USBS BEHAVING BADLY
HOW TO CONTROL USB USAGE IN OPERATIONAL NETWORKS
Which one is safe?
USB Doppelgangers!

USBs Behaving Badly

- USBHarpoon
- Rubber Ducky
- Bash Bunny
- O.MG Cable
The State of USB Security
How likely is:

a malicious file trying to enter your site through an USB device?
This is what we found...
50 Locations

4+ Industries

4 Continents

Oil & Gas

Energy

Chemical

Pulp & Paper
26% Potential to cause major disruption to an industrial control system

e.g. loss of view or loss of control

- Oil & Gas
- Energy
- Chemical
- Pulp & Paper
15% Are well-known threats e.g. Mirai, Stuxnet, TRITON, WannaCry
Threats are Changing...
For example, this:

May pretend to be this:
SMX Protects Against Advanced USB Threats

**BadUSB**
- Manipulation of USB firmware.
- USB device will act as a HID - Human Interface Device (e.g. a keyboard), and can execute scripts.

**Rubber Ducky**
- A keystroke injection tool disguised as generic USB drive.
- Computer recognizes the USB as a “normal” keyboard and automatically executes the preprogrammed rubber ducky scripts.
- Execution speed around **1000 words per minute!**

**Bash Bunny**
- A fully featured Linux computer with the ability to execute all Rubber ducky scripts, as well as more complex attacks leveraging data connections (e.g. Ethernet over USB or Ethernet control model - ECM)
- Can also impersonate mass storage or serial devices
USB Device Attack Categories Visualized

Attack Categories*

Programmable Microcontrollers
Maliciously Re-programmed Peripherals
Not Re-programmed Peripherals
Electrical

* Ben Gurion University of the Negev, 2017
## USB Device Attack Categories Visualized

<table>
<thead>
<tr>
<th>ATTACK</th>
<th>USB Peripheral</th>
<th>Persona of USB Connected Micro-controller</th>
<th>Host</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rubber Ducky</td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>PHUKD / URFUKED</td>
<td>✔ ✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>USB drivey</td>
<td>✔ ✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Evlduino</td>
<td>✔ ✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Unintended USB Channel</td>
<td>✔ ✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>TURNIPSCHOOL (COTTONMOUTH-1)</td>
<td>✔ ✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>RIT attack via USB mass storage</td>
<td>✔ ✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Attacks on wireless USB dongles</td>
<td>✔ ✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Default Gateway Override</td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Smartphone based HID attacks</td>
<td>✔ ✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>DNS override by modified USB firmware</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Keyboard emulation by modified USB firmware</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Hidden Partition Patch</td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Password protection bypass patch</td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Virtual Machine Break-Out</td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Boot Sector Virus</td>
<td>✔ ✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>iSeeYou</td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>.LNK Stuxnet / Fanny</td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>USB Backdoor into air-gapped hosts</td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Data hiding on USB Mass Storage drive</td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Autorun exploits</td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Cold Boot</td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Buffer Overflow</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Driver Update</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Device Firmware Upgrade (DFU)</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>USB Thief</td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Attacks on smartphones via the USB port</td>
<td>✔ ✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>USBee attack</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>USB Killer</td>
<td></td>
<td></td>
<td>✔</td>
</tr>
</tbody>
</table>
What We Learned

- Relying solely on the USB Device information is not good enough
- What the USB device reports is not definitive!!

What matters is how the OS treats the device

- OS decision process is complex, taking into account many factors
- The driver the OS chooses may be “OS Standard” or “Vendor Specific”… makes all the difference
The Myths of USB Security
Common Myth “Locked USB Ports”

**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 as an approved device at the firmware level.

**Rubber Ducky**
- A keystroke injection tool disguised as generic USB drive.
- Computer recognizes the USB as a “normal” keyboard and automatically executes the preprogrammed rubber ducky scripts.
- Execution speed around 1000 words per minute!
Common Myth “My AV Will Protect Us”

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

Reality:
• AV is not a be all end all solution to preventing malware brought in from removable media such as USB drives.
• AV also requires the USB to be inserted on the workstation before it can be scanned. This can be problematic.
Common Myth “I Have AWL, This Will Protect Me From all Inbound Threats”

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

Reality:
• AWL cannot stop “all inbound malware”, typically AWL will not prevent script/macro attacks embedded in authorized application files. Make sure your USB solution can do this.
What Can We Do About It?
Apply What You Have Learned Today

• **Next week** you should:
  - Assess existing USB defensive measures, considering all 3 attack types

• **In the next three months** you should:
  - Complete an inventory of USB devices currently in use
  - Assess your supply chain: what USB devices are you using?

• **Within six months** you should:
  - Adjust USB and removable media policies to account for your findings.
  - Consider technical controls to enforce these policies
Establish and follow good (USB) security basics

1. Enforce Technical Controls
2. Monitor and Manage Network Traffic
3. Consider all USB attack types
4. Patch and Harden End Nodes
5. Secure the USB device supply chain
6. Deploy (and test!) Backup and Recovery
TRUST (Trusted Response User Substantiation Technology)

SMX ST
- Award winning
- Portable design
- Enterprise management capability
- Enforces USB device authorization
Why Customers Choose HON for Industrial Cyber Security

End-To-End Solutions

- Trusted partner for industrial cyber security
- Complete portfolio of industry proven cyber security products, services & solutions
- Operational Technology (OT) domain expertise
- Vendor neutral solutions for site or enterprise deployments
- Global capabilities and local presence

Professional Security Consulting Services
Managed Security Services
Cyber Security Software
3rd Party Integrated Security Products

Industry Proven Products, Services & Solutions
Thank you!

To learn more, visit:

http://becybersecure.com

And never trust doppelgangers … 🙃