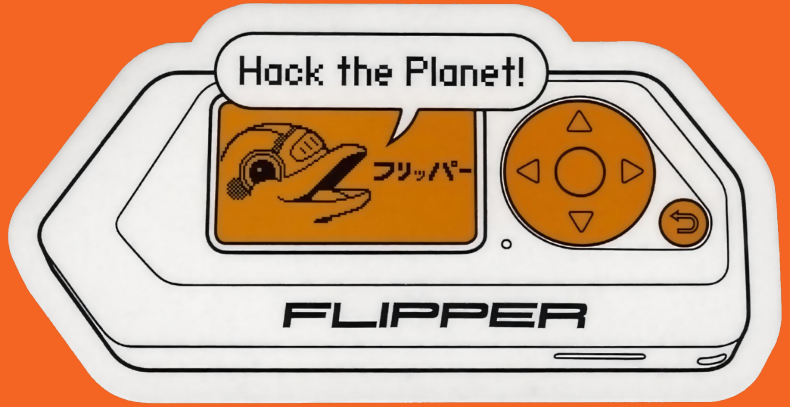
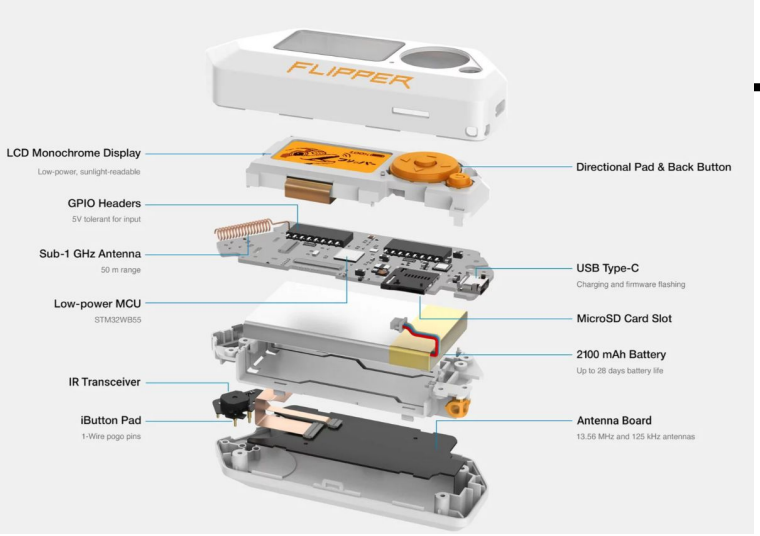
Flipper Zero - Evil Portal Attack



By: Chris, Jordan, Joseph, and Seth



What is the Flipper Zero?

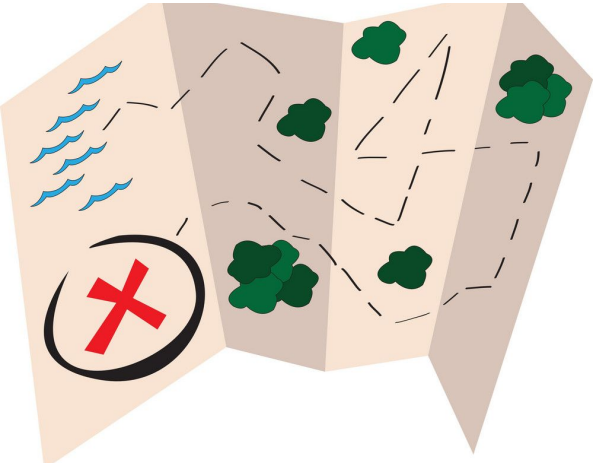
- The Flipper Zero is a “hacker’s pocket knife”, a multi-tool device for the digital world.
- It’s capabilities are extensive and can be used to hack radio protocols, access control systems, hardware and much more.

Why did we choose the Flipper Zero?

- We all agreed that it seemed fun, easy to learn, and something we could learn from.
- Learning what the Flipper can do increased our awareness and will help us be more careful with our devices in public.

Flipper Zero Capabilities

- The Flipper can learn and transmit infrared signals. For example, it can learn the signals used for radios, TV remotes, and printers and have control over them. It can also be able to learn the radio signals of a garage door opener, so that would be a big vulnerability if compromised.
- It can write and emit 125 kHz RFID, or Radio-frequency Identification, which would mean it can copy the low frequencies given from access cards for the office. It can also copy high frequency proximity cards using a built-in NFC (near field communication) module, allowing it to be used in contactless payments of the cards it copied.
- A big thing that stood out to all of us is that the Flipper Zero can create fake wifi access portals to have people “login”, but once they do, the Flipper stores a log showing the credentials it just captured, and the user will be able to do whatever they want with them. This can be done anywhere such as cafes and hotels.



