



En cybersécurité aussi, le savoir n'a de valeur
que si il est partagé.

In Cybersecurity too, knowledge only
increases in value once shared.

Bad USB presentation

Disclaimer

Disclaimer

The following demonstration is for educational purposes only.

We do not promote or encourage illegal activities.

Knowing your enemy is a half-won battle

La connaissance n'est réellement profitable que lorsqu'elle est partagée

What is Bad USB?

- Like a normal USB key
- When plugged in, performs predefined action
- Can be the source of a compromise if not monitored closely
- PlugX malware was distributed in a campaign through badUSBs



Malduino, from Maltronics

Why does it work?

- Peripherals announce their type when connected
- The computer has no choice but to **trust** them

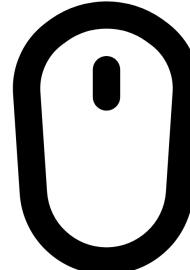
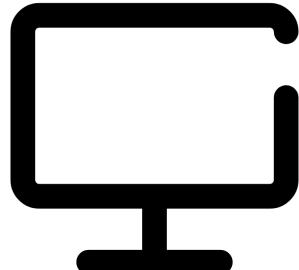
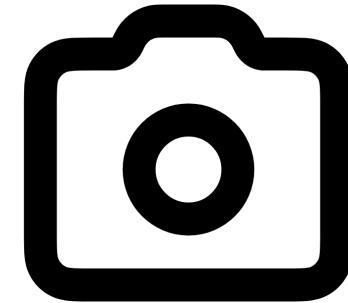
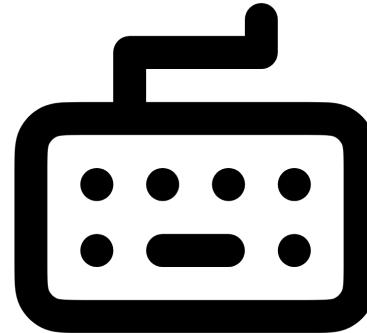
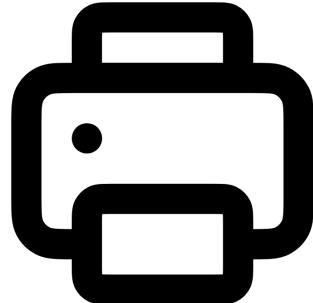
In cybersecurity, **hardware and the human factor** are the **MOST VULNERABLE** parts.

Combining them, a user plugging an USB key is a **deadly method**



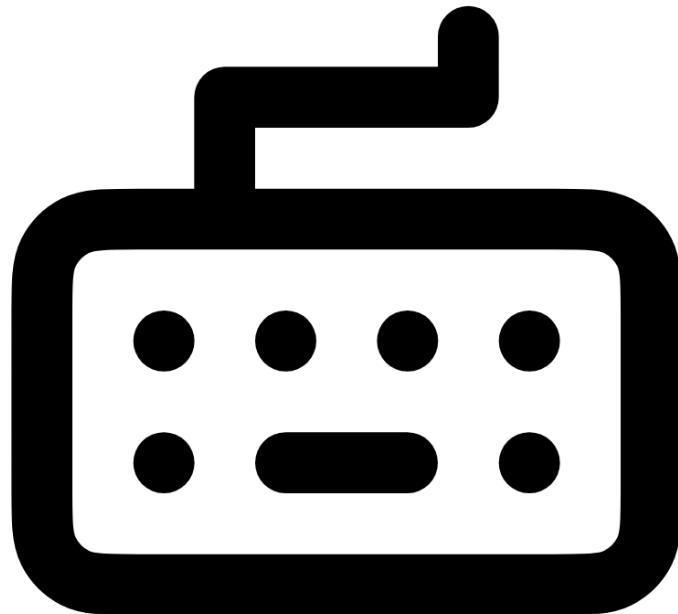
Rubber ducky

How it's being exploited



Which peripheral
should the badUSB
pretend to be?

How it's being exploited



**A keyboard
enables it to
send
keystrokes to
the computer!**

The human factor

As this attack is hardware-based, a human needs to perform the attack, and another has to make a mistake

