Honeywell | Industrial Cybersecurity

# USB Security – Myths vs. Reality

*Latest USB Security Threats & Best Practices to Follow*

USBs continue to be one of the most convenient ways to share and update files, but they can be a serious security threat. Learn more about the latest threat, myths and best practices related to USBs.

White Paper

# Table of Contents

## Introduction

An estimated 9 out of 10 maintenance engineers still use Universal Serial Bus (USB) as they connect to targeted plant machines (Honeywell research 2019). Despite the advent of the Internet, and innovations such as the cloud and even SD-WAN, why do personnel still rely so heavily on removable media and external hardware, such as USB flash drives?

- Industrial Enterprises still require USBs for several reasons:
  - Not all sites/plants are connected
  - USB may be the only way to get updates from certain vendors
  - Ease of use. People gravitate toward the path of least resistance, and quickest success
  - Banning USBS as a policy has proven ineffective.

## What makes USBs such a successful attack vehicle?

Much of the fiction surrounding cyber-attacks and espionage features hoodie-wearing teenage hackers fueled by caffeinated sodas and pounding away at their keyboards. In reality, the most successful cyber-attacks target people and their behavior rather than directly hacking of systems.

Why? Because it's far easier and much more lucrative to exploit risky behaviors inside of a company, than it is to hack past numerous firewalls and security systems from outside of a company, without arousing suspicion.

Since people are rather predictable and USB sticks are ubiquitous, they combine to create a very successful attack vector. Here's how.

1. USBs are so convenient to carry around and easy to use, most people tend to disregard their potential as a catastrophic security risk.
2. It's not always what you think! There is a plethora of seemingly innocuous devices that connect to a USB port for power. USB-based attacks are not limited to storage drives. Phone chargers, vape chargers, USB fans and any device with a USB can become a threat vector.
3. People have a tendency to just plug them in. Researchers at the University of Illinois and University of Michigan found that a discarded USB stick has a nearly 50% chance of getting picked up by someone who will plug it into a computer and start clicking around inside.
4. A USB may be compromised long before it reaches the hands of a plant employee or third-party engineer. For example, just last year, it was reported that infected USBs may have inadvertently shipped to customers by an equipment vendor.

## USBs - Past and Future Threat

ICS-CERT has long maintained that the USB attack vector is a considerable and ongoing threat. "Owner operators are also cautioned that USB drives have been involved in many cases involving the loss of sensitive information. Their small size and increasingly high storage capacity has been instrumental in the loss of or theft of sensitive information". ICS-Cert underlines that the risk is not isolated to enterprise corporate networks. USBs pose a considerable risk to ICS and OT networks.

"It is important to emphasize to control system owners and operators that this attack vector can threaten control system networks just as easily as enterprise networks," warns ICS-CERT. "Due to the increasing reliance on commercial-off-the-shelf software and operating systems in control systems networks, ICS-CERT believes that USB thumb drives represent a significant malware attack vector for control system owners' networks"

According to the latest Honeywell research, USBs remains a significant threat vector. The inaugural Honeywell Industrial USB Threat Report found that, "Of the locations studied, nearly half (44%) detected and blocked at least one malicious or suspicious file that represented a security issue. This high-level finding confirms that USB remains a significant vector specifically for industrial threats. The data also indicates that risk of industrial facility exposure to threats via USB is consistent and statistically relevant.

