rubber Ducky Attacks



WonderHowTo

Look for USB Rubber Ducky Attacks on Your Computer...

If left unattended, a hacker with a USB Rubber Ducky and physical access to the computer can infiltrate even the most secure...

new ducky 2022

DuckyScript 3.0

extension functions(like libraries) to build with, and create more creative attacks,

keystroke reflection[1]

data is gathered using keystroke injection, encoded into CAPS LOCK/NUM LOCK combos, which is read by Ducky

hardware id cloning

mimic any USB device's vendor & product id, as well as manufacturer, serial number and product strings

Listen Up, Blue Team!

1

trust but verify

before you plug in your device, make sure it's malware-free! use a disk image tool to make a copy of your hard drive, and check it against the original. don't risk infecting your computer with malicious code.

2

use firewall

use a firewall to control what programs access your network and the internet. create rules to block malware and keep company systems safe.

3

enable password authentication for administrative access

setup group policies by enabling password authentication for administrative access. it's a simple way to protect your sensitive data from unauthorised access.

what did we learn?

- bad USB attacks have crazy potential, but you can protect yourself.
- building a rubber ducky alternative is cost-effective, highly educational, and extremely customizable.
- cucumbers in fruit salad are heaven on earth

/nileshevrywhr

the answer to your questions?

“ask and it will be given to you" (Matthew 7:7)