Protecting USB against malware

© *Rob Hulsebos*

Version 27 December 2023

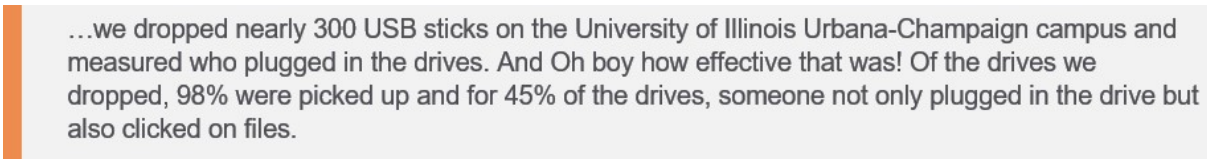
Introduction

In recent years, USB-ports are increasingly used for their power supply: charging up mobile phones and tablets. But when the USB-cable is plugged in, not only the power-supply is connected, but *also* a bidirectional network connection. There is more need than ever to assure that unsuspecting users in dire need of some mAh do not accidentally bring malware with them. Conversely, a device may get hacked via a device that looks like a charger ("juice jacking").

Apart from charging, USB is of course also used for transferring files between systems. Malware can travel via USB-sticks, just like in the past with floppies. Finally, USB can also be used to connect a variety of equipment, most of which are innocent, but for a few $/€'s less innocent equipment can be bought on EBay/Amazon or other web shops. Hacking via USB-equipment is now in reach of anyone.

USB is a hacker's dream. It allows unlimited access to many systems, with a large variety of hardware: mice, keyboards, USB sticks (thumb drives), disks, WiFi, audio, screens / monitors, printers, etc. It is also not difficult to impersonate devices: a CPU on the USB-device looking like a memory drive can fake a keyboard instead, and suddenly automatically any command can be executed as if it were typed by the owner of the device. Fake network devices make a PC (= Windows) route all network traffic to it, allowing that device to inspect the data in each and every network message. USB devices with storage (thumb drives, mobile phones, tablets) can be used to extract files from a PC, but also to inject malware into it.

Another attack vector using USB is malware that infects the internal CPU of the device (instead of the data on the device). This attack, called "BadUSB", was revealed during the Black Hat conference in August 2016. It is little known that such a CPU is present, with its own software stored in local memory. This CPU and its local memory is completely inaccessible for virus scanners and other malware-scanning tools.



…we dropped nearly 300 USB sticks on the University of Illinois Urbana-Champaign campus and measured who plugged in the drives. And Oh boy how effective that was! Of the drives we dropped, 98% were picked up and for 45% of the drives, someone not only plugged in the drive but also clicked on files.

Figure: Result of a test by Google's anti-abuse team

Honeywell report
Is this a realistic scenario, or is it just hear-say? For years we've been hearing about the dangers posed by USB, but there were little figures available. But now we have data! According to a Honeywell report[1] published November 2018, with an update in 2021 and 2022, it is even worse

[1] *See*: *https://www.honeywell.com/content/dam/honeywellbt/en/images/content-images/cybersecurity-threat-report-2021/Industrial%20Cybersecurity%20USB%20Threat%20Report%20v5.pdf*

than they expected. With their product "SMX" (described below) USB-sticks (thumb drives) are scanned for malware before their use is allowed in an industrial installation. SMX was deployed 50 production locations worldwide. Because these systems report back what they have detected, Honeywell was able to put together "the big picture".

The data show that infection of malware via USB is a *very* realistic scenario:

- In 44% of the sites using SMX, at least one suspicious file was found.
- Of these files, some 26% could have caused a disruption in an industrial system.
- Even after 8 years, Stuxnet is still detected.
- Some 16% of the malwares detected was specially made for industrial systems.

All sorts of malware were detected by SMX: adware, hacking tools, password crackers, viruses, ransomware, rootkits, etc.

Honeywell also found that 10% of the malware variants were less than a week old. This means that antivirus-solutions that are not kept up-to-date would likely not have detected these malwares. And 11% of the malwares were not detectable by traditional antivirus products at all.

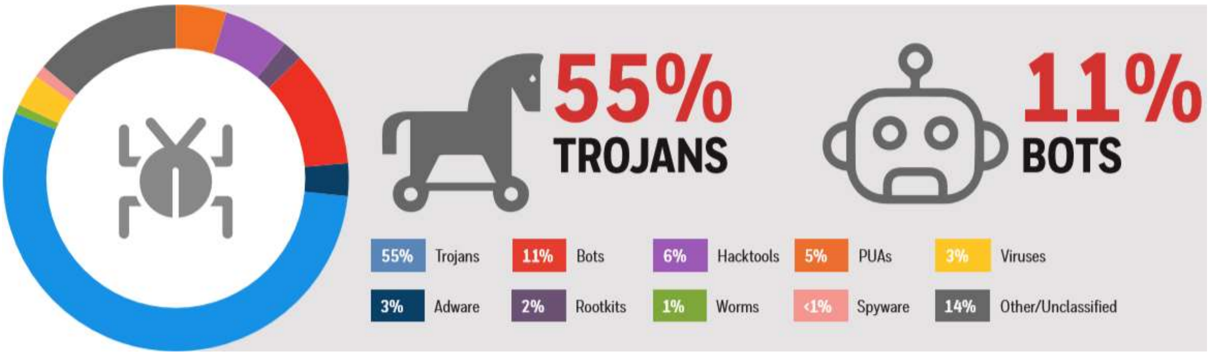


Figure: Types of malware detected by SMX. Source: Honeywell.

It is therefore mandatory to think about how to properly protect the USB-ports in an industrial control system, without stifling employee productivity. Below, we will discuss various strategies, each with its own advantages and disadvantages.

Background

The YouTube-video https://www.youtube.com/watch?v=nuruzFqMgIw is a recording of a presentation during BlackHat 2014 about the weaknesses of USB.

Malware propagation

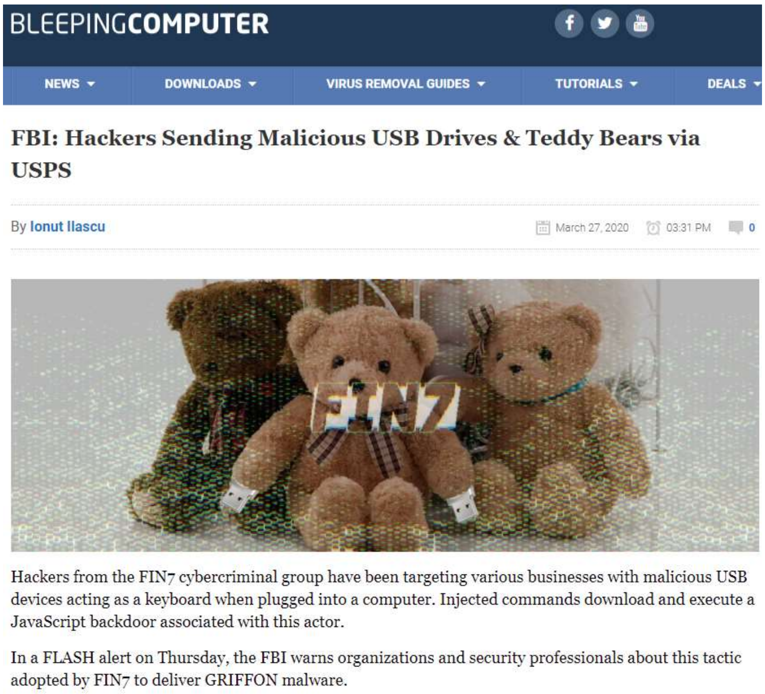
Just as in the past floppies were the medium for viruses to spread from PC to PC, thumb drives are now used as medium. In 2020, a cryptomining botnet called "VictoryGate" was discovered[2] that used this method to propagate.

Hacker groups

A well-known tactic used by hackers is to put infected thumb drives on the parking lot of a company. There's always someone interested in what's on the device. But by now, many companies have trained their staff to discard such devices.

Hackers have now started a new tactic in 2020: sending infected thumb drives by mail. To lure the recipient into plugging in the thumb drive, a $50 "BestBuy" gift card also in the envelope, which is said to contain instructions how to activate the gift card.

[2] *https://www.welivesecurity.com/2020/04/23/eset-discovery-monero-mining-botnet-disrupted/*



FBI: Hackers Sending Malicious USB Drives & Teddy Bears via USPS

By Ionut Ilascu — March 27, 2020 — 03:31 PM — 0

Hackers from the FIN7 cybercriminal group have been targeting various businesses with malicious USB devices acting as a keyboard when plugged into a computer. Injected commands download and execute a JavaScript backdoor associated with this actor.

In a FLASH alert on Thursday, the FBI warns organizations and security professionals about this tactic adopted by FIN7 to deliver GRIFFON malware.

Figure: Teddy bears and gift cards sent by mail to lure unsuspecting recipients.

Note: because Linux and MacOS are little used in industrial automation, we will mainly discuss solutions for Windows, whenever software is involved. This does not mean that for other operating systems identical solutions do not exist.

1 Examples of (unwanted) devices

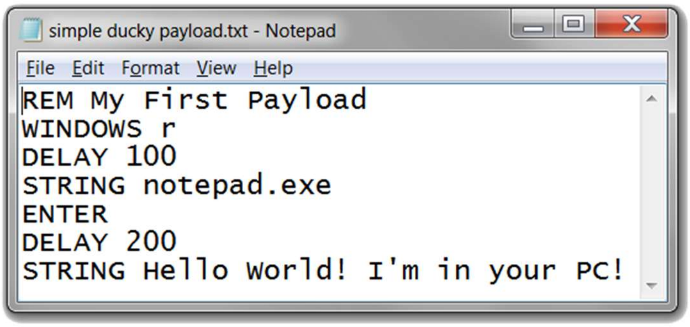
In this chapter we'll describe a set of USB-devices, most of which are useful in their own right. But other uses are possible as well!

1.1 Rubber Ducky

The figure below shows a so-called "Rubber Ducky". It is a device that can be bought from HakShop.com for $60. Despite it looking like any ordinary USB-stick, it isn't one. A small processor emulates a keyboard. The characters that it feeds to the PC can be stored on an SD-card, which can be programmed via a simple scripting language.

Figure: A "Rubber ducky" in its innocent looking packaging (top), and its internals (below). At the left the slot where an SD-card can be inserted.

On the SD-card there is ample space to store very large scripts, 16 megabytes of storage suffices to store event the largest scripts one could ever think of. Scripts can be edited by taking the SD-card out of the 'Ducky', plugging it into a PC, and then any editor can be used to compose the script.



simple ducky payload.txt - Notepad
File Edit Format View Help

```
REM My First Payload
WINDOWS r
DELAY 100
STRING notepad.exe
ENTER
DELAY 200
STRING Hello World! I'm in your PC!
```

Figure: Example of a script that can be executed by the rubber ducky. It starts notepad.exe on the PC, and types one line of text.

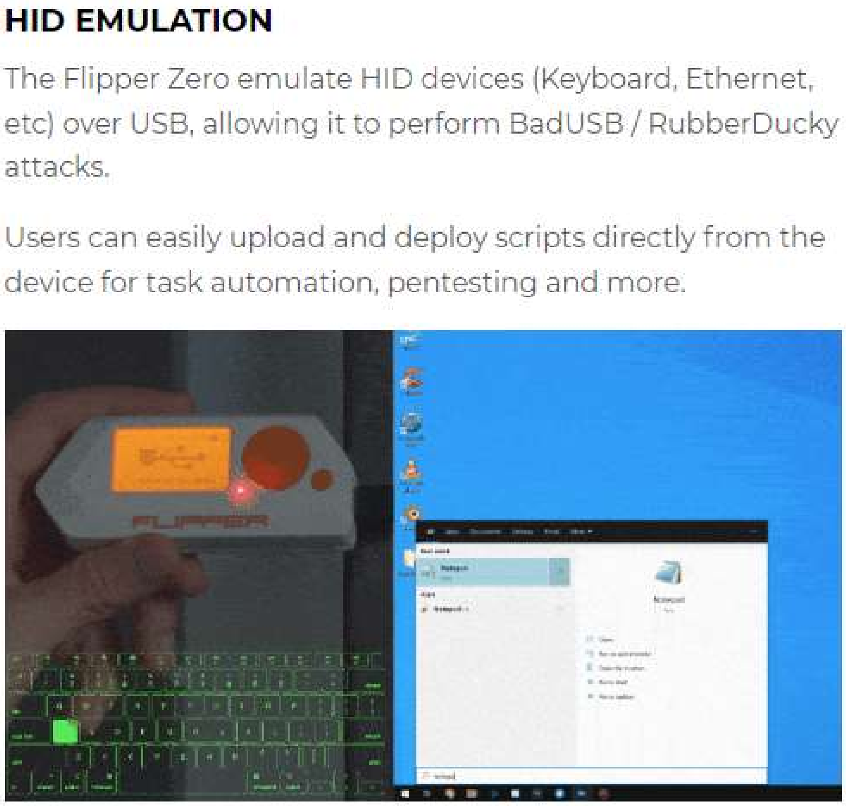
When the 'Ducky' is plugged in a PC, it starts 'typing' after a few seconds. To my surprise, the device even worked on some embedded devices. This means that not only PC's can be taken over, but probably any device that allows a keyboard to be attached to it via USB.

New version

In 2022, a new version of the Rubber Ducky was launched, with the "DuckyScript 3.0" programming language, and a web-based development environment, compiler and debugger.The webpage https://shop.hak5.org/blogs/payloads gives examples of the new capabilities.

Similar devices

There are other devices on the market that work similar like the Rubber Ducky. An example of this is the "Flipper Zero" (which has far more functionality than just keyboard emulation).



HID EMULATION

The Flipper Zero emulate HID devices (Keyboard, Ethernet, etc) over USB, allowing it to perform BadUSB / RubberDucky attacks.

Users can easily upload and deploy scripts directly from the device for task automation, pentesting and more.

Figure: Flipper Zero in action

1.2 Commercial product promotion device

Once I received an envelope with product promotion folders, and also containing a flat, small, piece of cardboard with a USB-connector sticking out.

Figure: The USB device that I received by mail.

Upon plugging this in, it took over my PC, started the browser, and surfed to a promotional website for the product. It stopped there, while in the meantime I scrambled to stop this script. Luckily for me it was benign, but it could as well have been malicious. I wonder why a company that promotes itself as being very conscious about cybersecurity sends this around.

1.3 Keyboard logger

Via Amazon I bought for $50 a key logger, delivered in two days per mail. Put it in a USB-port, plug the keyboard cable in the device, and ready. All keystrokes can now be followed via a built-in WiFi access point. In case you're not in the neighbourhood, the device has 16 Mbytes of memory where all keystrokes are stored. Because it is small, it is hardly noticeable, especially at the back of a PC.

Figure: The $50 key logger-with-WiFi

For hackers, using key loggers is expensive, since they must leave the device behind, which they may not be able to retrieve later.

Keyboard loggers can also be home-made with a Raspberry Pi Zero W, loaded with some software publicly available via: github.com/xcellerator/usbninja/blob/master/doc/HID.md, or as on https://github.com/spacehuhn/wifi_keylogger.

Maltronics has a WiFi-accessible keylogger which is small enough to be inserted in a keyboard itself. This makes it very difficult to discover!

