RubberNugget

🐦 **WiFi_Nugget** 🔗 **wifinugget.com**

About the RubberNugget

Thank you for buying a HakCat RubberNugget! Your purchase helps us continue to develop open-source products and free educational content for the hacker + maker community.

The RubberNugget is a cat-shaped USB attack tool that deploys keystroke injection payloads in seconds. Use the on-screen interface to monitor the status of your attacks! Features of the RubberNugget include:

📱 Remote attacks from any web browser

👾 Custom cat graphics + reactive LED feedback

💾 Built-in flash drive for data exfiltration

⌨ Quick 3-click payload selection system

RubberNugget Payloads

The RubberNugget is powered by DuckyScript and supports existing RubberDucky and BashBunny payloads! You can find official payloads & commands in our Hak5 GitHub repo.

Docs / Payloads: github.com/Hak5/RubberNugget-Payloads

Using the RubberNugget

ℹ **Make sure your Nugget is up to date by flashing the latest firmware at flash.wifinugget.com**

Plug in your RubberNugget and upload payloads over USB. Payloads must end in .txt and be uploaded under an OS / Category subfolder. Run up to 36 payloads in 3 clicks using the Nugget screen + buttons!

```
        📁 Linux ──── 📁 Recon ──── 📄 Payload1.txt
 ⌁ ┬── 📁 Mac        📁 Phishing     📄 Payload2.txt
USB └── 📁 Windows    📁 Backdoor     📄 Payload3.txt
```

Web Interface

Use the RubberNugget Web UI to create, edit, and deploy payloads over WiFi! To get started:
- Connect to the **RubberNugget** AP with password **nugget123**
- Open **192.168.4.1** in a web browser

Development & More

- To report bugs, create an issue on our code repo at: **github.com/HakCat-Tech/RubberNugget**.
- For more docs + info check out **docs.wifinugget.com**

Hardware: v2.1-Dev **Color:** Purple
Software: v1.0-beta

A product by **HakCat.com**