



# Rubber Ducky in Cybersecurity: Antivirus Deactivation / Data Extraction / Backdoor

PLARD Maël / VIVET Alice / FOURNET Alexandre / Inge2C

## CONTEXT

USB devices, like the Rubber Ducky, represent a double facet in cybersecurity: powerful tools for security professionals and potential weapons for cybercriminals. The Rubber Ducky looks like an ordinary USB stick, but acts as an automatic keyboard capable of executing scripts at unrivalled speed. This tool is commonly used in penetration tests to assess the robustness of IT security systems.

The aim of this project is to demonstrate how a Rubber Ducky can be used to disable antivirus software and extract sensitive data to an FTP server and how it can create backdoors in a Windows computer. By simulating this attack, we are exploring not only the capabilities of this tool, but also the vulnerabilities of modern security systems. This project highlights the risks associated with USB devices and underlines the importance of robust defense measures against such threats.

## Which tools have we used ?

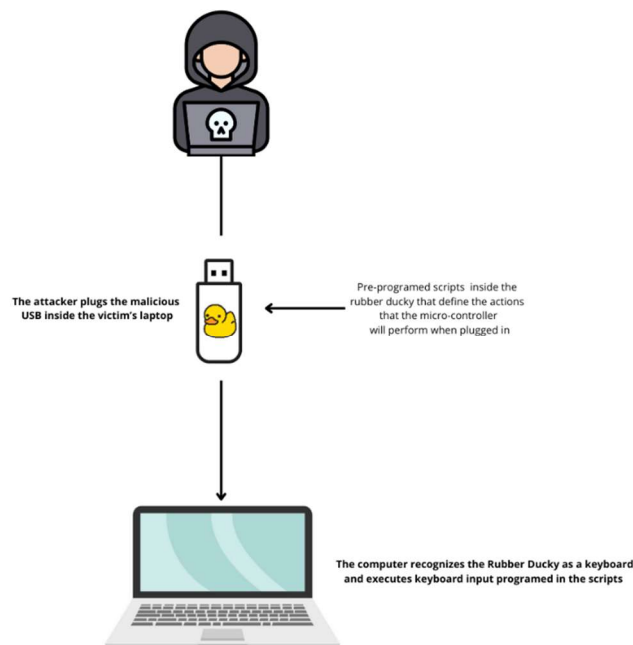


**Raspberry Pi 4B (Basic hardware):** The Raspberry Pi acts as the hardware platform on which CircuitPython is installed. Why a Raspberry pi 4 ? Because it offers superior performance, capable of handling heavier tasks and running several processes simultaneously without slowing down. Ethernet connection options offer greater flexibility for connecting additional peripherals and components, with the possibility to make a Rubber Ducky through Ethernet port.



**CircuitPython (Programming language):** CircuitPython is used to write scripts that emulate keyboard behavior. The adafruit library provides a custom keyboard layout that associates ASCII and higher ASCII characters with USB HID key codes.

## Course of a rubber ducky attack








## In our first case we attempt to exfiltrate data :

- 1  Deactivate the antivirus by navigating into the victim's settings
- 2  Open a terminal with administrator privileges to be able to create critical files copies
- 3  Export the registry hives SAM, SYSTEM, and SECURITY in the temporary files of the victim's system. Those hives are present on every Windows computers and contain users' credentials (username + hashed password)
- 4  Transfer data to a distant FTP server hosted in a Windows 11 Virtual Box
- 5  Remove the traces by deleting the registry hives copies

## Results

The use of our rubber ducky on a poorly protected windows computer enabled us to obtain sensitive files from a remote server. Using tools such as hashcat or john the ripper on these hives registries can enable us to retrieve the cleartext passwords of various users. On the other hand, the simple fact of obtaining password hashes raises security concerns. Indeed, using the "pass-the-hash" method can enable us to authenticate on a Windows server, for example. Moreover, we have been able to connect remotely to a computer, after plugging the rubber ducky into a victim's device and get access to sensitive data.

## In our second case we attempt to create a backdoor :

- 1  Open a terminal with administrator privileges to be able to modify the registries
- 2  Add a user account that will grant us access to a remote desktop
- 3  Add this user to local administrators group to get all necessary privileges
- 4  Add a rule to the firewall settings which allows us to connect to our remote user from any device
- 5  Disable UAC remote restrictions and hide our user account

## CONCLUSION

This project demonstrated the effectiveness and flexibility of using CircuitPython on a Raspberry Pi to emulate a Rubber Ducky USB. By harnessing the power of the Raspberry Pi 4, we were able to disable an antivirus and extract sensitive data to an FTP server automatically and quickly, as well as place a backdoor in a Windows computer. This project highlights the importance of ongoing cybersecurity training and constant vigilance in the face of new threats. We encourage security professionals to adopt rigorous security practices and share their knowledge to strengthen the collective defense against cyberattacks.