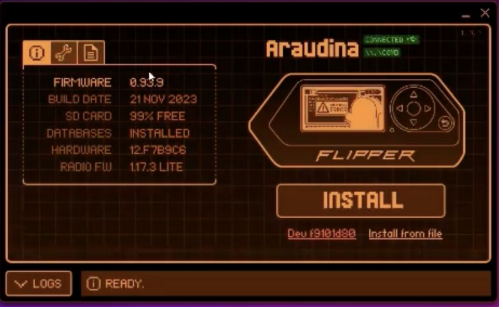
Research Steps Taken

1. We started our research on the official Flipper Zero website and discovered what it is and what the capabilities are.
2. We searched the kinds of attacks it can take place in and saw a couple of videos describing the wifi access point credential farming called “Evil Portal”.
3. We went over the importance of only doing this kind of thing on our own devices and would be for educational purposes since using the Flipper in public can be seen as an illegal action.
4. We’ve managed to have one of us get their hands on an actual Flipper Zero so that we could practice creating fake wifi hotspots ourselves on our own devices using those tutorials.
5. Demonstration and Summary!

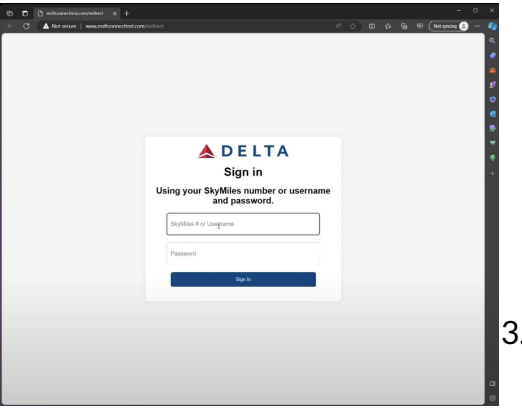
Demo preview

- Joseph the attacker is going to be demonstrating how to steal user credentials with Evil Portal on the Flipper Zero.
- The firmware and setup process is all done through open source. Once the Dev board and the flipper have been setup.
- Joseph will create a fake wifi hotspot that will display an HTML page and can start capturing user credentials with the flipper zero.
- Using an HTML login page, we can display a Google login page or a Delta Airlines login page that is identical to the actual site login page; the possibilities are endless.

Demo



Demo Summary



1. After downloading all of the firmware and setting up the flipper. By plugging in the wifi dev board and navigating to the Evil Portal, click on the start portal which the light turns blue to green and that's how we know its working. After clicking the start portal it will display pur HTML trap.
2. Go to set AP Name/SSID. Where we decide the name for our counterfeit wifi hotspot that will display for people to see on their devices. Select the HTML such as Delta Airlines, Amazon etc. Click Start Portal which starts the HTML trap. Go to our wifi settings on our computer/smart phone and connect to the counterfeit wifi hotspot. The HTML will pop up as “Delta Airlines”. Once we type the username and password our credentials immediately displyas to the Flipper and saves as logs.
3. We go to the qFlipper and click “Stop portal” which stops it from running. We select “Save logs” for the logs to save and then we go to sd card/app_data/evil_portal/logs and then download the log(s) on the computer. Open it the logs on our desktop via notepad or text editor and scrolled until we see the username/password or credentials that we type inWe

Mitigations

- Always be very cautious and skeptical with unsecure wifi and don't be quick to trust them.
- Do not join any unsecure wifi hotspot anywhere especially public places such as airport, starbucks, hotels, gyms, etc.
- Do not type in your username and password.
- Don't hesitate to ask any personnel which wifi hotspot is theirs.
- Use a VPN
- Use HTTPS
- Restrict WiFi access/Disable Auto Connect
- Pick A Secure Network-(if available)
- Create A Secure Ssid


OH MY GOD!
Thank you!
oUqF7sz!
%9.mP5H

Works Cited

Github link to flipper zero software

Flipper Zero Official Website

Video 1 of Tutorial for Fake Wifi

Video 2 of Tutorial for Fake Wifi