Rubber Duckies / Bad USBs

By Zach Riback

What is it?

A rubber ducky (often called a bad USB) is a keystroke injection tool designed to be inserted into the USB port of a computer. Although it often is intentionally crafted to look like a normal flash drive, it does not behave like one. Once connected to a computer it acts as an external keyboard and is able to send keystrokes to the machine. A programmer can make a computer compromised by the rubber ducky do almost anything through these pre-programmed keystrokes. Often a malicious bad USB will be able to steal data, download malware, or otherwise freeze up a computer making it unusable.

On the most basic level, a rubber ducky / bad USB device is a little device that when plugged into the USB port of a computer can pretend to be a keyboard and send key strokes to a computer. It is through these keystrokes that the device can control the computer and make it do harmful things.

What is it used for?

Beyond its obvious malicious use by bad actors, this tool has many real and useful capabilities in the world of penetration testing. To get a rubber ducky device inserted into a company computer is a way to prove that the system is vulnerable to such attacks. If a penetration testing professional is able to get to a company machine to insert the device or trick an employee into inserting the device it shows the existence of a vulnerability. This process is key to mitigating such types of threats in the future.

Conclusion

Rubber duckies / Bad USBs are both a dangerous and useful tool in the realm of cybersecurity. It is important for orginizations to protect themselves from vulnerabilities involving this type of technology due to the speed and power of such an attack. They stress the importance of holistic security within an organization, as protecting against threats from bad USBs involves both physical security and an educated employee workforce.