DID YOU KNOW...

USBs are an extremely successful instrument for attack.

We all use them and they come in many different shapes and forms; we use them to store or transport business and personal information, we also use them to charge our phones, watches, Go Pros, E-Cigs and so much more. Needless to say, these devices are extremely vulnerable to attacks.

WHY ARE USBs AND CHARGING CORDS SO VULNERABLE?

The main reason USB devices are vulnerable to attacks is because you can plug them in anywhere which makes it easy to spread malware to other devices. For example, at some point during the day our phones will need to be charged and we will choose the most convenient or closest place to plug them in. We may even borrow someone else's charger in a pinch. Do you know if the charger you borrowed is secure? Do you know if the charging station you plugged into at the airport was tampered with? Do you know if the e-cig charger that you plug into your work computer to charge your device is virus free? RAVENii recommends you train your employees to not get caught in a trap. Don't let your curiosity get the best of you and plug in a device you randomly found on the ground, don't borrow USBs from people you don't know and don't plug in your USBs to untrusted devices. These actions can lead to serious problems for your organization if your employees aren't trained.

WHAT KIND OF ATTACKS CAN USBs AND CORD CHARGERS TRANSPORT?

One of the main attacks that has been documented is USBHarpoon. This specific malware attack is difficult to detect and allows the attacker to reprogram the USB chip, acting as a human interface device. Along with USBHarpoon, another known threat is OMG Cables which are also easily hidden. This attack hides a back-door inside the USB layers, which will reveal a computer to the possibility of remote incidents over WI-Fi.

HOW CAN I PROTECT MY ORGANIZATION FROM THESE ATTACKS?

There are many methods you can execute that can help reduce your risks for USB attacks. RAVENii recommends to lock down the use of USB devices to only essential business employees with esital business needs. You shall also have a well-defined policy and process in place that outlines how to request permission to use a USB device. Implementing technical regulations like blocking access to USBs throughout your organization can also make a big impact.

RAVENii's best practice recommendation for gaining visibility and hardening your security systems is by implementing a suite of security tools to identify and manage vulnerabilities, monitor on-wire traffic, stay up to date on patching and firmware upgrades, and properly backup data in order to recover it in case something were to happen.

RAVENii

CYBER SECURITY

844-317-0944

Think about this for next time..

Sensitive Data. All businesses have it. Where is yours stored? How is it protected? In the next article we will be discussing more on what it takes to maintain and protect your sensitive data.