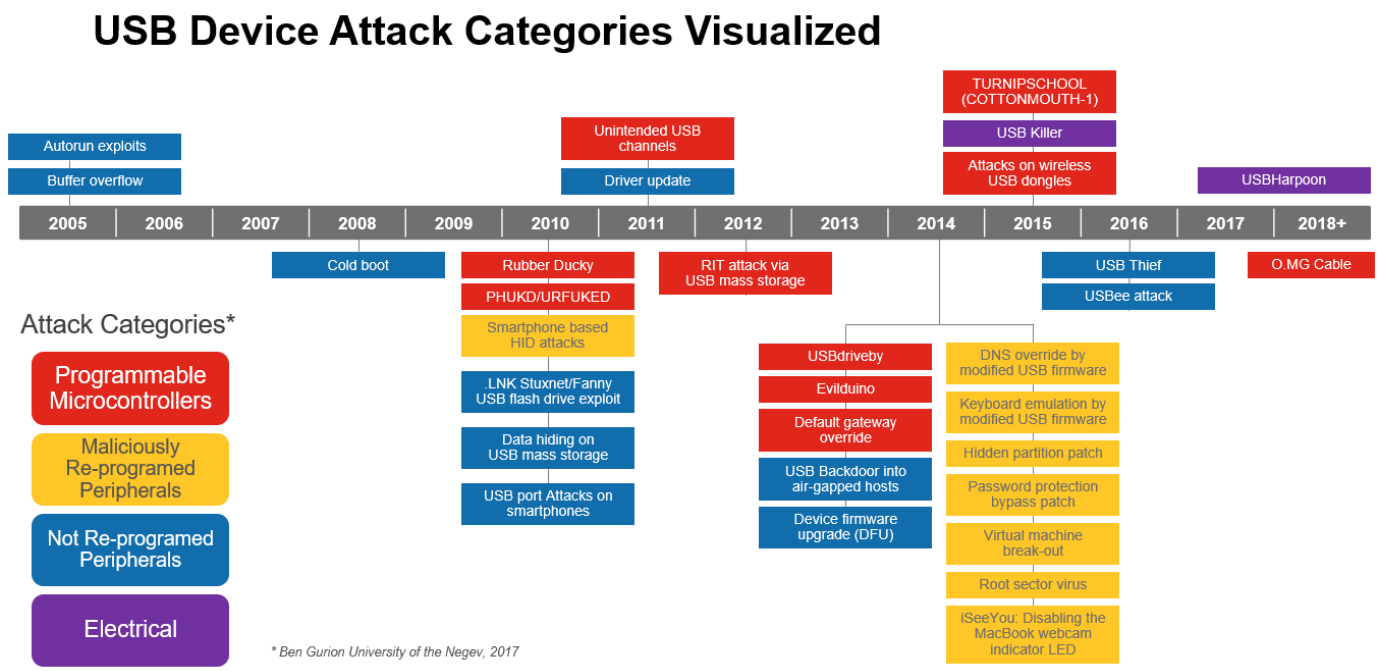



*Figure 1 - History of USB targetted attacks*

In total, 26 percent of these threats had the potential to cause operational problems, including the loss of visibility or control by operators. Figure-1 above lays a concise history of USB targeted threats,

## Advanced USB Threats

Recently, researchers from Ben-Gurion University of the Negev in Israel have discovered 29 (yes, you read it correctly) ways someone can insert malware into your computer or smartphone via a USB port. Following are some of the more prominent methods.

### USBHarpoon and OMG Cable

USBHarpoon and OMG Cables are a malicious version of a USB charging cable that enables an attacker to reprogram the controller chip of a USB drive and make it appear to the computer as a human interface device (HID). The cable can be modified to allow both data and power to pass through, such that it is impossible for a victim to detect any suspicious behavior. The O.MG cable (or Offensive MG kit) from [MG] hides a backdoor inside the shell of a USB connector, which exposes a computer to the prospect of remote attacks over WiFi.

### Rubber Ducky and PHUKD/URFUKED

The Rubber Ducky USB stick is a ransomware threat developed in 2010 with a primary aim to encrypt your files by acting as a keyboard with pre-entered keystrokes. It works on every operating system that recognizes a USB thumb drive as the main input device—keyboard.

The most probable ransomware scenario is for the attacker to offer a PIN code to decrypt the files in exchange for money. Unfortunately, a simple Google search shows that the Rubber Ducky USB stick is available for purchase for a mere $3. The PHUKD/URFUKED malware works on the same principle as Rubber Ducky, with a subtle difference that allows the attacker(s) to choose a specific time to activate the keystrokes thanks to a programmed timer.

