# The USB port – an infamous harbor for pirates, not only those from the Caribbean

Jakub Kralka,
Product Manager Axence

If you think you have read everything that has been written on attacks exploiting the USB ports, please make sure you read this article. Not only is the technique far from obsolete – it is constantly evolving and efficient precautions are always needed. There is no such thing as too much training!

## Primitive, but efficient

An attack exploiting the USB port can be compared with cutting of the brake lines in a car. It does not require much skill and anyone can do it; the attack is very cheap and deadly effective. Many malware code carriers can be bought on the Internet for a few dollars[1]. How do these work? Mostly by imitating other devices (BadUSB vulnerability). USB controller software, which is responsible for the correct recognition of the component within the system, can, after the hacker's manipulations, 'introduce itself' to the machine as a keyboard and capture the inputted data (keylogging). It can also input pre-programmed strings, effectively allowing the running of any code with the authorization of the logged in user. Some modified USB devices only need 30 seconds to obtain the computer's login credentials, even if the machine is blocked[2]. That's not all – a mutated Flash drive acting as network adapter can redirect your network traffic.

## An insult to enemy's intelligence

A flash drive found underneath your desk or in a corporate corridor is a real treat. The secret of what is stored inside is a lure not only for low-level employees. Few people can resist the temptation and take the finding to the IT department. The situation is especially dire, if the USB stick you find is a top-brand product and offers large capacity. This is like finding a one-hundred dollar bill on a street. You only need to check what is on it, format the device and you get extra storage for your private photos and films, which is always in demand in the digital world. Why wait, you can do it on your company laptop as well… The same scenario happened one day in an Iranian nuclear weapon plant, where a planted Flash drive destabilized the operation of uranium enriching centrifuges (see Stuxnet[3]).

[1] https://sekurak.pl/poison-tap-za-20-zlotych-wykrada-ciastka-z-zablokowanych-kompow/

[2] http://http://www.centrumxp.pl/Aktualnosci/16523,Kradziez-danych-logowania-za-pomoca-USB-PC-i-Mac-wciaz-niezabezpieczone.aspx

[3] https://niebezpiecznik.pl/post/stuxnet/

## Why does it still work?

Why are USB attacks still so popular and effective? Network security training which is provided in companies – if any is offered at all – is based on the latest examples of attacks. Employees may learn how to recognize phishing and what is ransomware, but are unaware that the danger may hit from the side they least expect. Who would think that you can infect your company with a dangerous worm by charging your e-cigarette through USB port[4]? Charging your phones, connecting China-made fans or lamps to ports in your corporate machines is a daily routine. Cheap gadgets of unknown origin are not the only 'unsure' products. An international scandal, which happened at the G20 summit held in Saint Petersburg in 2013, when participants received a multi-purpose charger with embedded malware within their welcome packs, has not been explained until now[5]. It is a highly dangerous game. When a cybercriminal wants to perform an APT attack, because the data they are targeting are highly valuable, they will create an exploit, which will not be recognized by any anti-viral software. If the company has a hardware sandbox, there is a chance the intruder will be intercepted – but it is still a rare sight in the server rooms of companies. Furthermore, an attack exploiting the BadUSB vulnerability, described above, can even escape the sandbox, as they do not use any files on the victim machine.

## What do we forget about?

Bruce Schneier – American encryption and ICT security expert said, "security is a process, not a product[6]" and we could not agree more. The network protection effort virtually never ends, and you can never be sure that any network is secure. According to Cisco report from 2016, 55% of respondents believed that employee behavior is one of the two biggest threats to data security, preceded only by the threat from organized cybercriminal groups (62%). Both groups often use USB data media to wreak havoc, produce failures or to extract data from our machines.

