USB Rubber Ducky info and demo

**Contents**

1. Introduction

2. How to work with Rubber Ducky

2.1 Developing model

2.2 Using model

3.How to change its function,payload and attack

3.1 System/environment requirement

3.2 Files requirement

3.3 Refreshing firmware

3.4 Changing payload

4. Code example and demo

4.1 Ducky code principle

4.2 Demo

1. Introduction

The USB Rubber is a **keystroke injection** tool disguised as a generic flash disk/drive. It’s also called “Bad USB”. A computer recognizes it as a regular keyboard and accepts its pre-programmed keystroke **payloads** at over 1000 words per minute. Nearly every computer including desktops, laptops, tablets and smartphones takes input from users via Keyboard. That’s why there’s a specification with the ubiquitous USB stand known as **HID**. Rubber Ducky claims to be a HID, thus will automatically be detected as a keyboard. On any OS Windows, Mac, Linuxs or Android, the keyboard is recognized.

Some explanations:

**Keystroke injection**: Using a simple scripting language to record keyboard buttons.

**HID**: Human-computer Interface Device.Such as Keyboard, Mouse, Bluetooth speaker, etc.

**Payload**:Payloads are crafted using a scripting language and can be used to drop reverse shells,inject binaries, brute force pin codes and many other automated functions for the penetration tester and system administrator.

2. How to work with Rubber Ducky

First, let’s observe its structure.