### BadUSB and BadUSB2.0

BadUSB manipulates USB firmware and will act as a HID (Hardware Input Device) such as a keyboard. BadUSB2 is able to achieve the same results as hardware keyloggers, keyboard emulation, and BadUSB hardware implants. Furthermore, BadUSB2 introduces new techniques to defeat keyboard-based one-time-password systems, by automatically replaying user credentials, as well as acquiring an interactive command shell over USB. Read more here

### Bash Bunny

Bash Bunny is a fully featured Linux computer with the ability to impersonate trusted mass storage or serial devices. According to the website description, Bash Bunny offers "easy setup & deployment with a simple 'Bunny Script' language, multi-position attack switch and a centralized repository of payloads. It's powerful with multiple attack vectors including HID keyboard, USB Ethernet, Serial and Mass Storage. Simultaneously perform keystroke injection attacks, bring-your-own-network attacks and intelligent exfiltration." Bash Bunny currently retails for $99.99.

## What makes USBs so vulnerable?

USB drives can automatically run applications when inserted into a PC that is running in the default configuration. During connection, each USB device identifies itself by sending a series of descriptors to the host.

**What does this tell us?**

- The USB spec for device identification was initially created in a "simpler time."
- The device is entirely responsible for presenting its descriptor information to the OS at runtime, with no other validation/checks.
- Many devices are insufficiently transparent in their descriptions.
- The hierarchy of descriptors has grown and gotten more complex.
- The Operating System has a big job, full of heuristics developed over time, to determine what a device is and what it will do once connected.

## Identifying USB Devices

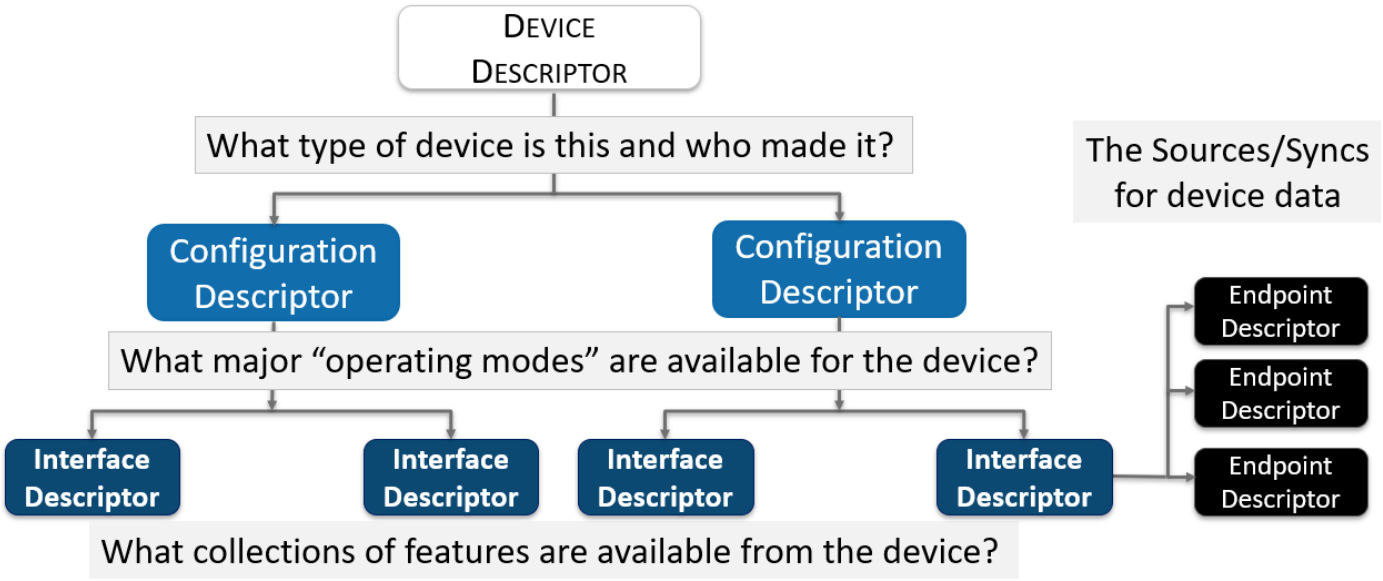



*Figure 2 - Each USB device identifies itself by sending a series of descriptors to the host*

