October 11, 2013 Release # 236

-- Begin Transmission --

The Risks of Using Portable Devices – Part 2

Attacks are growing even more sophisticated and hard to detect as attackers use small circuit boards inserted in keyboards and mouse devices to launch malicious code when a certain key is pressed or condition is met. Once malware infects your PC to steal or corrupt your data, it might spread to other PCs on your home or organizational network. And these devices are an easy way for attackers to quickly propagate malware by passing it across all PCs that the device connects to.

Because these storage devices can install malware inside of any firewalls set up on your PC or network, you might not detect the malware until major damage has been done. Storage devices can also give malicious insiders the opportunity to steal data easily and inconspicuously because the devices are easy to hide and their use is hard to track.

Smart devices also have the potential to surreptitiously infect your PC or network when you download applications or games containing malware or viruses. Their use by a large population, emphasis on usability, and immature security tools make them ripe for malware attacks. Also, the potential for irreparable data exposure or loss arises from practices commonly used for storing sensitive data on smart devices. For example, users frequently keep personal bank account numbers or proprietary client information on their smart device that may be running untrusted applications or be connected to untrusted and vulnerable networks.

In addition, the features that make smart devices so attractive—such as Bluetooth and Wi-Fi— can also pose the most risk. When Bluetooth is on, the device becomes "discoverable" to both your headset and malicious attackers seeking to exploit the connection. They also target home and public Wi-Fi networks; public Wi-Fi hotspots are especially risky and a frequent target of attackers looking for data to pilfer. Attackers often linger nearby and use tools to intercept unencrypted data.

-- End of Transmission –

Information Security: It's a Shared Responsibility

REFERENCE(S): http://www.us-cert.gov/