PENNSYLVANIA CRIMINAL INTELLIGENCE CENTER

Information Bulletin

CIKR 08-2023 April 20, 2023

(U) FLIPPER ZERO PENETRATION TESTING DEVICE

(U) SCOPE

(U//FOUO) The Pennsylvania Criminal Intelligence Center (PaCIC) is providing this Information Bulletin to alert critical infrastructure owners and operators of the potential for adversaries to exploit vulnerabilities in access control systems using digital hacking tools. This bulletin will support the development of protective measures to identify and mitigate potential threats to infrastructure and assets.

(U) OVERVIEW

(U//FOUO) The PaCIC has observed increased interest in low power, handheld digital hacking tools across clear web and dark web sources. The PaCIC is providing this bulletin for situational awareness of an increased interest specifically in the Flipper Zero device, a digital hacking and penetration testing tool capable of scanning nearby radio signals, copying signal data, writing captured data to a secondary device, and/or broadcasting the data to a suitable receiver. The device can be used to activate access control systems, to include some security gates, garage doors, and other keyless entry systems. The device can also be used to initiate keystroke injection attacks against vulnerable systems.

FLIPPER ZERO DEVICE

(U//FOUO) Flipper Zero is an example of a commercially available hacking device with an active user base that is constantly expanding its capabilities. The presence of a Flipper Zero device does not alone indicate criminal or nefarious activity. However, as the device becomes increasingly popular, additional modules and programming tutorials will likely decrease the level of sophistication necessary to operate the device. This has the potential to lead to increased use of Flipper Zero devices to facilitate trespass, theft, and other crimes of opportunity.

(U) DEVICE AND CAPABILITIES

(U//FOUO) Flipper Zero is a multi-function hacking device that supports common wireless communication protocols typically used to interact with various access control systems. The device is 4” by 1.5” in size. It is controlled with a five-position directional pad and a separate back button. The screen is a monochrome liquid crystal display (LCD) with an orange backlight. The device’s menu structure includes various images of a dolphin, bearing a resemblance to a Tamagotchi toy. The device includes the following onboard wired and wireless communication protocols:

- Near Field Communication (NFC) – access control systems, payment transactions, keycards

PENNSYLVANIA CRIMINAL INTELLIGENCE CENTER sp-protectpa@pa.gov

Pennsylvania State Police • Bureau of Criminal Investigation • Intelligence Division (855) 772-7768 • FAX: (717) 772-6917

Thank you for taking the time to provide feedback. It is important in helping us improve our products and services.

CLICK HERE FOR PACIC CUSTOMER SURVEY

- Radio Frequency Identification (RFID) – access control systems
- Infrared (IR) port – television remote controls, laptops, and tablets
- Bluetooth Low Energy (BLE) – proximity communication with other BLE devices
- General purpose input/output (GPIO) pins – wired communication protocols and expansion modules
- External micro-SD card slot – storage for data, applications, firmware, and operating system updates
- USB-C – charging and interfacing with a computer

(U//FOUO) NFC, RFID, and IR communication protocols are routinely used for commercial and residential access control systems designed to secure sensitive areas. Open-source forums have plausibly demonstrated Flipper Zero devices activating security gates, including those which provide perimeter security barriers to critical infrastructure, certain vehicles' remote keyless entry systems, and residential buildings which rely on RFID keycards. Facilities utilizing keycard access with a PIN remain at a lower risk unless the PIN has also been compromised.

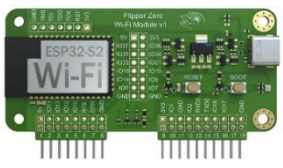
RFID READER

(U//FOUO) As a network defense strategy, many organizations disable USB autorun functionality on systems connected to their computer network to prevent USB devices from automatically executing a malware payload. To circumvent this, adversaries have developed keystroke injection attacks, such as the "badUSB" attack, in which a USB-based microcontroller is disguised as a flash drive. Upon connection to a system, the badUSB device identifies as a human interface device (HID), most commonly as a keyboard, and sends preconfigured keystrokes and commands to the targeted system. A Flipper Zero device can deploy a badUSB attack against a vulnerable computer system. BadUSB payloads are written to a .txt file in Rubber Ducky script syntax, and are executed by the Flipper Zero device. Activity on a popular software development website provided links to a repository containing a collection of preprogramed badUSB payloads to be deployed from a Flipper Zero. The files referenced common attack methods, to include keylogging, ransomware, phishing, data exfiltration, data destruction, network reconnaissance, and remote access.