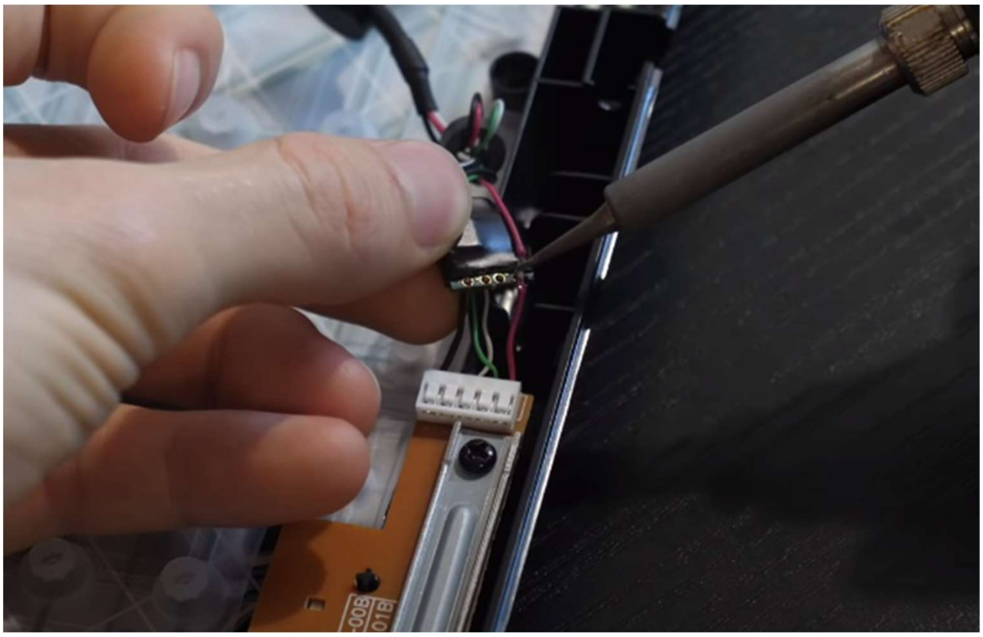


Figure: Maltronics keylogger PCB being inserted in a keyboard. Source: maltronics.com

1.4 LAN Turtle

Via the web shop of "HakShop" a variety of products can be ordered for use by penetration testers and network administrators, and of course also by hackers. An example of this is the "LAN Turtle", which has a USB connection and an Ethernet port. It looks like a generic USB/Ethernet converter, to "allow it to blend in easily in IT-environments" (according to HakShop).

LAN Turtle 3G
• Unlocked world-band 3G modem
• Out-of-band remote access
LAN Turtle SD
• Storage expansion via microSD
• Capture packets, exfiltrate data
USB Ethernet adapters with covert backdoors
These seemingly innocent USB Ethernet adapters are discrete remote access toolkits and man-in-the-middles for penetration testers and systems administrators.

Figure: The advantage of the LAN Turtle family explained.

The Turtle allows access from an outside network via a VPN connection, it can scan the internal network, it allows running toolkits like Meterpreter, it can run as a "man in the middle", it can exfiltrate data, do DNS spoofing, etc. And that for only $55. It only needs the USB for the power supply.

How devices like the LAN Turtle work is explained in detail on the "Poison Tap" website (https://samy.pl/poisontap). Basically, the subnet of a low-priority network always has a higher priority than the default gateway. At starting up, the device has sent a specially crafted DHCP message that make the PC think that the whole IPv4-address space is accessible via this device, routing all internet traffic through it. This works even when the PC is locked or password protected.

1.5 Power bank

Power banks only contain batteries, isn't it? But they do have an USB-capability as well. A hacker could easily modify a power bank to contain a rubber ducky.

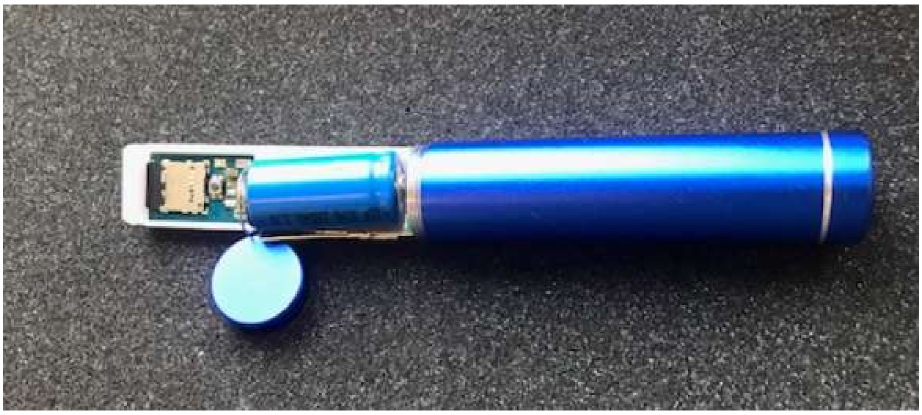
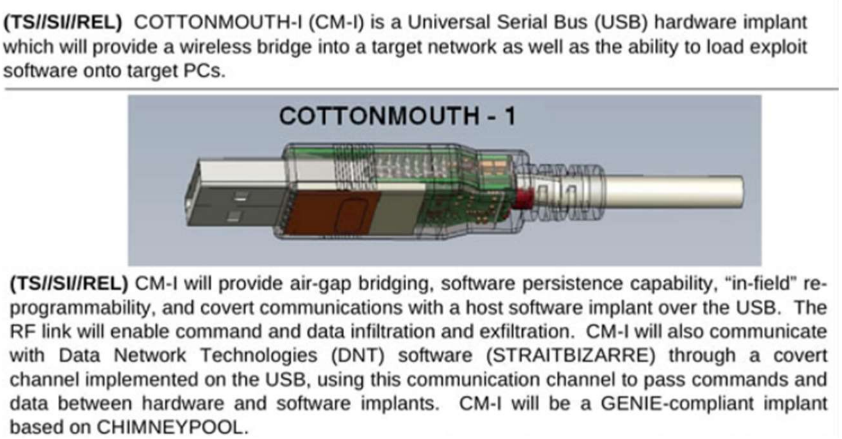


Figure: A rubber ducky inside a power bank. Source: Sepio Systems.

1.6 COTTONMOUTH

This is an NSA (National Security Agency) device, whose existence became known after a publication by the German newspaper Der Spiegel in 2013. It was part of 49-page catalog of spying devices. The COTTONMOUTH devices (and its successors) allowed wireless access to the device the USB cable was plugged into.



(TS//SI//REL) COTTONMOUTH-I (CM-I) is a Universal Serial Bus (USB) hardware implant which will provide a wireless bridge into a target network as well as the ability to load exploit software onto target PCs.

COTTONMOUTH - 1

(TS//SI//REL) CM-I will provide air-gap bridging, software persistence capability, "in-field" re-programmability, and covert communications with a host software implant over the USB. The RF link will enable command and data infiltration and exfiltration. CM-I will also communicate with Data Network Technologies (DNT) software (STRAITBIZARRE) through a covert channel implemented on the USB, using this communication channel to pass commands and data between hardware and software implants. CM-I will be a GENIE-compliant implant based on CHIMNEYPOOL.

Figure: The NSA "COTTONMOUTH" USB device

The Der Spiegel publication triggered various open-source projects (see below for examples) to make identical devices, but for an affordable price (around $100) – the original had a price tag of $20000. More info about COTTONMOUTH on: https://en.wikipedia.org/wiki/ANT_catalog.

1.7 Chargers

USB chargers are usually large, allowing other equipment to be easily sneaked in. One example of this is the "KeySweeper" (https://samy.pl/keysweeper), containing an Arduino-based wireless receiver that sniffs, decrypts and logs all keystrokes on a Microsoft wireless keyboard, and sends the data away via a GSM connection. It can also send an SMS when the unsuspecting user is accessing interesting websites (i.e., his bank).

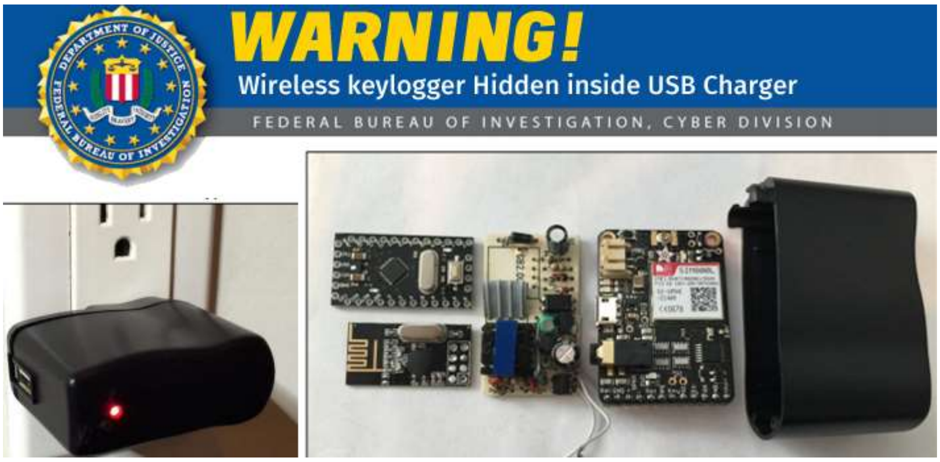

WARNING!
Wireless keylogger Hidden inside USB Charger
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Figure: Plenty of room to add other electronics (source: FBI).

Technically this device doesn't use any USB connection, other than hiding the electronics in the housing of a USB charger.

1.8 Mouse

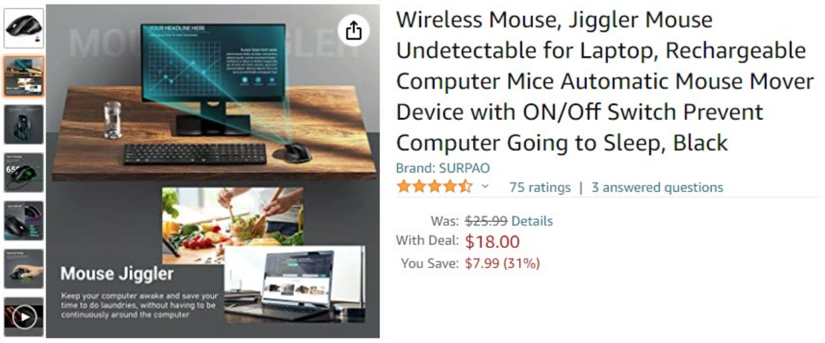
Some organizations do not allow the use of USB memory sticks to prevent data exfiltration. Actually that is very difficult to keep in check, since data can also be smuggled out via SD-cards, which are small enough to be hidden everywhere.

But a USB memory stick does not have to look like a memory stick; the memory can also be hidden in another USB device, like (an innocent looking) mouse.

Figure: The Microsoft "Memory Mouse 8000" includes 1 Gbyte of flash memory.

Mouse jigglers
In many organizations, PC's may be configured to automatically lock if no mouse or keyboard activity has been seen for a while. This is to prevent somebody else using the PC.

As some users resent the automatic lock, devices are on the market which simulate mouse movements, thus so preventing the PC to be locked, so-called "mouse jigglers" (search on amazon.com, and find a large variety of these things). It is even possible to have jiggler built into a mouse itself, this saves the usage of a USB-port.


Mouse Jiggler
Keep your computer awake and save your time to do laundries, without having to be continuously around the computer

Wireless Mouse, Jiggler Mouse Undetectable for Laptop, Rechargeable Computer Mice Automatic Mouse Mover Device with ON/Off Switch Prevent Computer Going to Sleep, Black

Brand: SURPAO

★★★★☆ 75 ratings | 3 answered questions

Was: ~~$25.99~~ Details
With Deal: $18.00
You Save: $7.99 (31%)

Figure: Two examples of mouse jigglers (source: amazon.com).

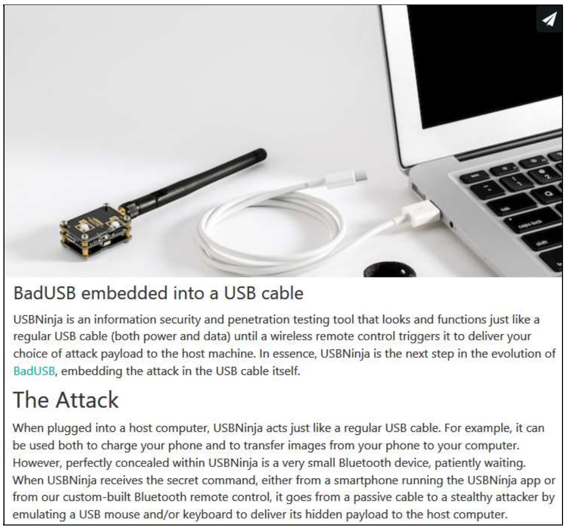
While mouse jigglers are not a cybersecurity threat on their own, their use introduces a secondary threat (possible abuse of a PC). Even if these devices can be detected, there are also mouse jigglers on the market that do not use USB.

1.9 Modems

A USB-device posing as a serial port can be a GSM-modem instead. It will allow access to a device from any location on earth, bypassing all security measures in a company (like a firewall). The advantage of USB is that the modem needs no batteries; the USB-port provides the power.

1.10 USBNinja / BadUSB / O.MG

Kevin Mitnick launched the "USBNinja" cable in 2018. It looks like a normal USB charging cable, and indeed it charges devices. But it also has a Bluetooth chip hidden in the connector. From an external Bluetooth device, it is possible to send (from a distance) data to the 'cable', which then emulates a keyboard and can execute downloadable scripts.



BadUSB embedded into a USB cable

USBNinja is an information security and penetration testing tool that looks and functions just like a regular USB cable (both power and data) until a wireless remote control triggers it to deliver your choice of attack payload to the host machine. In essence, USBNinja is the next step in the evolution of BadUSB, embedding the attack in the USB cable itself.

The Attack

When plugged into a host computer, USBNinja acts just like a regular USB cable. For example, it can be used both to charge your phone and to transfer images from your phone to your computer. However, perfectly concealed within USBNinja is a very small Bluetooth device, patiently waiting. When USBNinja receives the secret command, either from a smartphone running the USBNinja app or from our custom-built Bluetooth remote control, it goes from a passive cable to a stealthy attacker by emulating a USB mouse and/or keyboard to deliver its hidden payload to the host computer.

Figure: The "USBNinja" ensemble (a cable and a Bluetooth sender) costs $150.

The device with the antenna has two buttons A and B, that cause payload A or B to be sent to the USB port. This payload is programmed in advance in the USBNinja (the cable). This is an Arduino, which can be easily programmed via the Arduino IDE, and a little bit of C-knowledge. Then, when the USBNinja is passed to a potential victim, there is nothing visible indicating that this cable is special. At any moment, an attacker in the vicinity can activate the payload by pressing button A or B, or use any Android phone (with a special app) which can also activate payload A or B.

Note that there is also "USBNinja" software, an open-source tool, that can be used to restrict USB-drive access for Windows (see http://usbninja.weebly.com for general info, and the source code on github.com/gfoudree/usbninja). Don't confuse this with the USBNinja software at https://github.com/xcellerator/usbninja, which uses a RaspBerry Pi Zero W to emulate various types of USB devices (serial port, Ethernet, mass storage and keyboard devices).

Following the USBNinja, various other products appeared on the market. One of these is the "O.MG", which has advanced functions like location detection, modify its behavior, trigger payloads, erase payloads, and clone its identity from trusted (by the user) devices, and has a keylogger function. Automated attacks can be executed via the WWW via Python scripts. It is available with USB-A, USB-C, USB-micro and Apple Lightning connectors.