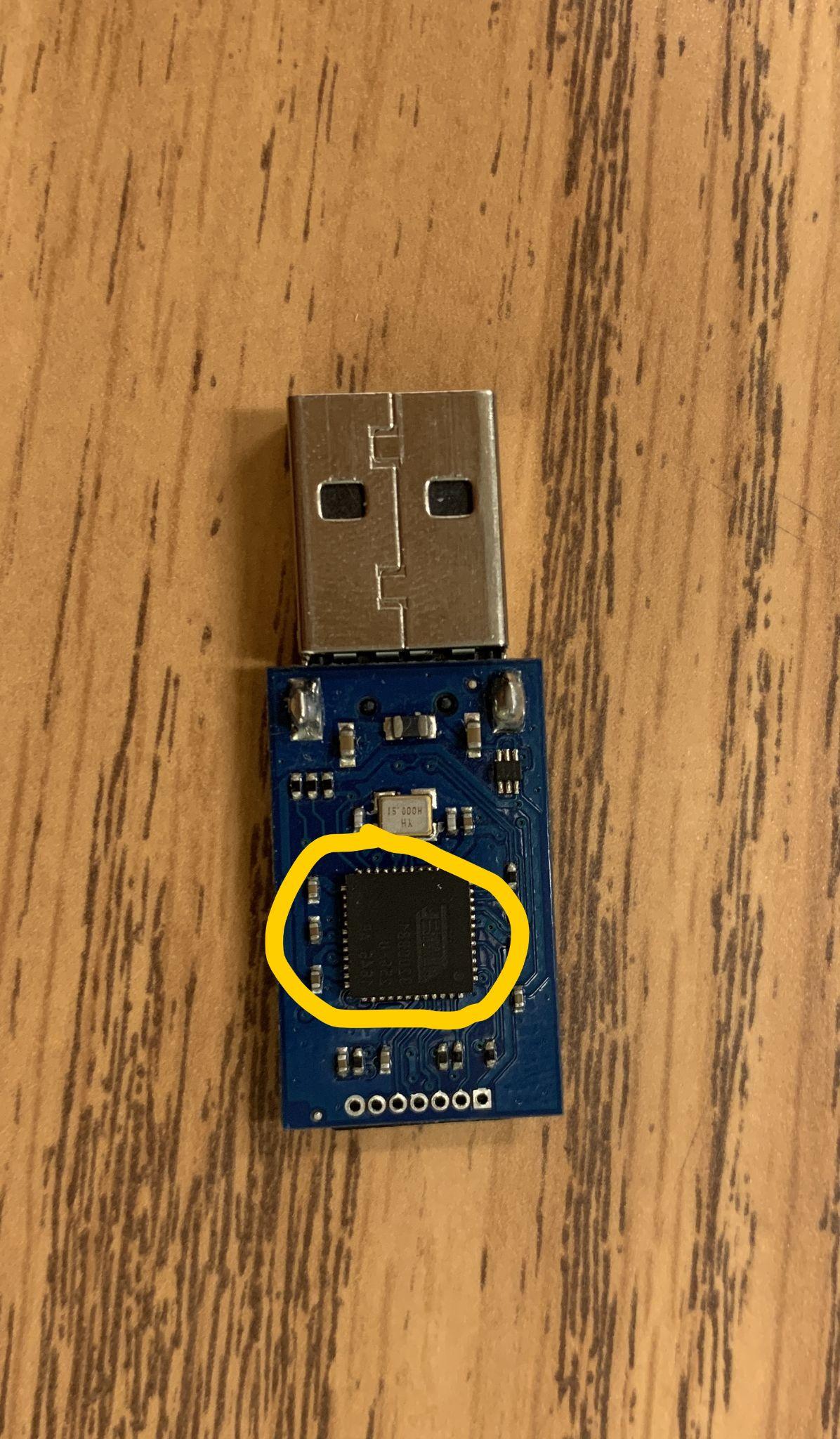


Figure1 : Front of Rubber Ducky . Figure2: Back of Rubber Ducky

Red circle: Memory disk.

Blue circle: Tiny button.

Green circle: Working light.

Yellow circle: Firmware.

2.1 Developing model

Developing model is also called DFU model—Device Firmware Update mode. We should press the tiny button and plug in at the same time. Then, we cannot see the working light that is in the DFU model.

In this model, we can update the firmware to “twin ducky”. Also we can recover it to a normal USB disk.

**Notice: We cannot read its memory when its firmware is “ducky”. If we want to change its attack, we must recover it to a USB disk first.**

2.2 Using model

We only need to plug Rubber Ducky into a PC to test. If the working light is green, it is working; If the light is red, it does not work,so we need to check memory, or refresh firmware or redo this.

3.How to change its function, payload and attack

# 3.1 System/environment requirement

Although it can work under Windows, IOS, and Linux systems, as a developer, Linux is the most suitable for developing USB Rubber Ducky. We can install it on a Virtual Machine (with LInux iso).

Mostly, we use Command and download [dfu-programmer-0.5.4](https://sourceforge.net/projects/dfu-programmer/files/dfu-programmer/0.5.4/dfu-programmer-0.5.4.tar.gz/download?use_mirror=netcologne&r=http%3A%2F%2Fsourceforge.net%2Fprojects%2Fdfu-programmer%2F%3Fsource%3Ddlp&use_mirror=netcologne) in Linux. **Notice: There are reported problems with dfu programmer version 0.5.2.**

# 3.2 Files requirement

All files are in the Google drive folder. We only use “duck\_v2.hex” and “usb\_v2.hex” for changing attacks.

# 3.3 Refreshing firmware

In Linux, we should open Command and follow these step:

1. Dump your firmware:

sudo dfu-programmer at32uc3b1256 dump >dump.bin

1. Reset (once):

sudo dfu-programmer at32uc3b1256 reset

1. First erase ducky:

sudo dfu-programmer at32uc3b1256 erase

1. Update firmware:

sudo dfu-programmer at32uc3b1256 flash --suppress-bootloader-mem ducky-file.hex

1. Reset(second time):

sudo dfu-programmer at32uc3b1256 reset

# 3.4 Changing payload

We can follow these step on every system that has a command line:

Using ducky code to write a script in a txt file.

Normally, we put all files in the same folder and enter in Command:

java -jar "PATH to \duckencoder.jar" -i "PATH to \script.txt" -o "Path to \inject.bin "

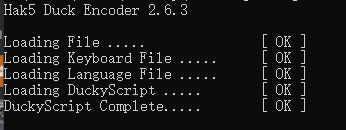
Example(for Windows):

java -jar E:\Documents\BadUSB\DuckEncoder\duckencode.jar

-i E:\Documents\Bad\_USB\DuckEncoder\script.txt

-o E:\Documents\Bad\_USB\DuckEncoder\inject.bin

We succeed when we see the following picture.



At last, put “inject.bin” file to your Rubber Ducky. Refresh it to Ducky firmware.

4.Code example and demo

# 4.1 Ducky code principle

GUI: Press “Windows” key. Always we need to add another key such as “GUI d” → show desktop.

DELAY: pause. time in milliseconds and the upper limit is 3000.

ENTER: Press “enter” key.

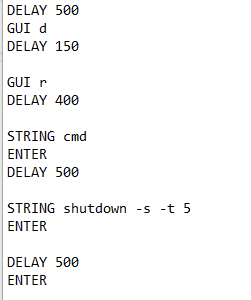
STRING: Typing what we want.

REM: Remark. Does not affect our code.

CTRL, ALT, TAB, SHIFT, etc ：One-to-one correspondence to the keys on the keyboard.

**Notic: All code words must be capitalized as shown above.**

# 4.2 Ducky code example

** Shutdown code for windows system.**