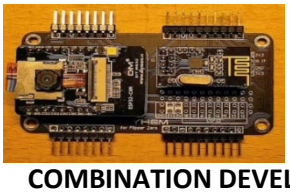
OPTICOM DEVICE

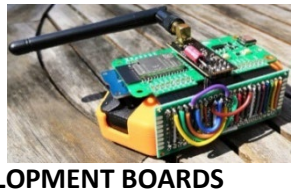
(U//FOUO) Public forums have plausibly demonstrated Flipper Zero devices activating some traffic signal preemption (TSP) devices. Mobile infrared transmitter (MIRT) devices are routinely used by emergency responders and fire departments to operate TSP devices to allow emergency vehicles to safely pass through an intersection. The pictured Opticom receiver, which is typically mounted on a traffic light pole, is an example of a TSP. During a test, a Flipper Zero was interfaced to a MIRT to activate emergency lights at roadway intersections.[1]

(U//FOUO) Flipper Zero provides the device's GPIO pinout and functionality information on their website, allowing developers to easily design new modules. Flipper Zero users continue to develop external expansion modules and development boards that utilize the device's GPIO pins. Expansion boards provide additional functionality, to include additional wireless protocols and increased transmitter distances. Online stores for printed circuit boards (PCBs) have assisted users in designing, prototyping and assembling new modules. Users on public forums have demonstrated custom Wi-Fi modules, camera modules, and additional wireless communication modules.



WIFI EXPANSION BOARDS





COMBINATION DEVELOPMENT BOARDS

PENNSYLVANIA CRIMINAL INTELLIGENCE CENTER sp-protectpa@pa.gov

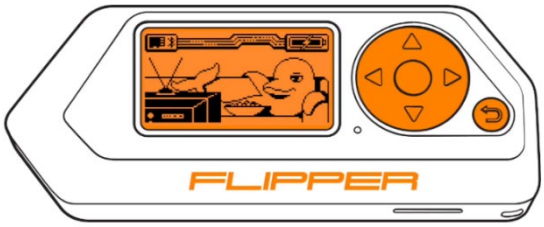
Pennsylvania State Police • Bureau of Criminal Investigation • Intelligence Division (855) 772-7768 • FAX: (717) 772-6917

Thank you for taking the time to provide feedback. It is important in helping us improve our products and services.
CLICK HERE FOR PACIC CUSTOMER SURVEY