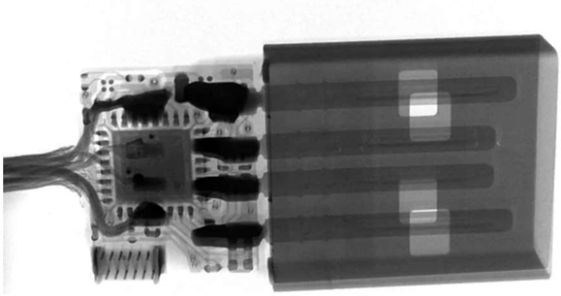


Figure: XRay of a O.MG cable showing the electronics

To detect traffic on USB cables which shouldn't have any, there is the "O.MG Malicious Cable Detector". It doesn't block any traffic, it just blinks a LED when traffic is seen.

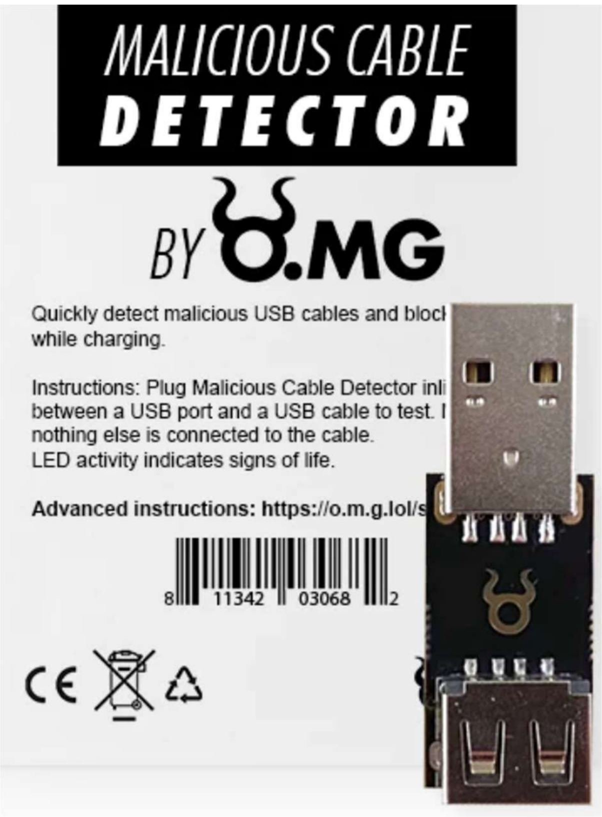
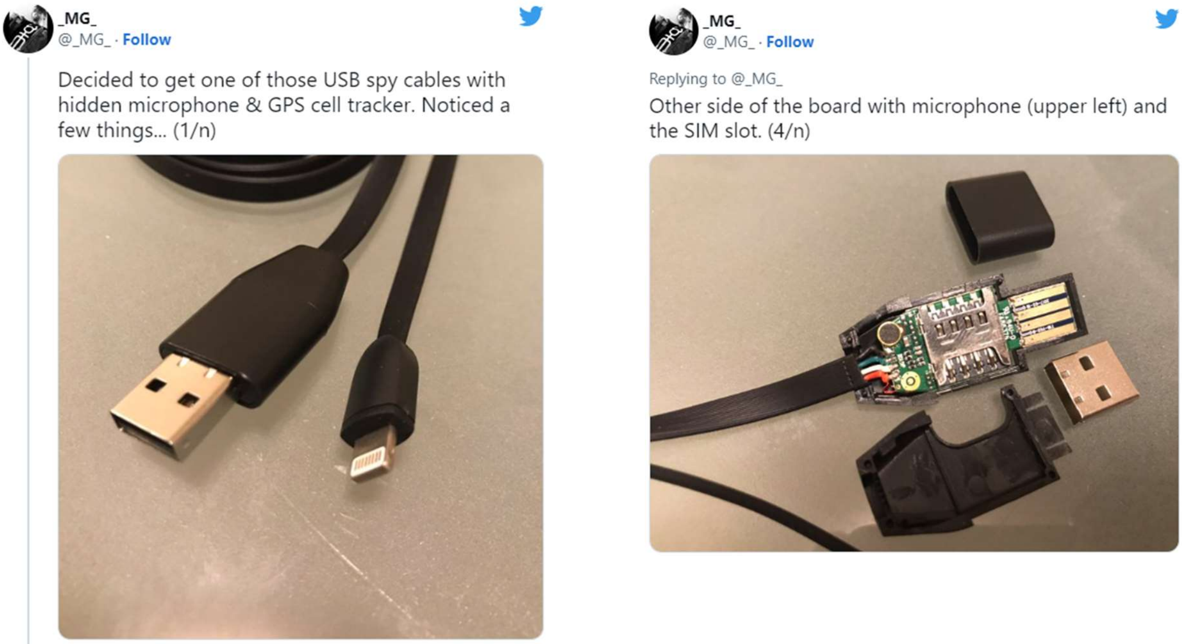

MALICIOUS CABLE DETECTOR
BY O.MG
Quickly detect malicious USB cables and bloc
while charging.
Instructions: Plug Malicious Cable Detector inl
between a USB port and a USB cable to test. I
nothing else is connected to the cable.
LED activity indicates signs of life.
Advanced instructions: https://o.m.g.lol/s
8 11342 03068 2

Figure: The "O.MG Malicious Cable Detector"

1.11 Spy cable

There are USB-cables on the market which have a microphone and geolocation capabilities via a GPS receiver (= where you are). Data is sent out via GSM.



_MG_
@_MG_ · Follow

Decided to get one of those USB spy cables with hidden microphone & GPS cell tracker. Noticed a few things... (1/n)

_MG_
@_MG_ · Follow

Replying to @_MG_

Other side of the board with microphone (upper left) and the SIM slot. (4/n)

Figure: Spy cable with microphone, GPS and GSM (source: https://mg.lol/blog/spycable/)

A variant of this device is available as an USB cigarette lighter adapter.

1.12 Bash Bunny

The “Bash Bunny” from Hak5 (shop.hak5.org) is “the world’s most advanced USB attack platform” (according to the vendor) which will set you back for some $120. It has the capability to act like a flash drive, serial (COM) port, Ethernet interface, and a keyboard. The payload select switches allow you to choose one of 16 preprogrammed payloads. These are programmed in a language called "DuckyScript”.

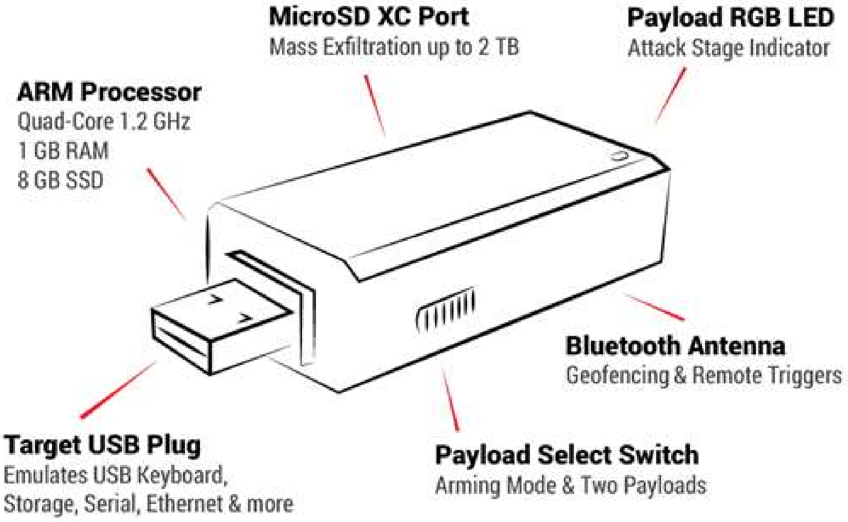
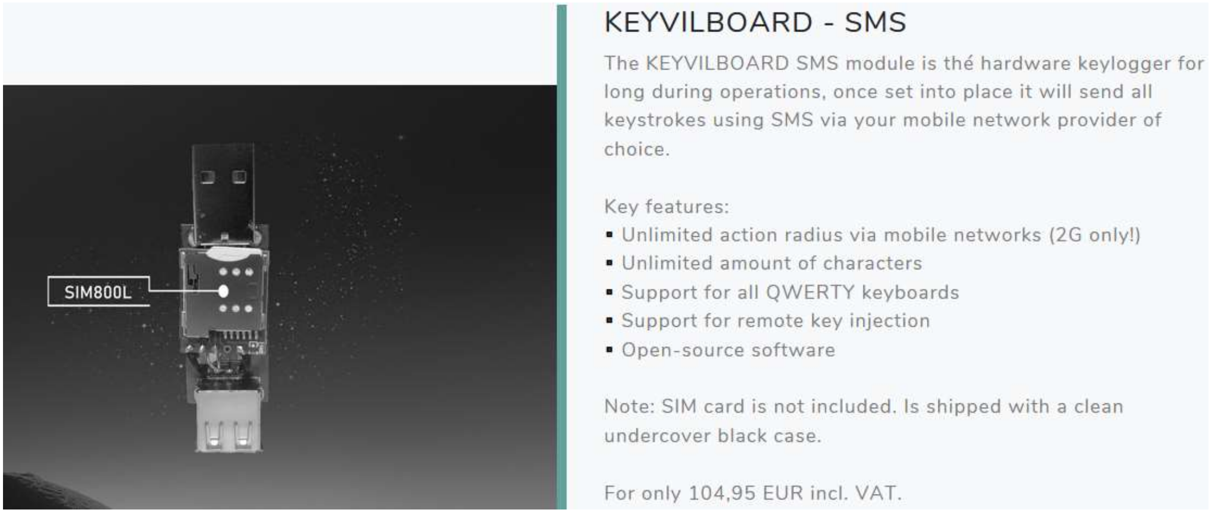


Figure: Capabilities of the HAK5 “Bash Bunny” (source: Hak5Shop)

In case you are handy with a soldering iron and willing to do some Linux programming, it is possible to make a simple version of the Bash Bunny, with almost the same capabilities; see https://www.cron.dk/poor-mans-bash-bunny/ for a description.

1.13 Keyvilboard

“Keyvilboard” is a Dutch device that is also a keyboard emulator. The text to be ‘typed’ can be sent via WiFi or an SMS (= text message). This allows attacks world-wide (www.keyvilboard.nl).



KEYVILBOARD - SMS

The KEYVILBOARD SMS module is thé hardware keylogger for long during operations, once set into place it will send all keystrokes using SMS via your mobile network provider of choice.

Key features:

- Unlimited action radius via mobile networks (2G only!)
- Unlimited amount of characters
- Support for all QWERTY keyboards
- Support for remote key injection
- Open-source software

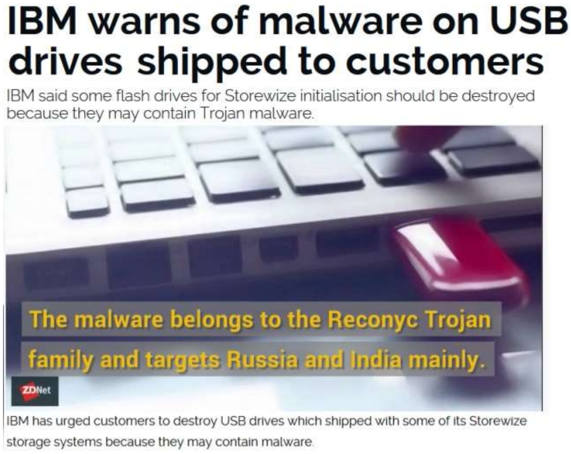
Note: SIM card is not included. Is shipped with a clean undercover black case.

For only 104,95 EUR incl. VAT.

Figure: The Keyvilboard SMS version

1.14 Normal USB sticks

Surprisingly, normal USB sticks can be dangerous as well. Of course, *you* protect your own USB sticks very well. But what do you do when you buy an IT/OT product from a renowned vendor who provides the documentation, drivers, user-software etc. on an accompanying USB-stick? Perhaps you assume that such vendors have their manufacturing processes in order, that no malware is accidentally put on the USB-stick. Unfortunately, that is not always so!

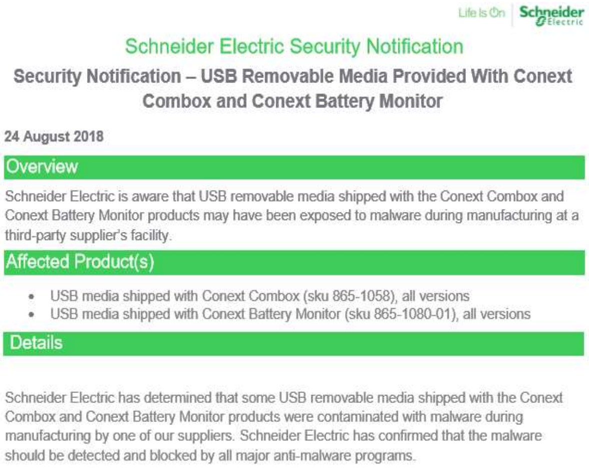


IBM warns of malware on USB drives shipped to customers

IBM said some flash drives for Storewize initialisation should be destroyed because they may contain Trojan malware.

The malware belongs to the Reconyc Trojan family and targets Russia and India mainly.

IBM has urged customers to destroy USB drives which shipped with some of its Storewize storage systems because they may contain malware.



Schneider Electric Security Notification

Security Notification – USB Removable Media Provided With Conext Combox and Conext Battery Monitor

24 August 2018

Overview

Schneider Electric is aware that USB removable media shipped with the Conext Combox and Conext Battery Monitor products may have been exposed to malware during manufacturing at a third-party supplier's facility.

Affected Product(s)

- USB media shipped with Conext Combox (sku 865-1058), all versions
- USB media shipped with Conext Battery Monitor (sku 865-1080-01), all versions

Details

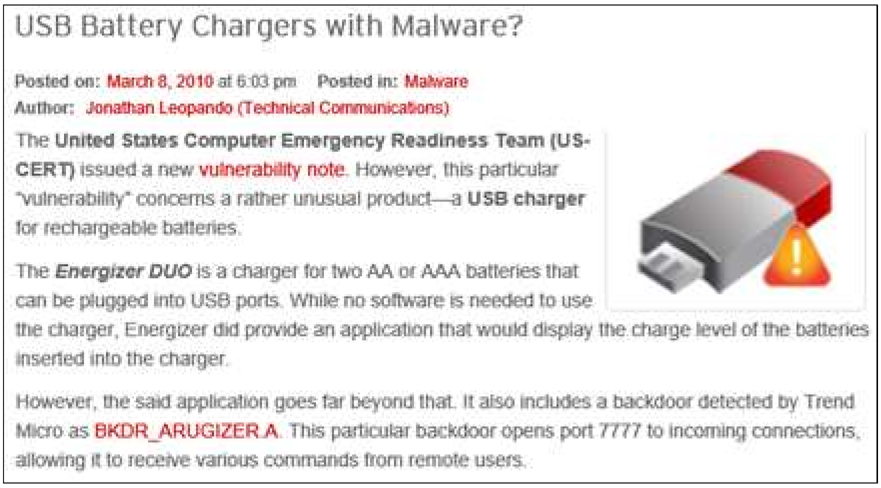
Schneider Electric has determined that some USB removable media shipped with the Conext Combox and Conext Battery Monitor products were contaminated with malware during manufacturing by one of our suppliers. Schneider Electric has confirmed that the malware should be detected and blocked by all major anti-malware programs.

Figure: IBM delivered malware on USB-sticks-
in 2017, and Schneider in 2018 (sources: ZDNet, Schneider)

The more a device looks like a normal USB-stick, the better the chance that it is used. This article explains how to make one (and much more interesting technical info):
https://elie.net/blog/security/what-are-malicious-usb-keys-and-how-to-create-a-realistic-one/

1.15More examples

A USB-battery charger with embedded malware:



USB Battery Chargers with Malware?