## USB Security Myths vs. Reality

A number of security professionals are relying on outdated threat information and thus misapplying security solutions. This is understandable given the dynamic nature of threats, and the constant technical innovation across systems, networks, and software. It's important to recognize myths versus realities when it comes to defending the USB threat vector.

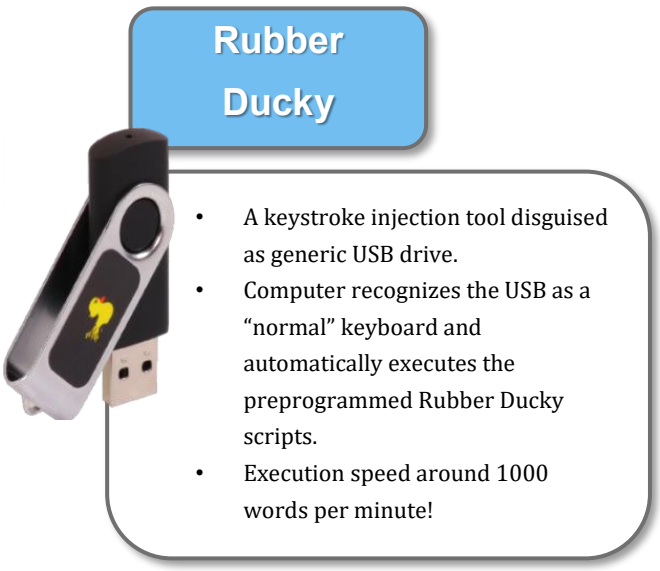
**Myth: We have traditional AV (Anti-Virus) installed onsite. This will catch all inbound malware from USB drives.**

**Reality:** AV is not an end-all, be-all solution to preventing malware brought in from removable media such as USB drives. Our recent study, the Honeywell Industrial USB Threat Report, was featured in The Wall Street Journal as some of the first major research into industrial USB threats and activity. It was found that, up to 11% of the threats discovered by Honeywell SMX in the study sample went undetected by traditional AV.

The design of Honeywell SMX intentionally separates the actual scanning of the USB drive from the user's workstation, unlike traditional AV which is installed on the workstation. When using SMX, the USB drive is scanned at the SMX System. This physical separation provides extra protection over AV, which requires the USB to be inserted into the workstation before it can be scanned. In some circumstances, once a malicious drive has been inserted, it is too late.

**Myth: We lock down USB ports. This prevents all USB based attacks and USB-borne malware.**

**Reality:** Many advanced USB and human interface device (HID) attacks such as BadUSB, Rubber Ducky and Bash Bunny are designed to circumvent these security measures by disguising themselves as an approved device at the firmware level. These tools are readily available to order online. For example, one can order a Rubber Ducky for as little as $3. Honeywell TRUST technology in the Secure Media Exchange (SMX) USB Driver helps protect against these threats by giving users an opportunity to examine and consciously approve every USB device before it's allowed to connect to the system.




**Myth: I buy qualified patches from the vendor. They send them to me through a secure VPN. I don't need a USB security solution.**

**Reality:** Distributing patches directly from your business systems is not a good idea. A secure method is essential for industrial cybersecurity best practices. For example, the Honeywell Security Guidelines state:

"It is not best practice to distribute Microsoft hotfixes, patches, and updates to virus definition files directly from the business network to nodes on the process control network as this is contrary to the goal of minimizing direct communication between nodes on these networks."