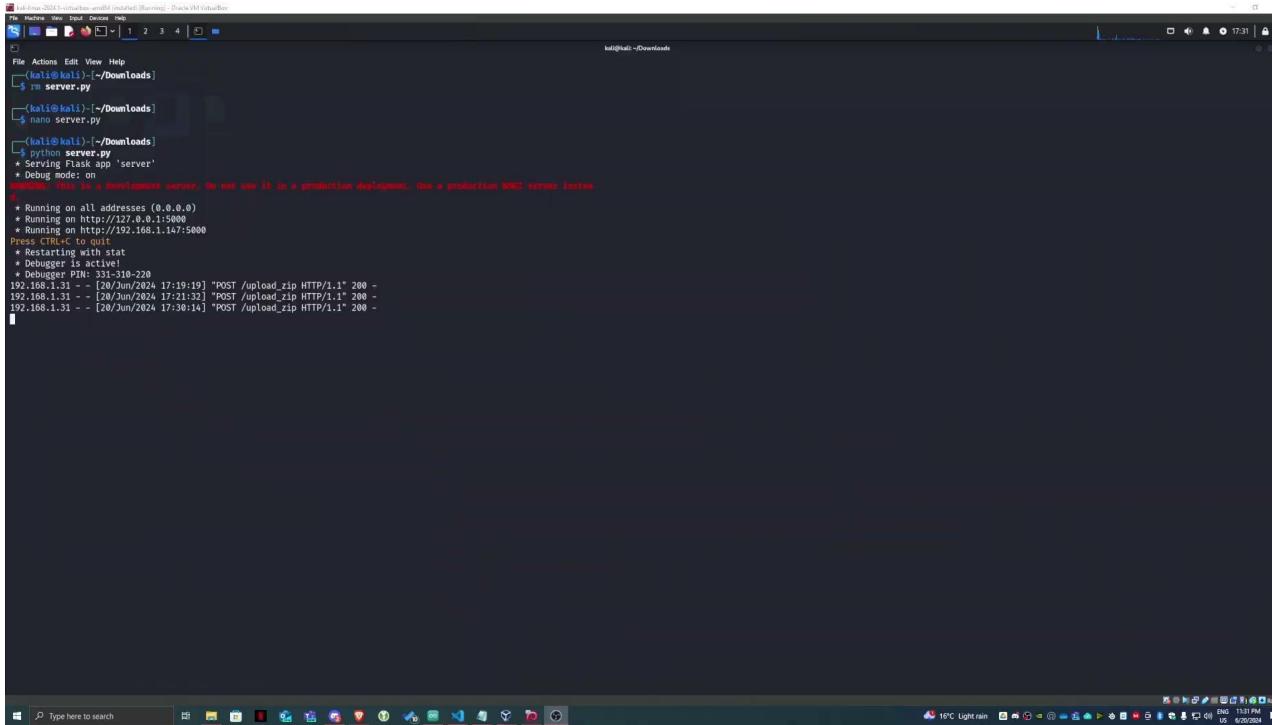
- The victim can leave the computer unlocked
- The attacker can perform social engineering to make the victim plug the computer



Example 1

A screenshot of a Kali Linux desktop environment. The desktop background features a dark, abstract design. At the top, there is a standard Linux-style header bar with icons for file operations, search, and system status. Below the header bar, the main workspace contains several windows. On the left, a terminal window titled 'File Actions Edit View Help' shows a command-line session where a Python web server is running on port 8080, serving files from a local directory. Another terminal window to the right shows a netcat listener on port 4444. A file browser window titled 'Downloads' is open, showing a file named 'script.py'. The bottom of the screen features a dock with various application icons, including a web browser, file manager, terminal, and system tools. The taskbar also displays system status information like battery level, signal strength, and system temperature.

Example 2



The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal output is as follows:

```
(kali㉿kali)-[~/Downloads]
$ nano server.py
(kali㉿kali)-[~/Downloads]
$ python server.py
* Serving Flask app "server"
* Debug mode: on
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead
* Running on all addresses (0.0.0.0)
* Running on http://127.0.0.1:5000
* Running on http://192.168.1.147:5000
Press Ctrl+C to quit
* Restarting with stat
* Debugger is active!
* Debugger PIN: 331-310-220
192.168.1.31 - - [20/Jun/2024 17:19:19] "POST /upload_zip HTTP/1.1" 200 -
192.168.1.31 - - [20/Jun/2024 17:21:32] "POST /upload_zip HTTP/1.1" 200 -
192.168.1.31 - - [20/Jun/2024 17:38:14] "POST /upload_zip HTTP/1.1" 200 -
```

How to protect ourselves

- Never plug an untrusted USB key
- Lock your computer when you need to leave it for some time
- You can use an “USB condom” or plug untrusted devices on an isolated machine first to check its behavior



WOCSA

Join Us!



-  www.wocsa.org
-  contact@wocsa.org
-  [@WOCSA-rx2mn](https://www.youtube.com/@WOCSA-rx2mn)
-  <https://discord.gg/pDunje3tpb>

-  [@wocsa](https://www.linkedin.com/company/wocsa)
-  [@wocsa_asso](https://twitter.com/wocsa_asso)
-  [@wocsa](https://facebook.com/wocsa)

-  Join us to change the digital world:
<https://www.helloasso.com/associations/wocsa/adhesions/bulletin-d-adhesion-2>
-  Please provide your feedback for our quality check process:
<https://www.wocsa.org/qcheck.php>