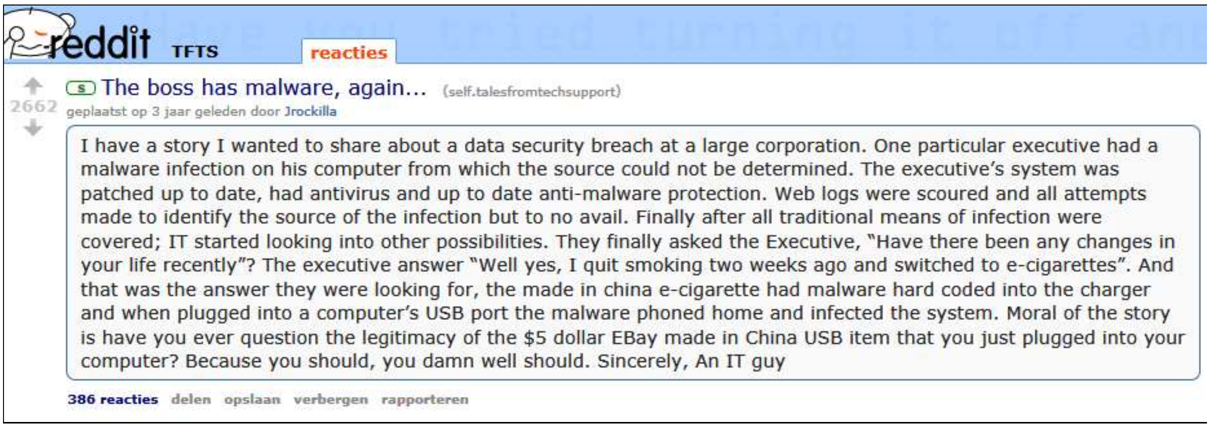
Posted on: March 8, 2010 at 6:03 pm Posted in: Malware
Author: Jonathan Leopando (Technical Communications)

The **United States Computer Emergency Readiness Team (US-CERT)** issued a new vulnerability note. However, this particular "vulnerability" concerns a rather unusual product—a **USB charger** for rechargeable batteries.

The ***Energizer DUO*** is a charger for two AA or AAA batteries that can be plugged into USB ports. While no software is needed to use the charger, Energizer did provide an application that would display the charge level of the batteries inserted into the charger.

However, the said application goes far beyond that. It also includes a backdoor detected by Trend Micro as BKDR_ARUGIZER.A. This particular backdoor opens port 7777 to incoming connections, allowing it to receive various commands from remote users.

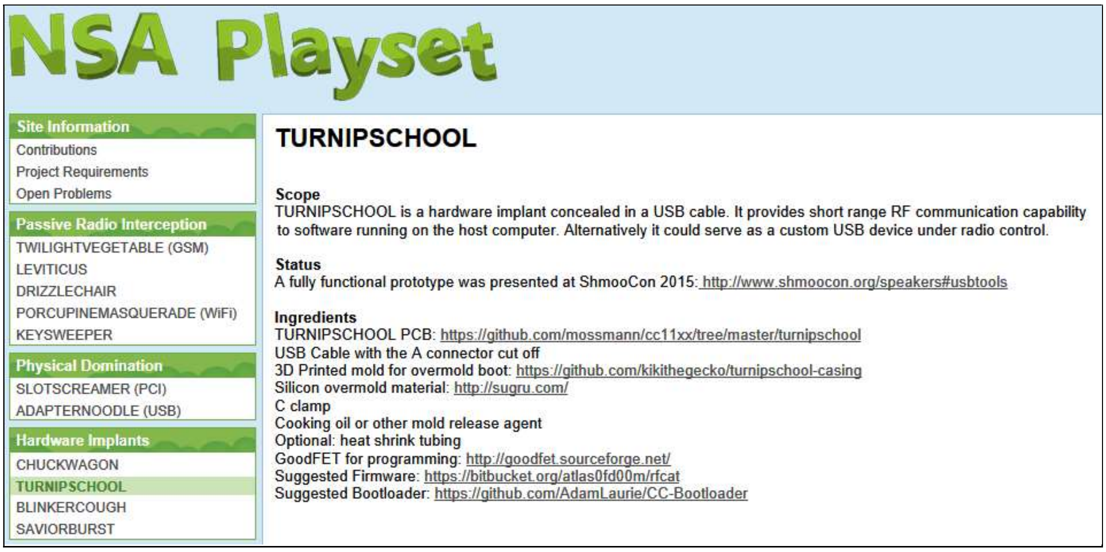
Figure: Source: TrendMicro



The boss has malware, again... (self.talesfromtechsupport)
geplaatst op 3 jaar geleden door Jrockilla

I have a story I wanted to share about a data security breach at a large corporation. One particular executive had a malware infection on his computer from which the source could not be determined. The executive's system was patched up to date, had antivirus and up to date anti-malware protection. Web logs were scoured and all attempts made to identify the source of the infection but to no avail. Finally after all traditional means of infection were covered; IT started looking into other possibilities. They finally asked the Executive, "Have there been any changes in your life recently"? The executive answer "Well yes, I quit smoking two weeks ago and switched to e-cigarettes". And that was the answer they were looking for, the made in china e-cigarette had malware hard coded into the charger and when plugged into a computer's USB port the malware phoned home and infected the system. Moral of the story is have you ever question the legitimacy of the $5 dollar EBay made in China USB item that you just plugged into your computer? Because you should, you damn well should. Sincerely, An IT guy

Figure: Source: Reddit (2015)



TURNIPSCHOOL

Scope
TURNIPSCHOOL is a hardware implant concealed in a USB cable. It provides short range RF communication capability to software running on the host computer. Alternatively it could serve as a custom USB device under radio control.

Status
A fully functional prototype was presented at ShmooCon 2015: http://www.shmoocon.org/speakers#usbtools

Ingredients
TURNIPSCHOOL PCB: https://github.com/mossmann/cc11xx/tree/master/turnipschool
USB Cable with the A connector cut off
3D Printed mold for overmold boot: https://github.com/kikithegecko/turnipschool-casing
Silicon overmold material: http://sugru.com/
C clamp
Cooking oil or other mold release agent
Optional: heat shrink tubing
GoodFET for programming: http://goodfet.sourceforge.net/
Suggested Firmware: https://bitbucket.org/atlas0fd00m/rfcat
Suggested Bootloader: https://github.com/AdamLaurie/CC-Bootloader

Figure 24: NSA devices (source: www.nsaplayset.org)

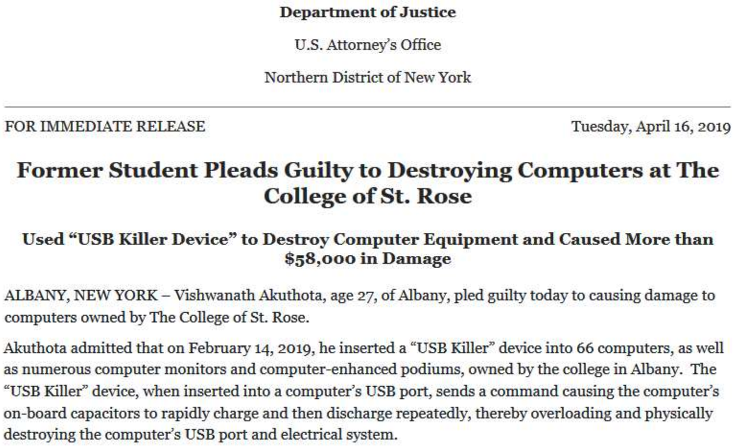
We could devote a lot of pages to the various ingenious USB-devices invented so far. But they're already summarized at: https://www.bleepingcomputer.com/news/security/heres-a-list-of-29-different-types-of-usb-attacks/.

1.16 USB Killer

The last device that I want to show is the "USB Killer" (usbkill.com). It is designed to test the surge protection circuitry of a device. When connected, it zaps the USB port with a 200 VDC surge 10 times per second (see what happens on: http://www.youtube.com/watch?v=3hbuhFwFsDU).

Figure: The 'anonymous' USB killer looking like an ordinary USB stick.

The USB killer device looks like an ordinary USB stick[3], waiting for a curious person to check what's on the stick… and zapping his PC instead. The ultimate DoS attack! With newer version, it is even possible to set a time-delay, or to trigger it over WiFi, or to zap a device even when it is switched off.



Department of Justice

U.S. Attorney's Office

Northern District of New York

FOR IMMEDIATE RELEASE Tuesday, April 16, 2019

Former Student Pleads Guilty to Destroying Computers at The College of St. Rose

Used "USB Killer Device" to Destroy Computer Equipment and Caused More than $58,000 in Damage

ALBANY, NEW YORK – Vishwanath Akuthota, age 27, of Albany, pled guilty today to causing damage to computers owned by The College of St. Rose.

Akuthota admitted that on February 14, 2019, he inserted a "USB Killer" device into 66 computers, as well as numerous computer monitors and computer-enhanced podiums, owned by the college in Albany. The "USB Killer" device, when inserted into a computer's USB port, sends a command causing the computer's on-board capacitors to rapidly charge and then discharge repeatedly, thereby overloading and physically destroying the computer's USB port and electrical system.

Figure: It works!

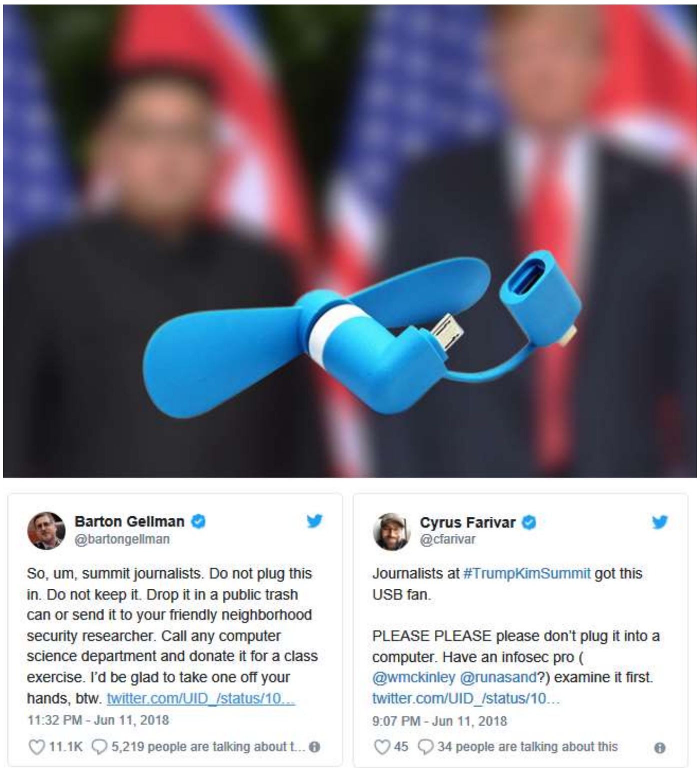
There is a protection device on the market called "USBKiLL Shield":

With the yellow LEDs it signals the detection of an overvoltage, and blocks it.

1.17 False alert

Most USB-devices are harmless. But what would you do when a North-Korean gives you a USB-powered ventilator during the Trump/Kim summit in 2018, given the reputation of this country in cyberattacks?

[3] *I didn't buy one on purpose, because a mistake is easily make and then one's PC is zapped…*



Barton Gellman
@bartongellman

So, um, summit journalists. Do not plug this in. Do not keep it. Drop it in a public trash can or send it to your friendly neighborhood security researcher. Call any computer science department and donate it for a class exercise. I'd be glad to take one off your hands, btw. twitter.com/UID_/status/10…

11:32 PM - Jun 11, 2018

11.1K 5,219 people are talking about t…

Cyrus Farivar
@cfarivar

Journalists at #TrumpKimSummit got this USB fan.

PLEASE PLEASE please don't plug it into a computer. Have an infosec pro (@wmckinley @runasand?) examine it first. twitter.com/UID_/status/10…

9:07 PM - Jun 11, 2018

45 34 people are talking about this

Figure: The gift to journalists from North-Korea

After investigation, the device was found to be harmless. See the report in: https://www.cl.cam.ac.uk/~sps32/usb_fan_report.pdf.

2 Protection procedures

In this chapter, we'll describe various procedures to counter the threats by USB devices. Each has its advantages and disadvantages. Which procedure is the most applicable, depends on the situation and the equipment being used.

Often all USB ports are just disabled. But this is not always a good solution, as it also prevents any data transfers, i.e. for PLC programs, quality reports, firmware updates, etc. If there is no solution offered for these legitimate use cases, staff may resort to work-arounds that may be more dangerous.

Below, I present all possible methods and products I could find that could help, with their advantages and disadvantages.

2.1 Administrative decrees

USB-ports can be left open, but remain unused by administrative decrees forbidding staff to use them, while still allowing their use by special permit to selected persons.

Advantages:

- It is simple to implement, no changes to systems (hardware/software) are needed.

Disadvantages:

- Persons disregarding the rules can still do as they like.
- Hackers will not play by the rules.

Despite the disadvantages, many people will play by the book. It decreases the risk of infection by USB, but not to zero. Additional measures are necessary!

2.2 Disable data lines only

When a USB-port is accessed for charging purposes, it also provides an (unwanted) bidirectional network connection (that's why the connector has 4 pins: 2 for power, 2 for data). For both the owner of the PC and the owner of the mobile device it makes sense to prevent unwanted extraction of data and/or installation of malware. So, the two data-lines of the USB-port need to be disabled.

This can be done hard-wired by cutting the two data-lines in the USB-link. A few minutes of work may suffice, for example see www.instructables.com/id/How-to-make-a-USB-no-data-charger-cable/.

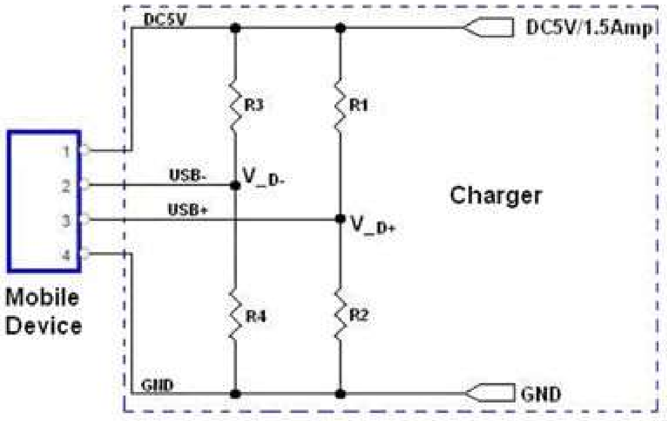


Figure: circuit needed for certain Samsung devices (source: Instructables.com).

