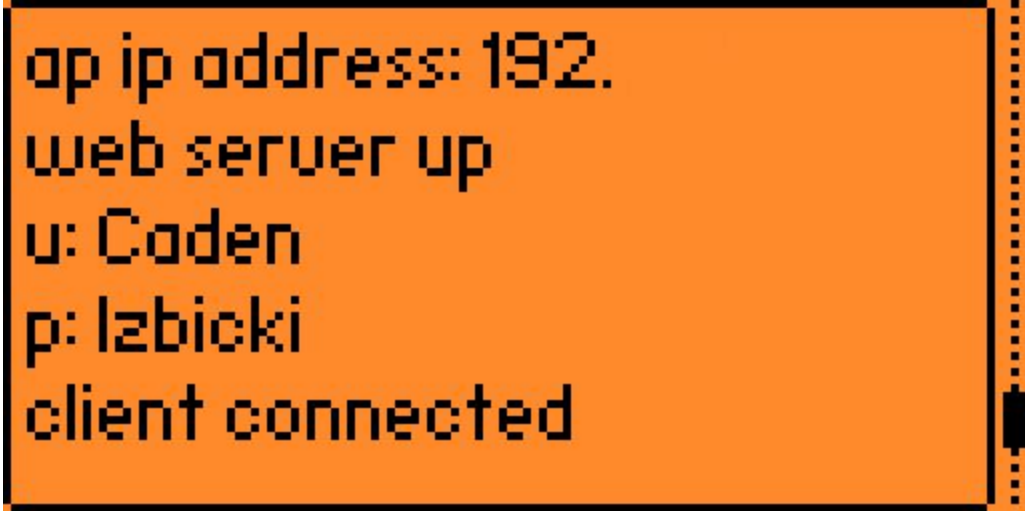# Evil Portal

Caden Izbicki

What is an Evil Portal

- An Evil Portal hack refers to a type of phishing attack involving the creation of a fake or malicious Wi-Fi network.
- In a Evil Portal hack, attackers will set up a rogue Wi-Fi networks or manipulate an existing public Wi-Fi network's settings to redirect users to a malicious captive portal. This can happen when users unknowingly connect to the rogue hotspot, thinking it's a legitimate network.

How are credentials stolen?

- Phishing Portal: The attacker sets up a fake captive portal that closely mimics the login page of a legitimate website, such as a social media platform or an email provider. When users try to log in, they enter their credentials into the fake portal allowing the attacker to see all information in clear text.

The Flipper Zero

- What's a Flipper Zero? The Flipper Zero is a handheld Pentesting tool with many tools built in such as Sub-GHz, NFC, Bad usb and tons of community made apps.
- The Flipper Zero also uses a Wifi Dev board which allows me to enable wifi and Wireless based attacks such as the one I will be demonstrating today
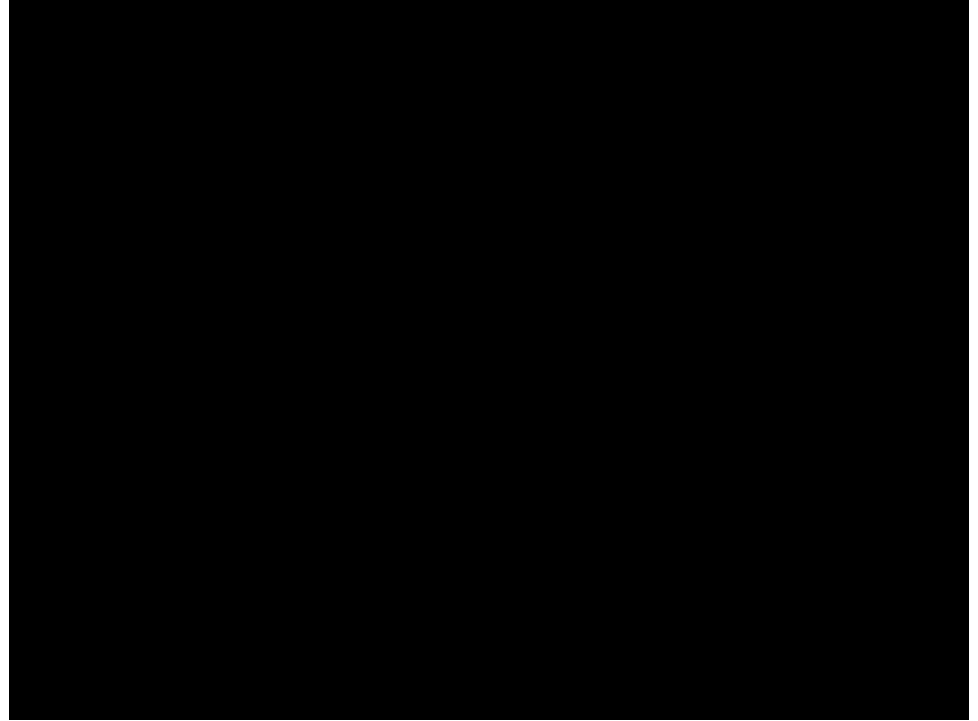
Why I picked this project

- I picked this project to show how fast and easy it is to set up a fake wifi networks with the flipper zero.
- Another reason i picked this project is to bring better awareness to unsecure public wifi network.

Demonstration

https://youtu.be/kotBjlvcGSs

What Happened?

- When user connects to the wifi network a portal for a cox login page opens automatically.
- From there when then user enters their login credentials
- The credentials are sent in clear text because the portal website uses http and is saved to a log directly on the flipper zero

Demo log

html set: Sets the false portal to the Cox login page

ap set: Sets the access point name from a file

starting ap: Starts the access point named NexusL

ap ip address: Shows selected Access point ip address

u: Is the username the stolen credentials

p: Is the password the stolen credentials

```
html set
ap set
all set
starting ap NexusL
ap ip address: 192.
web server up
u: caden
p: izbicki
client connected
```

Mitigating risk

- Whenever possible, use networks you trust, such as those provided by reputable establishments like hotels, coffee shops, and airports.
- Be cautious about sharing sensitive information, such as passwords or credit card details, while connected to public Wi-Fi networks.
- Vpn
- Overall it's best not to connect to public wifi at all if possible.

Rickroll attack