A USB Rubber Ducky Demo

Objective: As we know OS usually trusts devices connected to a USB interface. The purpose of this demo is to show you how attackers can exploit this trust to steal information from a PC.

Background:

- A USB is a universal interface which can connect many devices, e.g. mouses, keyboards, printers, scanners, web cameras, telephones, etc
- Once plug in a device, OS automatically determines the type of device and loads the required drivers
    - In fact, device tells the OS what kind of device it is (read USB device initialization algorithm for more details)
        - Class codes communication
            - USB flash drive will have class codes
                - e.g. Mass Storage Device (08h), a web camera with a microphone (01h for Audio, and 0Eh for Video Device)
        - When connected, the USB device is registered, receives an address and sends its descriptors
        - Then OS installs necessary drivers
        - Once the work is done, the device is de-registered

In our demo, USB thumb drive I use claims to be **a keyboard** and quickly enters all commands in the malicious payload.

Do you want to create your own? https://hackmag.com/security/rubber-ducky/