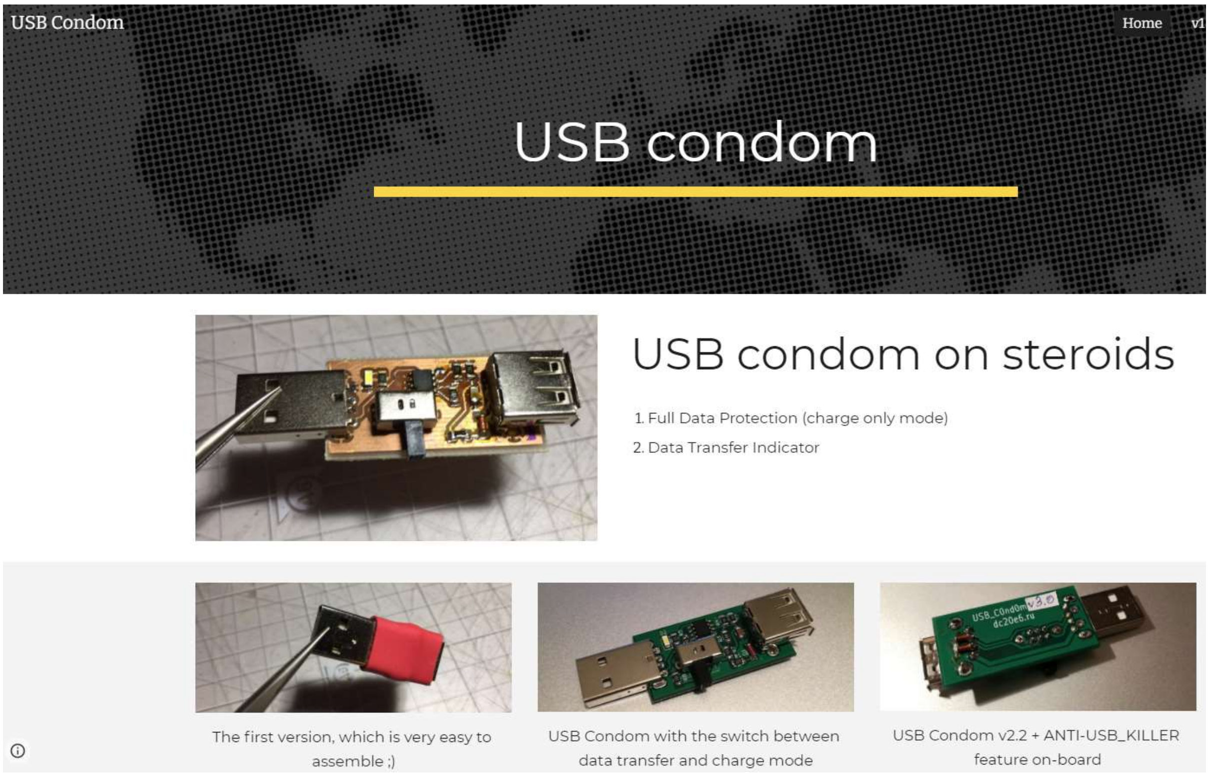
A disadvantage of this solution is that some devices refuse to accept power when the data-lines are not showing any voltage present (i.e., Apple, Samsung). This is because the data lines are used for determining how much power a device can pull from the power source. Some more details on how this works can be found on https://mg.lol/blog/data-blocker-teardown/.

Instead of soldering yourself, a more professional solution is to buy a "Charge-Only" cable, or a so-called "USB Condom", commercially available under names as "SyncStop".

Figure: A "USB Condom" called "SyncStop"

Figure: Similar devices like the SyncStop are now abundantly available. Here's a selection of what is available via Amazon.com

For the electronics buffs, making such a data-blocker device yourself is easy. The website "usbcondom.org" gives instructions and schematics. The version 3 even claims to protect your PC against USB killer devices wanting you fry your PC with a high-voltage pulse.



USB condom

USB condom on steroids

1. Full Data Protection (charge only mode)
2. Data Transfer Indicator

The first version, which is very easy to assemble ;)

USB Condom with the switch between data transfer and charge mode

USB Condom v2.2 + ANTI-USB_KILLER feature on-board

Figure: Three generations of USB condoms

Advantages:

- Good solution for protecting a single device when travelling (i.e. charging a mobile phone in a hotel), or at work (charging at work without giving employer access to your data, or allowing malware from home to be installed on your office-PC).
- It works on any USB-port, even on embedded devices.

Disadvantages:

- The device is not mechanically connected to the USB-port, so can easily be removed.
- It is not a solution for protection of all USB-ports on a PC (one needs too many devices, and they may take up too much space).

Note: many USB chargers will only deliver power when there is a certain voltage detected on the USB "D+" or "D-" signal lines (i.e. 2V for Apple, 3.3V for Samsung). This attempt to create a vendor lock-in, i.e. device can only be charged with a charger from the same vendor, unnecessarily creates problems with the use of some mobile equipment. More information about this subject can be found in the electronics magazine "Elektor" march/april 2018.

2.3 Cut the wires

When the USB-ports are connected to the PCB (PC motherboard) via a separate cable, this cable can be cut with a pair of scissors. This is quite a drastically solution, which cannot be easily reversed. Also make sure than when you cut the cable, the loose end connected to the motherboard does not short-circuit anything against the line carrying the +5V (= the red wire).

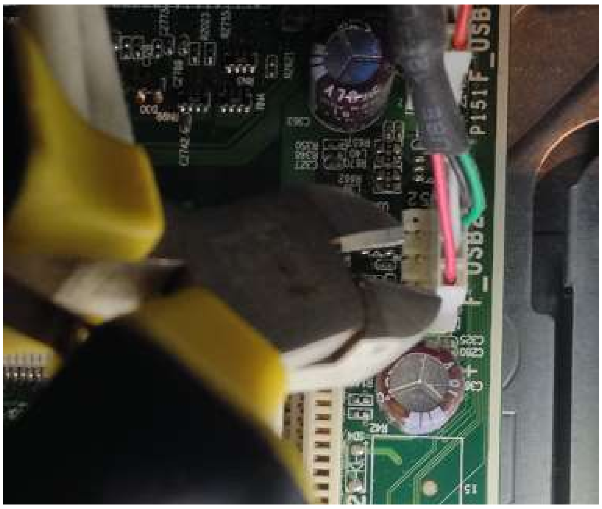


Figure: Cutting the wires leading from the motherboard to the USB connector.

Advantages:

- It cannot be easily undone, the more so since it requires access to the PC cabinet.

Disadvantages:

- It cannot be easily undone.
- Impossible when the USB-port is directly connected to a printed circuit board (as in a laptop, or in many embedded devices).

2.4 Remove all the USB wires

When the cable to the USB-port is connected to the printed circuit board (PC motherboard) via a socket or connector, just remove the cable.

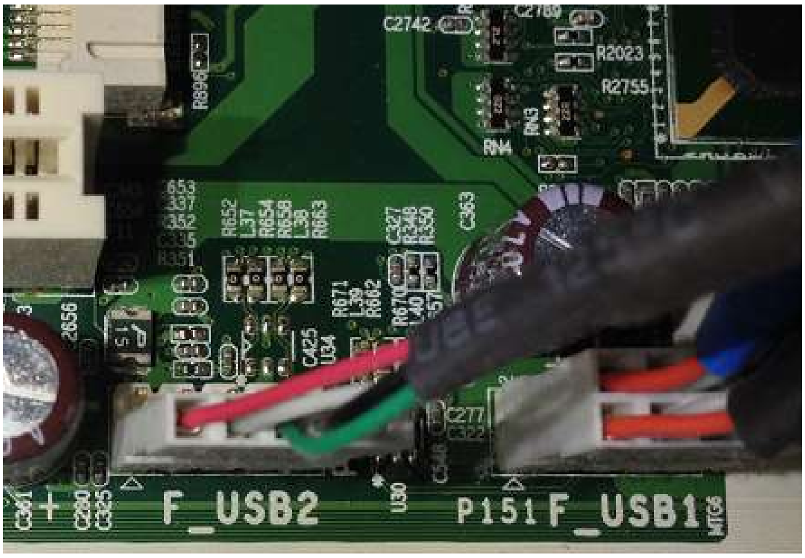


Figure: Two connectors with cables leading to the front USB-connectors in a PC.

Advantages:

- The USB port(s) can be easily reconnected, if necessary.

Disadvantages:

- The cable can be easily plugged in again, which is invisible from the outside (unless the cabinet is opened again).
- Impossible when the USB-port is directly connected to a printed circuit board (as in a laptop, or in many embedded devices).

2.5 Disable USB administratively

Any USB-port requires software to work. This software is usually by default capable of recognizing USB sticks, keyboards, mouses, etc. and when such a device is plugged in, the accompanying "driver" is automatically started. For an ordinary user this makes USB oftentimes "plug and play".

On Windows, USB devices can be disabled via the "Device Manager", often per group (a "hub") of 4 devices. Be careful to not disable the hub on which your keyboard and/or mouse are connected!

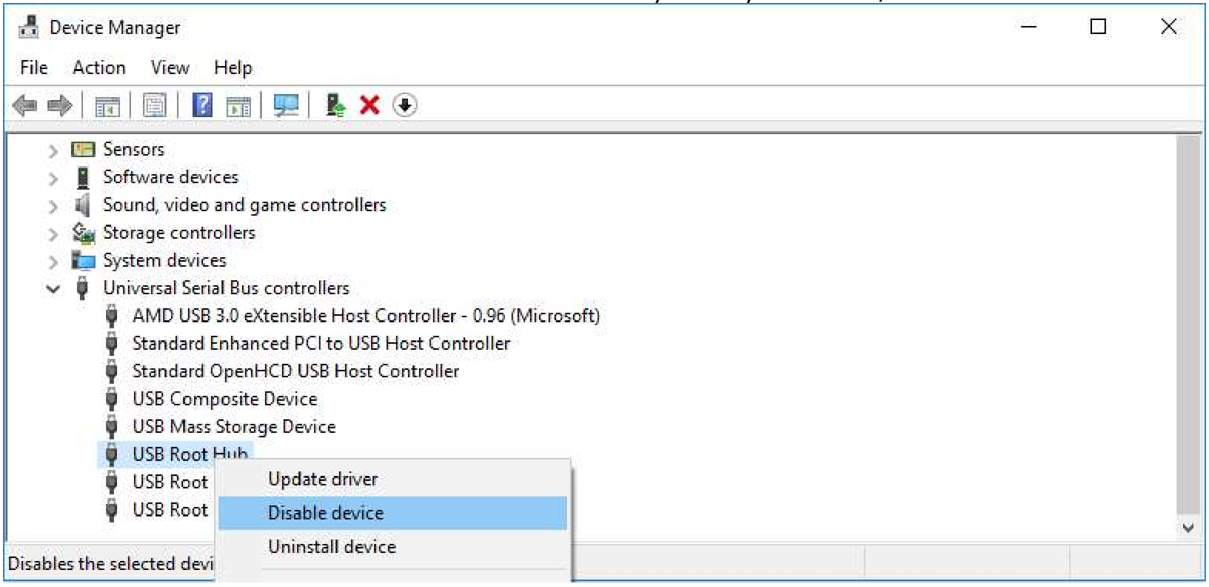

Device Manager
File
Action
View
Help
Sensors
Software devices
Sound, video and game controllers
Storage controllers
System devices
Universal Serial Bus controllers
AMD USB 3.0 eXtensible Host Controller - 0.96 (Microsoft)
Standard Enhanced PCI to USB Host Controller
Standard OpenHCD USB Host Controller
USB Composite Device
USB Mass Storage Device
USB Root Hub
USB Root
USB Root
Update driver
Disable device
Uninstall device
Disables the selected devi

Figure: Disable a USB-hub via Windows' Device Manager.

Advantages:

- Requires "administrator" rights to undo. No problem when you always run as administrator, but in that case you might have serious other cybersecurity problems as well!

Disadvantages:

- A PC on which a user has "administrator" rights can easily enable a USB-hub again. But it can be argued whether running with administrative rights adds more risks to a system than disabling USB.
- Usually cannot be disabled on small/embedded devices.
- Not all ports can be disabled, for example when the hub also has ports on which essential devices are connected (i.e., keyboard or mouse).
- It may not be possible to do this on embedded devices.

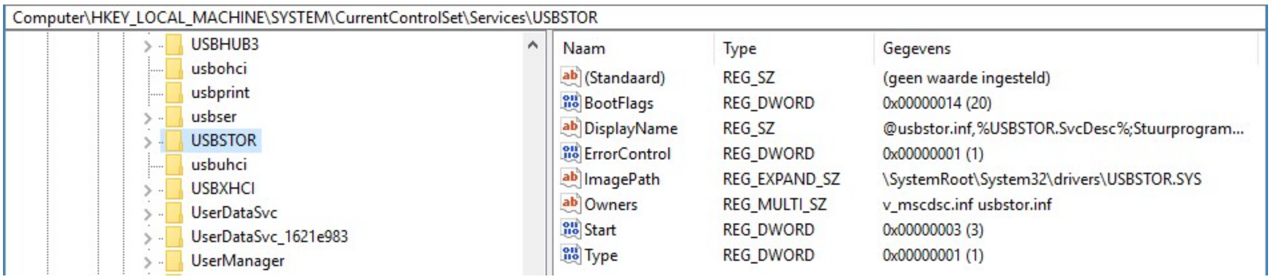
2.6 Disabling USB via the Window registry

Windows has an internal database in which it stores all configuration settings for all its subsystems, so also for USB. It is called "the registry‟ and can be modified with a special tool called "regedit". Using this tool requires more detailed knowledge of how Windows functions, it is not meant for casual users. But it does provide access to all of Windows capabilities, sometimes even to features that cannot be accessed via the standard tools (i.e., the "Device Manager" as described in the previous section).

