FBI Warning Citizens of Wireless Keystroke Loggers

Ninja Bits: Near the end of April, the FBI has released an issue of a public alert in regards to "KeySweeper". KeySweeper is a piece of custom designed hardware that had been created by security researcher, Samy Kamkar, as a way to provide a proof-of-concept project. His project is fully capable of stealing keystrokes from wireless Microsoft keyboards by the ability to intercept nearby radio signals and then decrypting the Microsoft keyboards protocol.

This new device operates on top of the known Arduino board. This is so tiny; it is able to fit just inside the case of a regular USB charger. Since the USB chargers are becoming a commonplace with the proliferation of mobile technologies that includes the smartphones and tablets. One seeing a device plugged into a wall socket as well as abandoned in a typical office, is not too far out from ordinary in today's technology world.

The FBI is now warning companies to provide a limitation onto the number of outlets that are steadily available for the usage of charging. They are instructing employees to be able to recognize who has chargers that are currently plugged in, as well as not leaving your devices unattended at any charger plugged into a wall, if it is not used.

Ultimately companies are also instructed on limiting the usage of wireless keyboards. By switching to a wired keyboard or one that utilizes Bluetooth communications would be much more secured. However, if in fact that companies utilize the Bluetooth keyboards, the FBI also instructs them onto utilizing an encryption as well as a strong PIN for secure connection.

The KeySweeper is not capable of harvesting your every keystroke from Bluetooth Keyboards. Kamkar only created the device for harvesting the RF-Based wireless keyboards that had been created and even sold by Microsoft. While Microsoft keeps

their documentation out in the open for everyone, anyone is able to easily adapt to other platforms and even other manufacturers.

While this was doing some massive damage control after Kamkar's announcement just last year, Microsoft had also stated that the keyboards that are operating on the 2.4 GHz frequency are also manufactured after 2011. Thus they are also safe due to Thoy that utilizes Advanced Encryption Standard (AES) encryption for the usage of securing the users keystrokes between the keyboard and the respective computer.

Kamkar had also released the device in January of 2015. However, the FBI has just recently released the issue of this alert. This means that while they had investigated it at least in one case in which someone used a KeySweeper device in order to log users keystrokes.

You can watch a simple video about how this new device operates on YouTube;

Sources: SoftPedia { } AmericanBar { } YouTube { }