## Most common threats

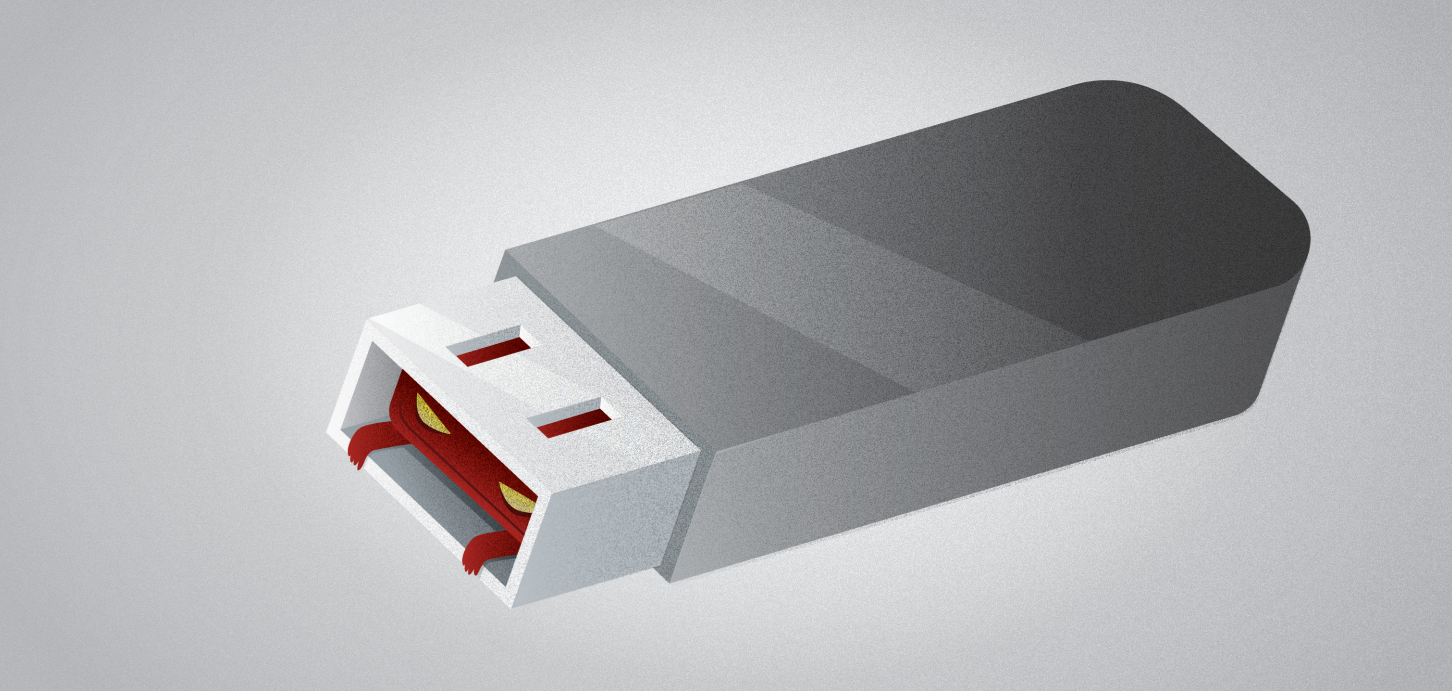
There are many types of attacks targeting unsecured USB ports. The most common are:

- Social Engineering: it uses a typical USB drive with HTML files. It is a phishing attack, obtaining users' logins and passwords during operations on files stored in the media.
- HID (Human Interface Device) spoofing: appropriately prepared USB drives use a specialized code to trick the computer into treating the USB stick as a keyboard. The false keyboard will only press buttons, if the device is connected. Button presses are a series of commands which interfere with the victim machine. In such a manner hackers can get full access to a user's workstation.
- 0-day: an example of an attack, using a security gap in the USB driver for the direct control over the machine, taken over as soon as the device is connected. It can happen when hackers find a gap in the USB device driver software before the manufacturer publishes appropriate patches.

[4] https://www.theguardian.com/technology/2014/nov/21/e-cigarettes-malware-computers

[5] https://niebezpiecznik.pl/post/rosjanie-wreczali-politykom-zainfekowane-ladowarki-i-pendrivey-na-szycie-g20/

[6] https://www.schneier.com/crypto-gram/archives/2000/0515.html



## Embedding the ports in concrete

How to protect yourself against the viruses infecting your network via USB ports? The solution is quite easy and is recommended even by the very malware code developers – at least those, who do it only as an exercise. However, not all endpoint security solutions offer such a feature. We are talking about simply blocking USB ports. But what can you do if your network contains a few hundred terminals? What you need is a solution allowing corporate port blocking policies to be created and then deployed in all computers in the network. This task is performed by the DataGuard module in the Axence nVision® suite. With it you can manage the access of the portable devices (save, run and read operations) to your corporate network, eliminating the risk of infection with worms equipped with automatic installation commands. Central configuration is possible: you can set rules for the entire network, for selected network maps or for Active Directory groups and users. With the use of DataGuard, the organization can additionally limit the leaks of strategic data on mass storage devices and mobile drives. The range of threats is very wide and you need to remember about the obvious to avoid an unpleasant surprise. It is also worth showing the above examples to your employees.