After starting "regedit", navigate to the folder called:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\USBSTOR
```

You'll see various keys there, one called "Start" with the value 3.



Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\USBSTOR

Naam	Type	Gegevens
(Standaard)	REG_SZ	(geen waarde ingesteld)
BootFlags	REG_DWORD	0x00000014 (20)
DisplayName	REG_SZ	@usbstor.inf,%USBSTOR.SvcDesc%;Stuurprogram...
ErrorControl	REG_DWORD	0x00000001 (1)
ImagePath	REG_EXPAND_SZ	\SystemRoot\System32\drivers\USBSTOR.SYS
Owners	REG_MULTI_SZ	v_mscdsc.inf usbstor.inf
Start	REG_DWORD	0x00000003 (3)
Type	REG_DWORD	0x00000001 (1)

Figure: How to disable USB storage devices via the registry.

Double click on "Start", change the value to 4, and restart the PC. The value 4 means to Windows that the USB drivers should no longer be started.

Advantages:

- It can be scripted, so it can be automated, i.e. every time a PC starts.

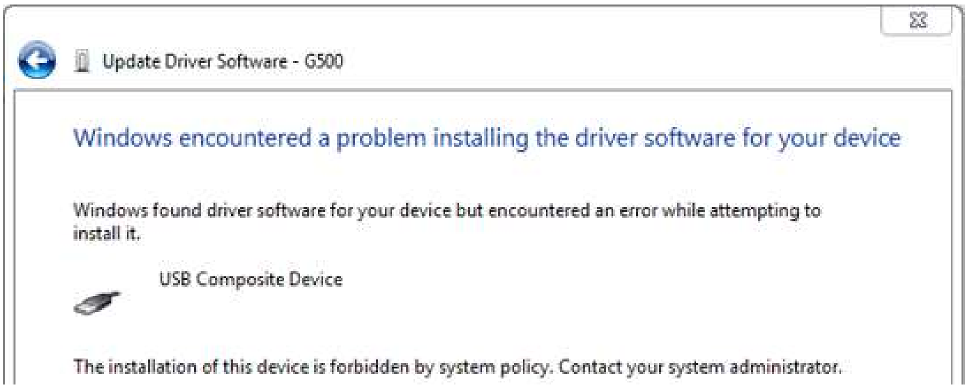
Disadvantages:

- It effects only the "Storage" devices that can be connected to an USB-port. It does not cause mice, keyboards, network interfaces, WiFi access points etc. to be rejected.
- It is not possible on other devices than a PC (but perhaps they have their own solutions).

A disadvantage of this method is that manual modification of the registry can be very dangerous when by accident the wrong data is modified, data is deleted, etc. This is oftentimes not immediately noticeable, but will be when the system is restarted the next time. This is why one is advised to *first* make a back-up of the registry before modifying it. In case you know what you're doing this is not necessary; the author never had any problems with modifying the registry in more than 25 years.

2.7 Group Policy

For Window systems (since Vista) that are part of a domain, a "group policy" can be used to allow (or disallow) the usage of specific types of devices. If a device is not allowed to be installed, a message box like the following may pop up:



Update Driver Software - G500

Windows encountered a problem installing the driver software for your device

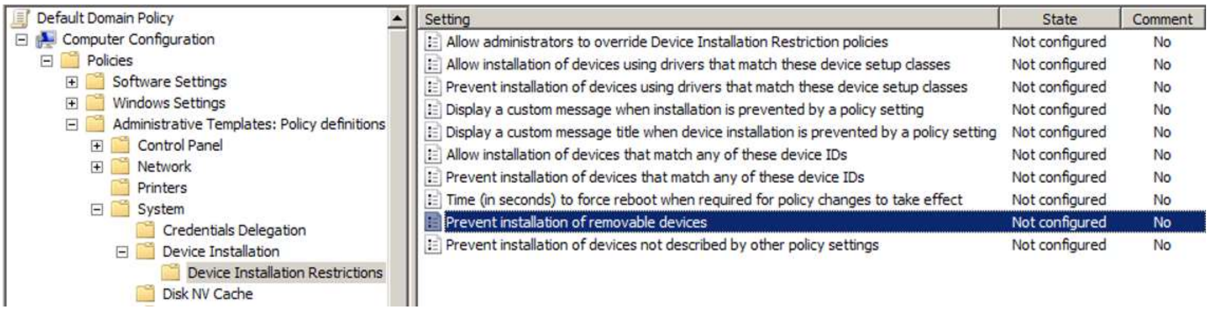
Windows found driver software for your device but encountered an error while attempting to install it.

USB Composite Device

The installation of this device is forbidden by system policy. Contact your system administrator.

Figure: Message that pops up when a device is not allowed to be used

To see which are active, start "gpedit.msc", go to "Computer Configuration", "Administrative Templates", "System", "Device Installation", and finally to "Device Installation Restrictions".



Default Domain Policy
- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
    - Administrative Templates: Policy definitions
      - Control Panel
      - Network
      - Printers
      - System
        - Credentials Delegation
        - Device Installation
          - Device Installation Restrictions
        - Disk NV Cache

Setting	State	Comment
Allow administrators to override Device Installation Restriction policies	Not configured	No
Allow installation of devices using drivers that match these device setup classes	Not configured	No
Prevent installation of devices using drivers that match these device setup classes	Not configured	No
Display a custom message when installation is prevented by a policy setting	Not configured	No
Display a custom message title when device installation is prevented by a policy setting	Not configured	No
Allow installation of devices that match any of these device IDs	Not configured	No
Prevent installation of devices that match any of these device IDs	Not configured	No
Time (in seconds) to force reboot when required for policy changes to take effect	Not configured	No
Prevent installation of removable devices	Not configured	No
Prevent installation of devices not described by other policy settings	Not configured	No

Figure: Where to edit he policy about installation of removable devices

The decision procedure is complex, and described by Microsoft in a 34-page publication named "Step-By-Step Guide to Controlling Device Installation Using Group Policy". It is not very clear that the policies only apply to storage devices (at least, I could not find otherwise).

Clean up first!
Note that Group Policies (GPO) only prevent the installation of devices, not their use. So it is necessary to remove evidence of all earlier installed devices, otherwise their use remains allowed despite any new GPO settings.

Advantages

- Can be centrally enforced inside an organisation.

Disadvantages

- Not applicable for "home" licensed Windows versions.
- It effects only the "Storage" devices that can be connected to an USB-port. It does not cause mice, keyboards, network interfaces, WiFi access points etc. to be rejected.
- It is not possible on other devices than a PC (but perhaps they have their own solutions).
- A GPO setting can be made to disallow keyboards, but then how does one use the computer? This leaves a hole in the protection of a PC enough to modify GPO settings.

The policy can be set differently for users running as administrator, according to the following flowchart.

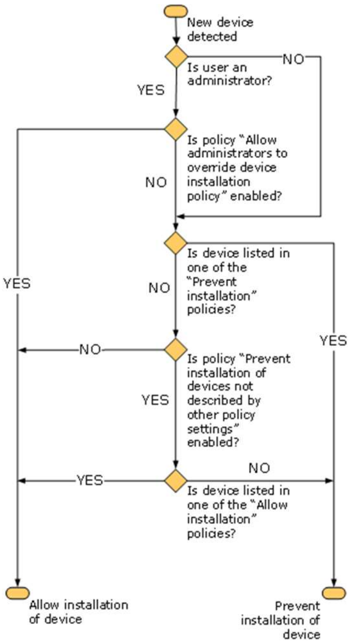
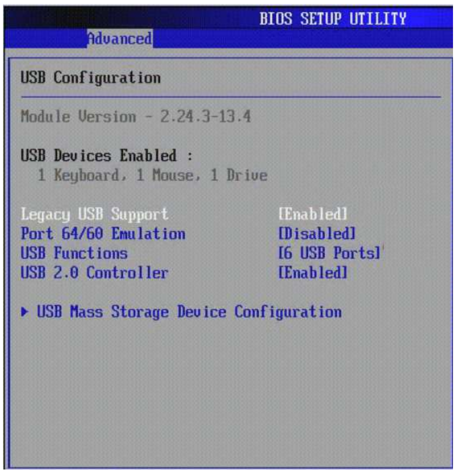

New device detected
Is user an administrator?
NO
YES
Is policy "Allow administrators to override device installation policy" enabled?
NO
YES
Is device listed in one of the "Prevent installation" policies?
NO
YES
Is policy "Prevent installation of devices not described by other policy settings" enabled?
NO
YES
Is device listed in one of the "Allow installation" policies?
YES
NO
Allow installation of device
Prevent installation of device

Figure: Administrator-users can be handled differently, or not (source: Microsoft).

An easier-to-read explanation of the procedure can be found on: symmetrixtech.com/articles/005-usb-lockdown.pdf.

2.8 Disable USB via a BIOS setting

In some BIOS / UEFI(like AMI / American Megatrends Inc.) there is a configuration option to enable / disable *all* USB ports. Check the user manual of your laptop / PC for the availability of such configuration options.



```
USB Configuration

Module Version - 2.24.3-13.4

USB Devices Enabled :
  1 Keyboard, 1 Mouse, 1 Drive

Legacy USB Support             [Enabled]
Port 64/60 Emulation           [Disabled]
USB Functions                  [6 USB Ports]
USB 2.0 Controller             [Enabled]