Honeywell SMX provides the ability to validate your vendor patches and securely distribute them to your systems in accordance with best practices. In addition, SMX software helps prevent malicious USB use elsewhere throughout your facility. These SMX capabilities help you manage compliance and meet cybersecurity standards for timely and documented patch management.

**Myth: I have Application Whitelisting (AWL), this will keep me safe from all inbound malware.**

**Reality:** For maximum protection, Honeywell recommends using both Secure Media Exchange and Application Whitelisting. SMX and AWL are complementary parts of a comprehensive defense strategy. For example, AWL cannot stop script/macro attacks embedded in authorized application files, while SMX can. This integrated solution has been tested in Honeywell's industrial cybersecurity lab.

**Myth: A USB security solution will impact my privacy. My sensitive files may be sent to Honeywell.**

**Reality:** Honeywell provides a technical solution to protect against new and emerging USB threats: Secure Media Exchange (SMX). SMX does not transmit any file contents out of your facility. When analyzing files, the first step is to calculate a hash of the file (similar to taking a fingerprint of the file) and send only the hash, to Honeywell Threat Intelligence for validation against a variety of threat intelligence services. If a file is not recognized by Honeywell Threat Intelligence, then the file is scanned locally by the SMX embedded engine.

## Recommended Best Practices

There are several actions companies can take to limit USB threats. Six categories of action are shown in Figure 3. Companies can also pace out how they approach the threat, understanding they face many daily tasks and challenges. Table-1 further below highlights several suggestions, such as assessing current USB defense measures and inventorying USB devices in use today. Finally, technical solutions.

## Establish and follow good (USB) security basics


*Figure 3 – Best Practices*

| Next Week |
|---|
| • Assess existing USB defensive measures, considering all 3 attack types |
| **Next Three Months** |
| • Complete an inventory of USB devices currently in use<br>• Assess your supply chain: what USB devices are you using? |
| **Next Three Months** |
| • Adjust USB and removable media policies to account for your findings.<br>• Consider technical controls and automation to enforce these policies |

*Table 1 – Suggested Steps*

## About Honeywell Secure Media Exchange (SMX)

Protect against current and emerging USB-borne threats with Honeywell Secure Media Exchange (SMX): easy-to-use security for safe, productive use of removable media in industrial networks. SMX Secures open USB ports from non-checked devices.


SMX prohibits known malware from being propagated via removable media, prevents unverified files from being read on Windows hosts and provides alerts on outbound threats and logs outbound file transfers.

SMX provides operators with unprecedented control and visibility into the secure use of USB and removable storage by personnel and contractors, effectively reducing cyber risk to process control networks globally. SMX provides the latest in advanced threat detection capability to critical infrastructures and isolated network environments. For more info visit Honeywell Secure Media Exchange.

## About Honeywell Industrial Cybersecurity

Honeywell is the leading provider of cyber security solutions that protect industrial assets, operations and people from digital-age threats. With more than 15 years of industrial cybersecurity expertise and more than 50 years of industrial domain expertise, Honeywell combines proven cybersecurity technology and industrial know-how to maximize productivity, reliability and safety. We provide innovative cybersecurity software, services and solutions to protect assets, operations and people at industrial and critical infrastructure facilities around the world. Our state-of-the-art Cybersecurity Centers of Excellence allow customers to safely simulate, validate and accelerate their industrial cybersecurity initiatives. Visit www.becybersecure.com to know more.

**For More Information**

To learn more about Honeywell Industrial Cybersecurity visit www.becybersecure.com or contact your Honeywell Account Manager, Distributor or System Integrator.



**Honeywell Process Solutions**

1250 West Sam Houston Parkway South
Houston, TX 77042

Honeywell House, Skimped Hill Lane
Bracknell, Berkshire, England RG12 1EB UK

Building #1, 555 Huanke Road,
Zhangjiang Hi-Tech Industrial Park,
Pudong New Area, Shanghai 201203

www.honeywellprocess.com

WP-19-02-ENG
April 2019



Honeywell