(U) OPERATION AND MENUS

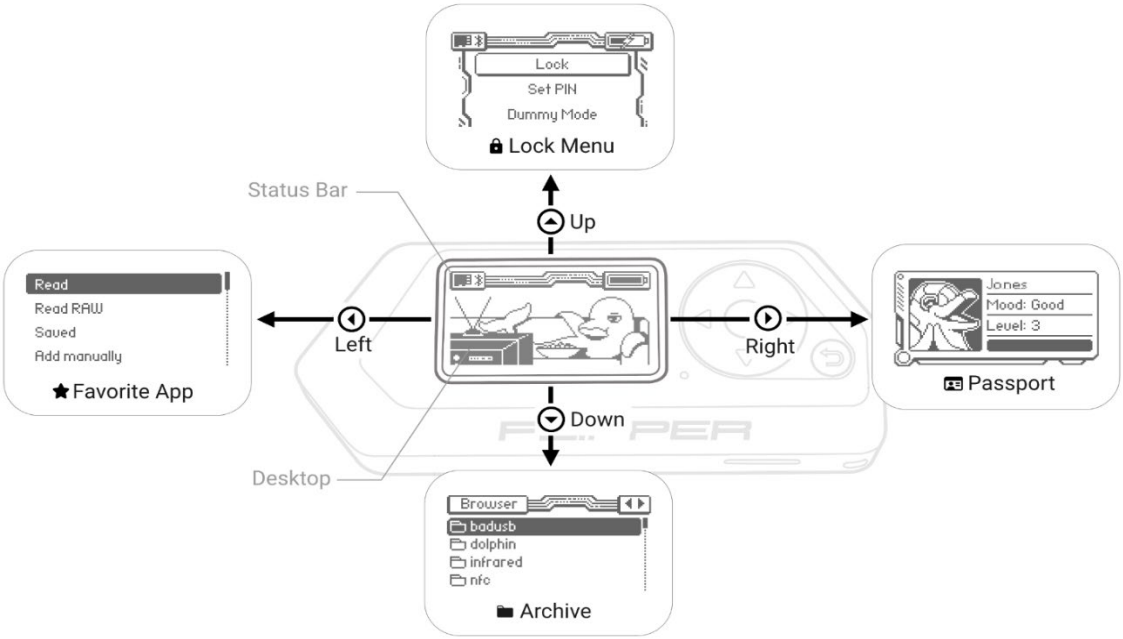
(U//FOUO) Operation of the device relies on a five-position direction pad (up, down, left, right, center buttons), and a separate back button. To power on the device, press and hold the back button until the unit displays the pictured home screen.[2] A user has the ability to lock a device using a PIN. To unlock a locked device, press the back button three times. From the device's desktop screen:

UP - The Lock menu: Lock the buttons, protect the device with a PIN code.
LEFT - Launch the Favorite app.
RIGHT - Dolphin passport, shows your dolphin's name, mood, and level.
DOWN - Archive with saved keys and remotes.
BACK – Return to the previous screen



FLIPPER ZERO HOME SCREEN AND

The Archive menu will show currently installed applications. Application names can be modified by the user, so the displayed filename may not provide an accurate description of the application's purpose.



(U) RECOMMENDATIONS

(U//FOUO) The PaCIC is providing this bulletin for informational and situational awareness purposes only. Critical infrastructure owners and operators are reminded to remain vigilant to detect suspicious activity targeting access control systems and vulnerable computer networks. The United States Department of Homeland Security (DHS) provides additional guidance on suspicious activity reporting indicators and behaviors.

(U//FOUO) In the event of a physical breach or cyber incident, owners and operators should contact law enforcement immediately. Suspicious activity should be reported to local law enforcement and the PaCIC CIKR Unit at sp-protectpa@pa.gov or (855)-772-7768.

Thank you for taking the time to provide feedback. It is important in helping us improve our products and services.
CLICK HERE FOR PACIC CUSTOMER SURVEY

The information used in this bulletin is drawn from open sources, DHS open source reporting, FBI and other law enforcement intelligence reports and court filings. The Pennsylvania State Police (PSP) has high confidence in the information obtained from court documents and those of government agencies. The PSP has medium confidence in the information obtained from open sources, which includes media reports and Internet websites whose information is credibly sourced and plausible but may contain biases or unintentional inaccuracies. When possible, open source information has been corroborated through other law enforcement and government sources.

CUSTOMER FEEDBACK

To assist in improving our production and dissemination processes, please provide feedback of this product by completing an online customer survey. A link to the survey can be found at the bottom of this page. This will allow us to ensure that our customers continue to receive valuable, relevant information in a timely manner.

---

[1] Stumpf, R. (2023, February 16). Hacker Uncovers How to Turn Traffic Lights Green With Flipper Zero. *TheDrive.* Retrieved on 02/17/2023 from https://www.thedrive.com/news/hacker-uncovers-how-to-turn-traffic-lights-green-with-flipper-zero.

[2] Control. (n.d.) *FlipperZero.one.* Retrieved on 02/17/2023 from https://docs.flipperzero.one/basics/control.

PENNSYLVANIA CRIMINAL INTELLIGENCE CENTER **sp-protectpa@pa.gov**

Pennsylvania State Police • Bureau of Criminal Investigation • Intelligence Division (855) 772-7768 • FAX: (717) 772-6917

Thank you for taking the time to provide feedback. It is important in helping us improve our products and services.

CLICK HERE FOR PACIC CUSTOMER SURVEY