▸ USB Mass Storage Device Configuration
```

Figure: Disabling USB via a BIOS configuration setting

Note! If your computer has a USB keyboard, it will not work anymore and you cannot modify the BIOS setting back. Probably the BIOS must be reset; how exactly this must be done differs per type of computer (i.e. pressing a switch on the motherboard, short-circuiting two pins on a chip, pressing DEL-INS keys while powering up the computer, or F12-ENTER-INS, etc.).

Advantages

- Only for PC's and laptops, not for other devices with USB

Disadvantages

- Manual action per device is very time-consuming.
- A reboot is needed.

2.9 Prevent USB devices to be plugged in

Physical protection measures, disallowing any type of device to be plugged in, are available on the market. Usually they just physically occupy the free space of the USB-port, secured with a screw or notch that can be locked/unlocked with a special tool.

Figure: Two examples of tools to physically prevent a device or cable to be inserted in a USB-port.

A company known for selling all sorts of port-blockers (not only for USB, but also for RS232 / COM-ports, VGA, HDMI, Ethernet RJ45) is "SmartKeeper".

Figure: USB blocker from SmartKeeper, and the accompanying insertion/extraction tools.

USB blockers cost around $2 each (price January 2024). If you find this too expensive, a solution is to make them yourself, if you have a 3D-printer available. Designs for this are available via internet. Within a few hours, you have hundreds of them.

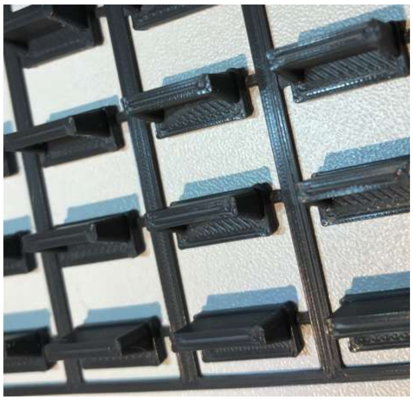


Figure: home-printed USB blockers

They worked very well, but I could not get them out any more (and there is no extraction tool !), since they fit very snugly in the USB.

Removal of a USB blocker without having an extraction tool at hand is possible, since the USB blocks is only kept in place via friction. With a small screwdriver and some effort the USB blocker can sometimes be removed. I tried this myself on a (yellow) SmartKeeper blocker, and within a few minutes I got it out, however the USB port got slightly damaged.

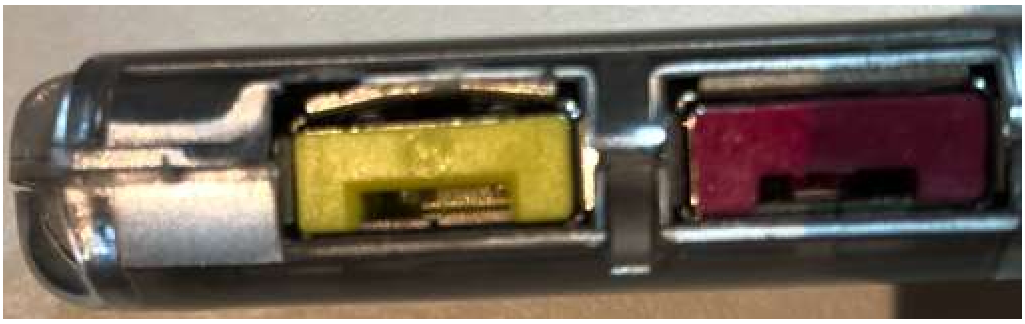


Figure: damaged USB port after removal of the yellow blocker with a screwdriver.

Advantages:

- Cheap.
- Simple, works on any USB-port.
- Easy to install.
- Allows laptop protection while in-transit.

Disadvantages:

- Can be removed by a determinate hacker.
- Not available (yet) for mini-USB ports.
- Removal without special tool may be difficult, or cause damage to USB-port.
- Removal of a lock goes unnoticed / undetected.

Removal of some brands of port blocks is impossible by extra physical measures:

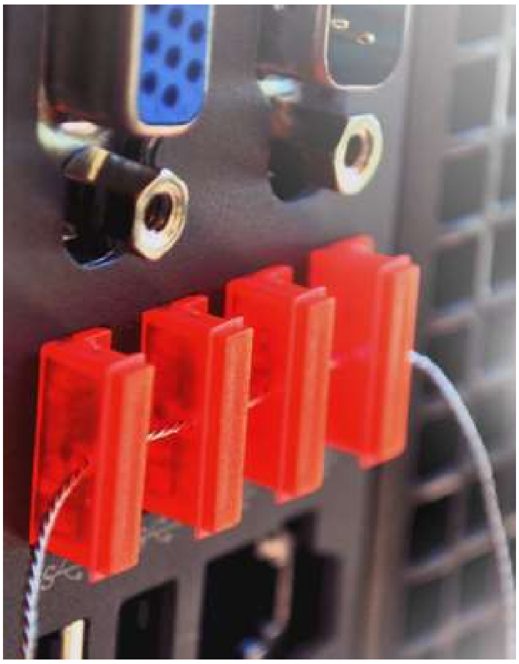


Figure: A "Padjack USB-lock" protected against removal (source: www.padjack.com).

In case you want to be notified when a USB lock is removed, simple physical measures are not enough. The company "HighSecLabs" has USB locks named "ELock" that contain an internal chip which allows software to detect that it is present, or has been removed, in which case an alert can be given. Removal of the ELock is made as difficult as possible.

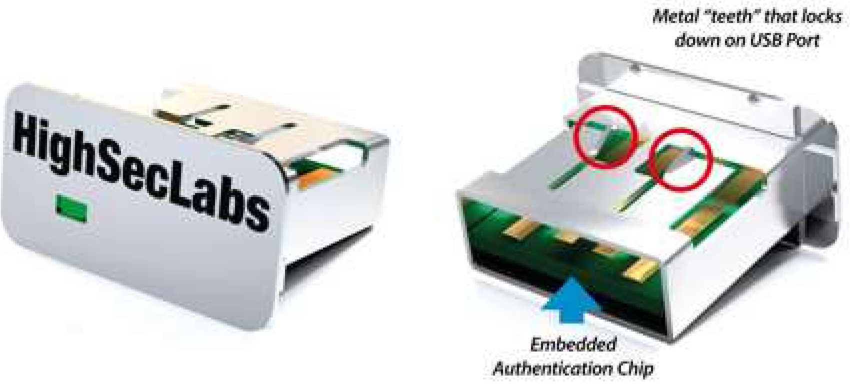

HighSecLabs
Metal "teeth" that locks down on USB Port
Embedded Authentication Chip

Figure: The HighSecLabs "ELock" device.

2.10 Use a "data diode"

A "data diode" is a device that is inserted in a network cable. Whereas a normal diode lets current pass in one direction but blocks it in the other direction, a data diode does the same but with data: data may flow in one direction, but not in the other direction.

Data diodes are available for networks like Ethernet from several suppliers. There is one supplier that sells a USB data diode: CRU-inc.com.

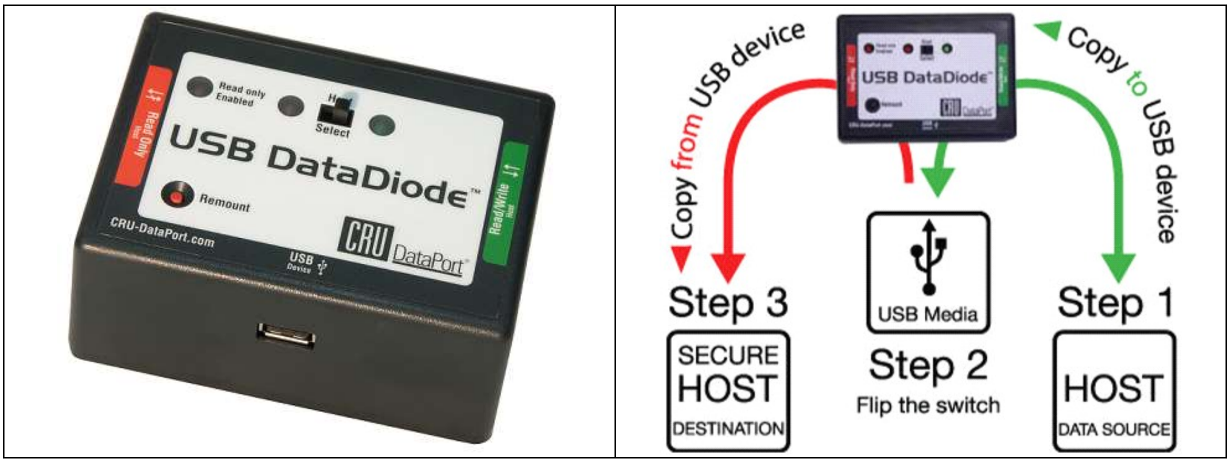


Figure: The CRU data diode (left), and its use (right).

Via the data diode, it is impossible to transfer data from the "red" connection to the "green" connection, while it is still possible to receive data. This is typical for use in a facility (i.e. military) where secrets may not be copied out. In an industrial facility, the secure side would be the "green" connection – data may be transferred out, but no malware is to be allowed in.

A product that looks like it is the "USB Write-Blocker". It allows a USB-drive or hard disk to be connected to a computer in "read-only" mode. Typically, this is used in forensic investigations, but may also help in other cases.

Advantages:

- Substantially cheaper than Ethernet data diodes.
- Data can still flow out of an industrial facility.

Disadvantages:

- Only useable for storage devices.
- Requires manual operation.
- The software in the data diode must be trusted to work.
- Expensive to protect multiple ports on a device.

Figure: A Wiebetech "USB Write-Blocker"

2.11 Install USB-stick detection

Instead of just forbidding USB-sticks to be used, it is better to *manage* its use. Various solutions exist that check USB-sticks for malware entering (or leaving!) a facility, while still allowing employees to transfer data per USB-stick.

Blue Coat

One such tool to protect PC's against malware on USB memory sticks is "Blue Coat". Before a USB stick can be connected to a PC, it must first have been scanned on a "Scanner Station". When there is no malware detected, the USB stick is "checked in" and can then be connected to a PC, where it can be used in the normal way. USB sticks that do not pass the scanner station can (of course) still be connected to the PC, but a special (kernel-mode) driver detects this, and will not allow the USB stick to be accessed.

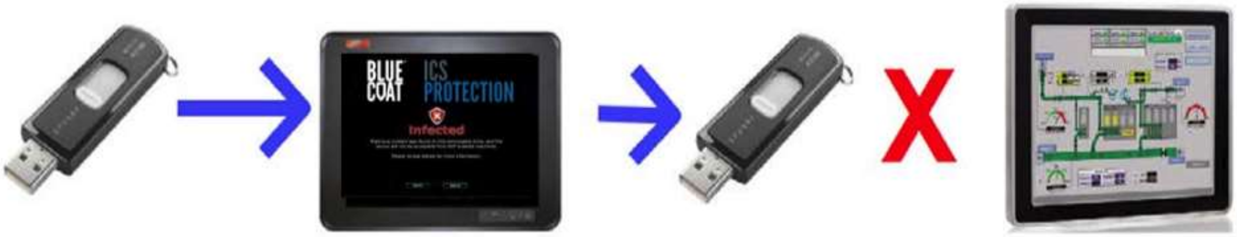


Figure: Operation of the "Blue Coat" protection suite.

SMX

Another tool that does this is "SMX" (Secure Media Exchange) by Honeywell. It also scans a USB memory stick for malware via a cloud-based platform which is always up-to-date with the latest malware signatures and virus definitions. When the USB stick is checked in, it can be connected to a PC, where (via special software) it is checked that this stick is allowed to be used. When finished, the USB stick is checked again, this time for malware *leaving* the facility.

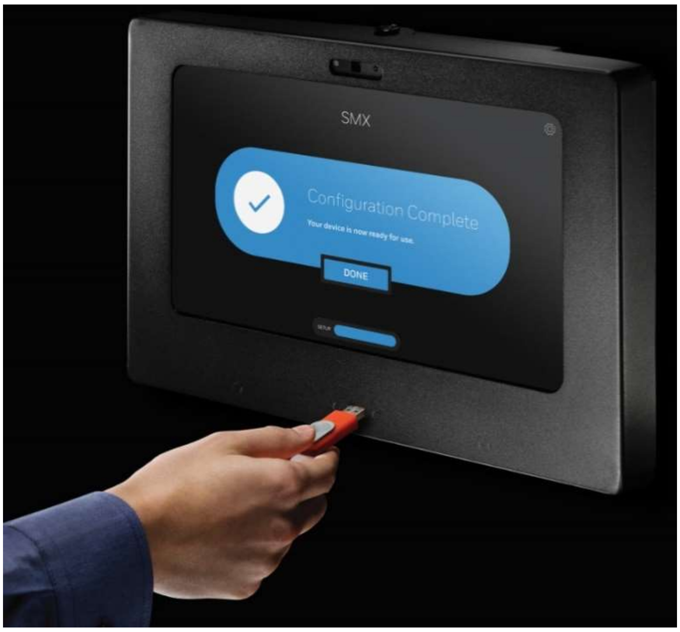


Figure: The Honeywell "SMX" solution.

Because checking large USB sticks may take quite some time, it is possible to not check files that are not needed. These are then put in "quarantine" and cannot be used on a PC. After checking out, these files can be used again.

Advantages:

- No reliance on PC's being updated with the latest malware.
- Central logging and reporting of scanned USB-sticks and detected malware.
- Also detects memory mice.

Disadvantages:

- Expensive.
- Scanning may take a while.
- All PC's must have the special software installed.
- Only usable on PC's running Windows.

In November 2018, Honeywell released an extensive report about the malware that were detected at 50 customers world-wide.

USBNinja

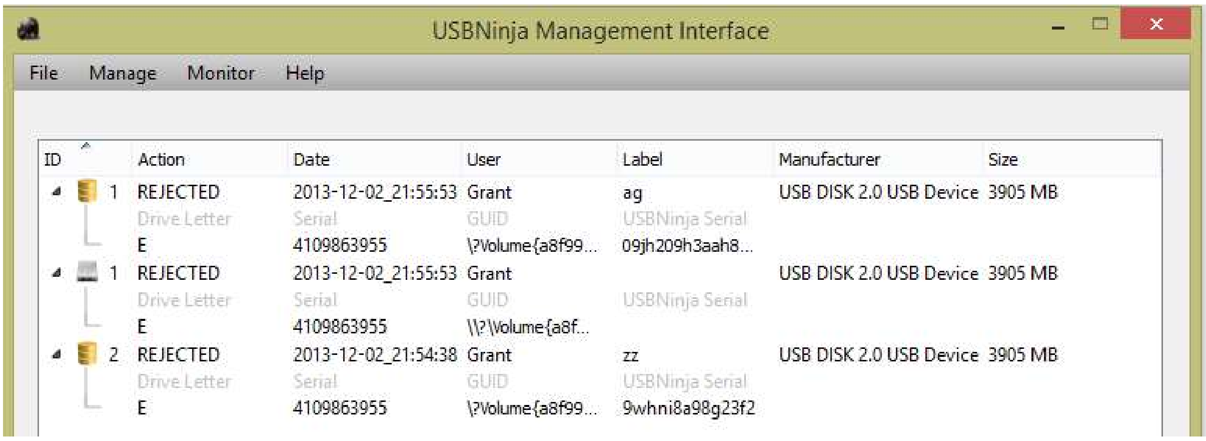
There is also an open-source solution called "USBNinja" (not to be confused with the USBNinja attack cable described in chapter 2). The source-code is available at github.com/gfoudree/usbninja so you can verify the code to verify it doesn't contain any harmful code, and the documentation at http://usbninja.weebly.com. With this software you can configure which USB-stick is allowed on which PC. In addition, each device plugged in is logged with a time-stamp. Data leaks and computer infection can be matched with the logs to reveal the culprit. Administrators can authorize as many or as little drives as they choose. All non-authorized drives are blocked by default.

Advantages:

- Free (GPL License).
- Logging feature.
- Source code available.

Disadvantages:

- Meant for small-scale installations, or for use at home.
- All PC's must have the special software installed.
- Only usable on PC's running Windows.



ID	Action	Date	User	Label	Manufacturer	Size
1	REJECTED	2013-12-02_21:55:53	Grant	ag	USB DISK 2.0 USB Device	3905 MB
	Drive Letter	Serial	GUID	USBNinja Serial		
	E	4109863955	\?Volume{a8f99...	09jh209h3aah8...		
1	REJECTED	2013-12-02_21:55:53	Grant		USB DISK 2.0 USB Device	3905 MB
	Drive Letter	Serial	GUID	USBNinja Serial		
	E	4109863955	\\?\Volume{a8f...			
2	REJECTED	2013-12-02_21:54:38	Grant	zz	USB DISK 2.0 USB Device	3905 MB
	Drive Letter	Serial	GUID	USBNinja Serial		
	E	4109863955	\?Volume{a8f99...	9whni8a98g23f2		

Figure: Example of USBNinja Management Interface.

2.12 Firewalls

Firewalls are products that are typically associated with Ethernet, but there is also a USB firewall on the market: the "USG" from Robert Fisk (github.com/robertfisk/USG/wiki). You can buy one for NZ$ 80, or build one of your own.

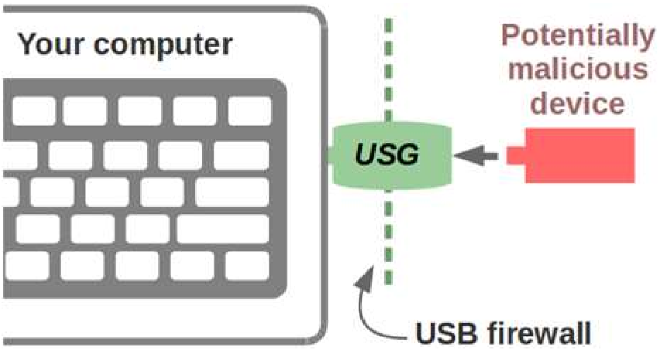


Figure: The firewall sits between a PC and a USB device

Internally, the firewall contains two CPU's that communicate with each other over a high-speed serial connection. This limits the achievable USB-speed to 12 Mbit/s. It recognizes mice, keyboards and memory sticks.

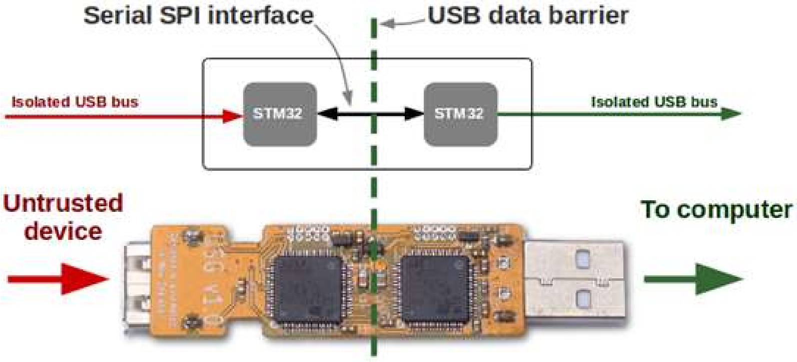


Figure: Internal structure of the firewall

The serial protocol between both CPU's only recognizes a limited number of safe commands, so all other commands are blocked. Additionally, the firewall will only support one USB device at a time. This stops USB devices which change their functionality, i.e. a memory stick which will suddenly also appear to be a keyboard.

On GitHub, all the source code is available, so you can experiment with the firewall yourself. And for the hardware: you can buy one from the developer, but also use readily available development boards. See the Wiki page for more information.

A commercial version is called "Armadillo", which sells for NZD $249 from https://globotron.nz:

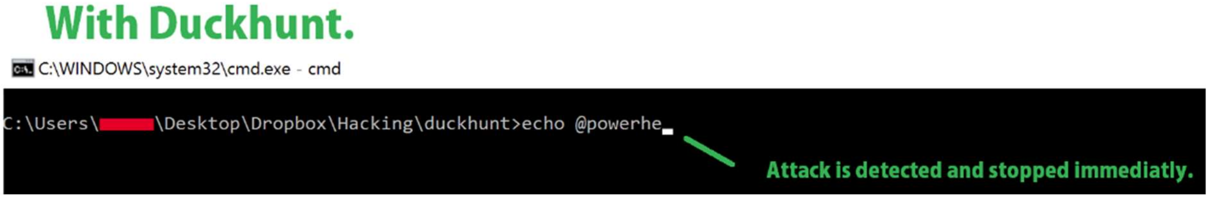
Figure: The "Armadillo" firewall

Advantages:

- May work on any controller, not only PC's.
- Open source.
- Nice for hobbyists.

2.13 Detect Rubber Duckies (and similar)

Although Rubber Duckies (and similar devices) cannot physically be detected, there are other methods. One is "Duckhunt", a Python script for Windows that tries to detect a ducky attack by timing the interval between key presses – if it is too fast (faster than a human could physically type), keyboard input is blocked and restored only after entering a password. Exactly what is "fast" can be configured in the script.



With Duckhunt.

C:\WINDOWS\system32\cmd.exe - cmd

```
C:\Users\[redacted]\Desktop\Dropbox\Hacking\duckhunt>echo @powerhe_
```

Attack is detected and stopped immediatly.

Figure: Duckhunt script in action

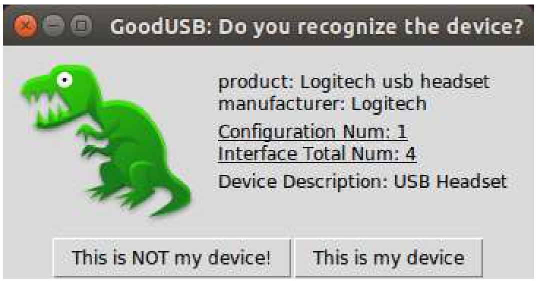
Of course, an attacker could make that a Rubber Ducky attack simulates keystrokes in the same rate as a human would type, which makes Duckhunt not infallible.

More info on: https://github.com/pmsosa/duckhunt

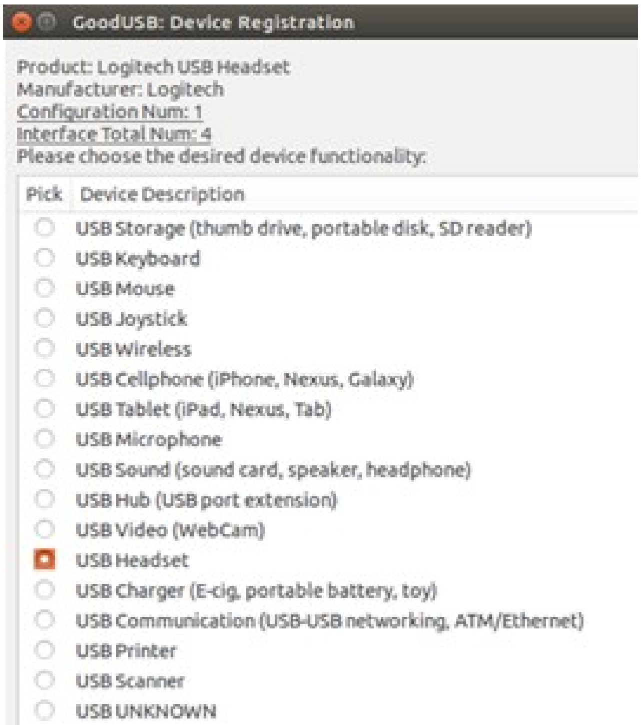
2.14 Detect all types of USB devices

A completely different way of keeping USB devices in check is to install additional software (on a PC) that detects (new) devices becoming active, and intercepting their installation. Various solutions exist on the market.

Example 1
The ability to detect all types of USB devices is not easily solved with standard software (such as Windows). The paper "Defending against malicious USB firmware with GoodUSB" (www.cise.ufl.edu/~butler/pubs/acsac15.pdf) describes the theoretical aspects and proposes a software solution, called "GoodUSB".



product: Logitech usb headset
manufacturer: Logitech
Configuration Num: 1
Interface Total Num: 4
Device Description: USB Headset



Product: Logitech USB Headset
Manufacturer: Logitech
Configuration Num: 1
Interface Total Num: 4
Please choose the desired device functionality:

Pick	Device Description
○	USB Storage (thumb drive, portable disk, SD reader)
○	USB Keyboard
○	USB Mouse
○	USB Joystick
○	USB Wireless
○	USB Cellphone (iPhone, Nexus, Galaxy)
○	USB Tablet (iPad, Nexus, Tab)
○	USB Microphone
○	USB Sound (sound card, speaker, headphone)
○	USB Hub (USB port extension)
○	USB Video (WebCam)
●	USB Headset
○	USB Charger (E-cig, portable battery, toy)
○	USB Communication (USB-USB networking, ATM/Ethernet)
○	USB Printer
○	USB Scanner
○	USB UNKNOWN

Figure: GoodUSB asks the user to decide whether a device is OK or not.

Unfortunately it is not a product available on the market. For Linux, an implementation is available on github.com/daveti/GoodUSB. More about this and firewall-like software ("usbtables") on www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/tian.

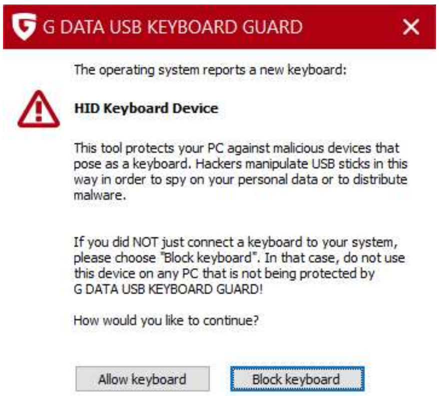
Example 2
An example of software for Windows to intercept USB devices is the program "Beamgun.io", that comes as freeware. Personally I haven't tried it as my virus scanner didn't like it, but since source code is also provided, you can check the implementation and compile it yourself (there is never a guarantee that an executable on a website is built from the source code, so the only way to be sure it compile it and then install *that* executable). Beamgun works by redirecting keyboard input to itself, and locking the PC after some time.

Figure: Beamgun is freeware for use under Windows.

The Beamgun software is great for protecting a single PC, but not for use in large installations. It also has no reporting feature. When not running under administrator privileges, it cannot be used to disable USB network adapters (this is a limitation of Windows).

Example 3
Yet another program to protect a (Windows) PC against rogue keyboards is DuckHunt. It monitors the speed with which keystrokes are normally entered, and when suddenly keystrokes are entered at a much higher rate, it blocks them. An explanation of how it works can be read on http://konukoii.com/blog/2016/10/26/duckhunting-stopping-automated-keystroke-injection-attacks/.

Example 4
A product to protect against USB devices masquerading as keyboard is G-Data's "USB Keyboard Guard". Upon detecting a new 'keyboard', the software asks you whether it is really a keyboard and is to be trusted, or whether it is not a keyboard and must not be allowed access to the system. Additionally, newly detected USB-sticks can also be stopped in their tracks. It is free, and works independent of any virus scanner.



G DATA USB KEYBOARD GUARD

The operating system reports a new keyboard:

HID Keyboard Device

This tool protects your PC against malicious devices that pose as a keyboard. Hackers manipulate USB sticks in this way in order to spy on your personal data or to distribute malware.

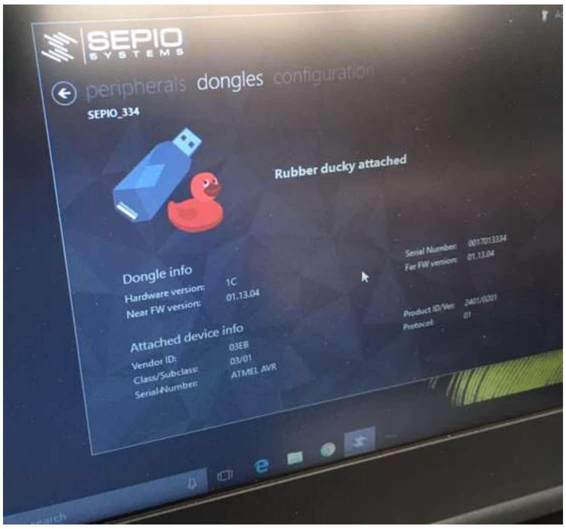
If you did NOT just connect a keyboard to your system, please choose "Block keyboard". In that case, do not use this device on any PC that is not being protected by G DATA USB KEYBOARD GUARD!

How would you like to continue?

Figure: The free tool "USB Keyboard Guard" from G-Data detects USB keyboards and asks whether to block them or not.

Of course I tried it out with the devices of chapter 1 which masquerade a keyboard, and the software correctly detected them. A *real* USB keyboard was also detected, but the keyboard logger was not.

Example 5
A professional product designed to detect (and possibly block) any sort of USB device is the product of Sepio Systems. It is designed to be installed and managed company-wide. It has a "threat dashboard" to monitor what is going on, showing all connected devices and their capabilities and behavior.



SEPIO_334

Rubber ducky attached

Dongle info
Hardware version: 1C
Near FW version: 01.13.04

Attached device info
Vendor ID: 03EB
Class/Subclass: 03/01
Serial Number: ATMEL AVR

Serial Number: 0017013334
Far FW version: 01.13.04

Product ID/Ver: 2401/0201
Protocol: 01

Figure: A message pops up on the Sepio Systems dashboard.

The product identifies (and subsequently blocks) malicious hardware devices before they damage normal operations. This is based on whitelist rules, i.e. only devices on the list are allowed access. Devices not mentioned in the whitelist are blocked, and reported to any SIEM (Security Information and Event Management) tool.

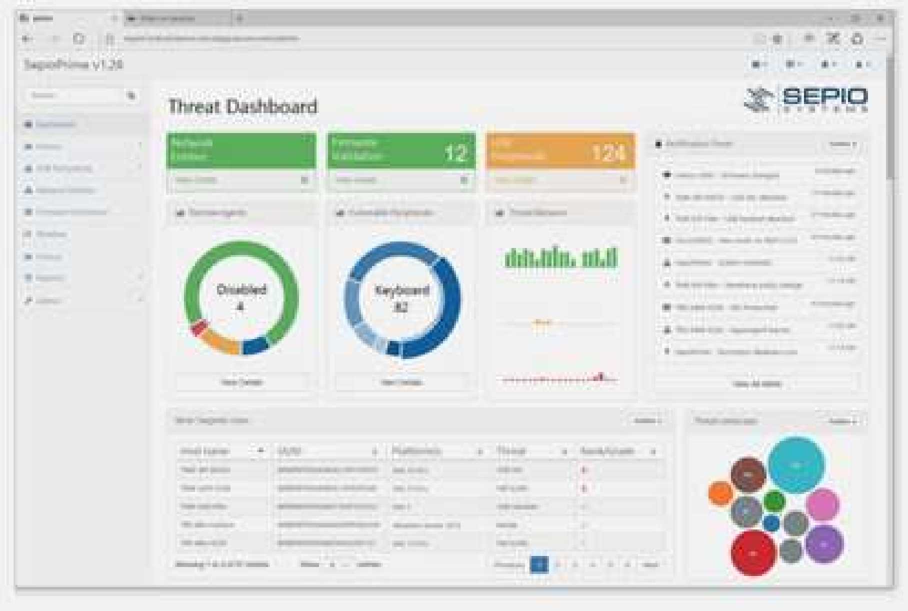


Figure: The Sepio Systems dashboard.

Example 6
The company "DeviceLock" has a product called "DeviceLock Endpoint DLP Suite" which is designed to prevent corporate data leaking out of the network, laptops, or devices in a lot of different ways, and USB is one of them. USB devices that are allowed to be used are put on a "white list"; any device not on this list is locked.

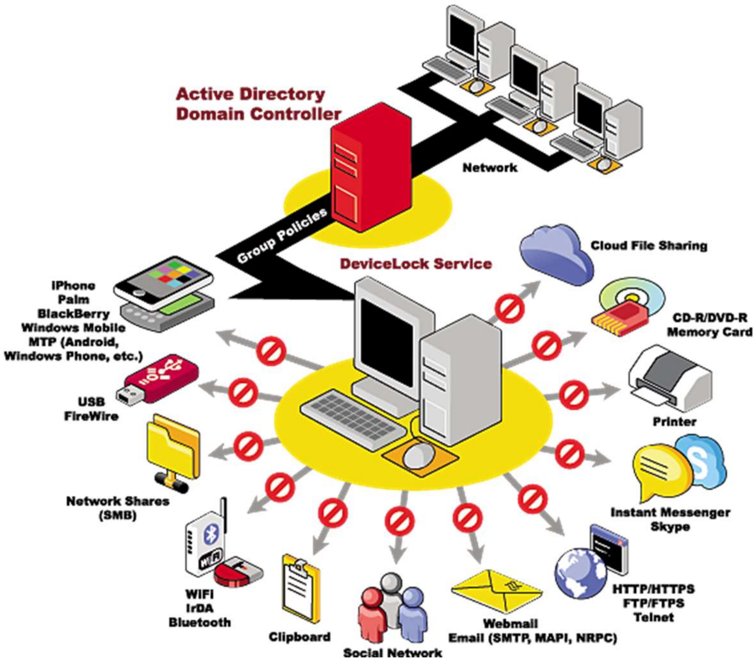
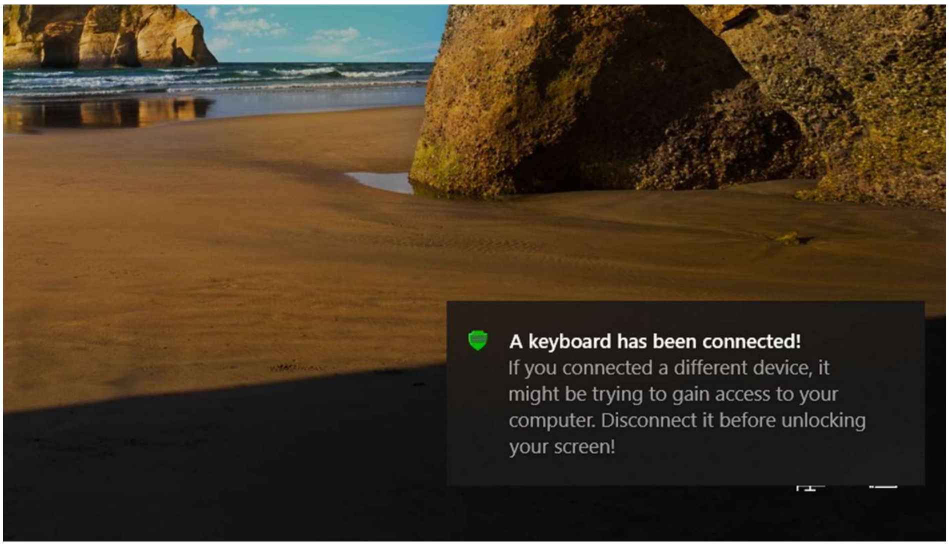


Figure: The capabilities as offered by DeviceLock's product (source: DeviceLock).

Example 7
The "Penteract Disguised-Keyboard Detector" software protects your (Windows) PC from malicious keyboard disguised as other USB devices. When such a device is seen, Penteract will lock the PC automatically and warn you. The software is free but only runs on Windows 10 (https://penteract.net).



A keyboard has been connected!
If you connected a different device, it might be trying to gain access to your computer. Disconnect it before unlocking your screen!

Figure: Penteract in action (source: Penteract).

Example 8
The French company KUB Cleaner has launched its "Kiosk for Universal Blocking" workstation in 2021, helping to analyse and decontaminate USB devices. On PC's an agent is running which blocks USB devices that have not been validated by the KUB Cleaner workstation.

Figure: The KUB Cleaner workstation.

For more info, see www.kub-cleaner.com/.

Example 9
The Israeli company OPSWAT has a suite of solutions to authenticate a user, audit / detect / control and sanitize data before it enters (of leaves) a secure network. From the "MetaDefender Kiosk", which accepts memory device but also MicroSD and CompactFlasgh cards, CDROMs, DVD's and even 3.5"diskettes, files can be transferred via datadiodes to/from a "Metadefender Vault" in the secure network, which can be accessed by devices in the secure network.

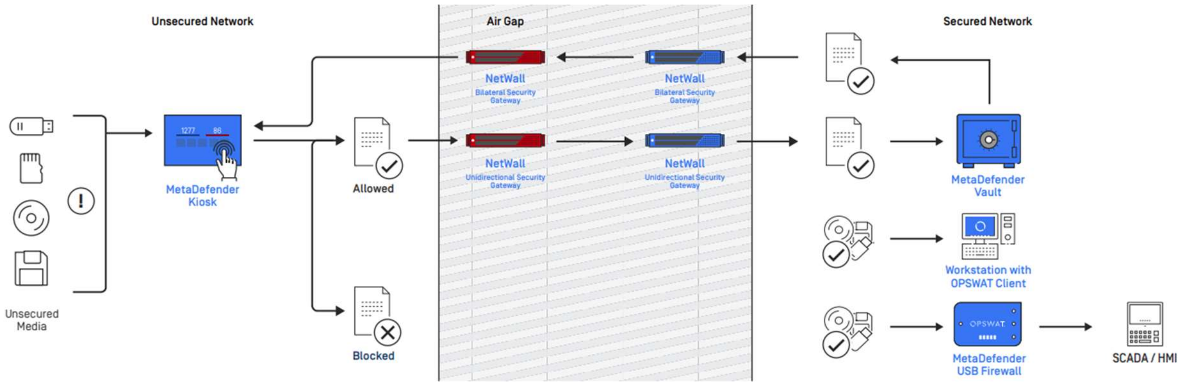

Unsecured Network
Unsecured Media
MetaDefender Kiosk
Allowed
Blocked
Air Gap
NetWall
Bilateral Security Gateway
NetWall
Bilateral Security Gateway
NetWall
Unidirectional Security Gateway
NetWall
Unidirectional Security Gateway
Secured Network
MetaDefender Vault
Workstation with OPSWAT Client
MetaDefender USB Firewall
SCADA / HMI

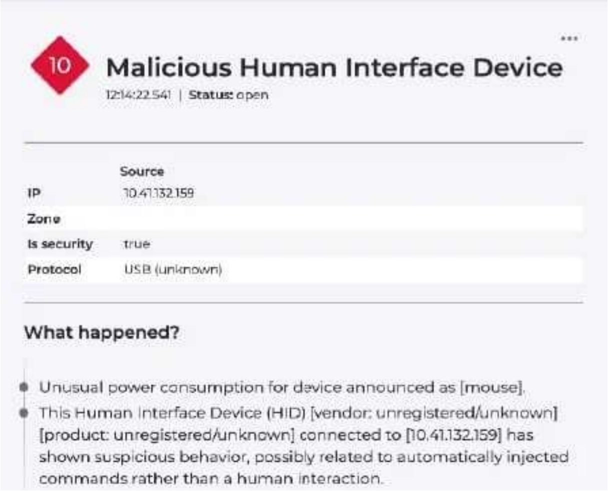
Figure: MetaDefender architecture.

Alternatively, a "MetaDefender USB Firewall" can be used for securing SCADA / HMI terminals.

MetaDefender™
USB Firewall
USB
SCADA/HMI
OPSWAT

Figure: The MetaDefender USB firewall

Example 10
The Nozomi Networks' "Arc" has a novel method of detecting malicious USB devices, i.e. by distinguishing keyboard devices based on typing speed, keystrokes, and usage of blacklisted/whitelisted words and sentences, or by excessive current usage. Arc runs on Windows, MacOS or Linux.



10 **Malicious Human Interface Device**
12:14:22.541 | **Status:** open

	Source
IP	10.41.132.159
Zone	
Is security	true
Protocol	USB (unknown)

What happened?

- Unusual power consumption for device announced as [mouse].
- This Human Interface Device (HID) [vendor: unregistered/unknown] [product: unregistered/unknown] connected to [10.41.132.159] has shown suspicious behavior, possibly related to automatically injected commands rather than a human interaction.

Figure: Detecting malicious USB "HID" devices (source: Nozomi)

This article is likely not complete in describing all possible USB protection measures. If you have any suggestions, comments or additions, please do not hesitate to contact me (email: rh[at]enodenetworks.com).