Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

29 April 2016

Alert Number
160429-001

Please contact the FBI with any questions related to this PIN Report at either your local **Cyber Task Force** or **FBI CYWATCH**.

Email:
cywatch@ic.fbi.gov
Phone:
1-855-292-3937
Local Field Offices:
www.fbi.gov/contact-us/field

Wireless Keystroke Logger Disguised as USB Device Charger Targets Wireless Keyboards

Summary

KeySweeper is a covert device that resembles a functional Universal Serial Bus (USB) enabled device charger which conceals hardware capable of harvesting keystrokes from certain wireless keyboards. If placed strategically in an office or other location where individuals might use wireless devices, a malicious cyber actor could potentially harvest personally identifiable information, intellectual property, trade secrets, passwords, or other sensitive information. Since the data is intercepted prior to reaching the CPU, security managers may not have insight into how sensitive information is being stolen.

Technical Details

KeySweeper is an Arduino-based[a] device which is contained within the shell of a USB phone charger. It is capable of detecting and decrypting radio frequency (RF) signals from certain Microsoft wireless keyboards manufactured before 2011 (many of which are still available for purchase). The wireless keyboard transmits these RF signals so the associated dongle plugged into a computer can identify which keys the user types.

- KeySweeper, which measures two to three inches, contains a Subscriber Identity Module (SIM) card that uses a cellular connection to send the data to an associated Web server. This SIM card also enables the device to send text messages to an associated mobile device when it picks up certain keywords such as Web site addresses. A small flash memory module can also store data if the SMS capability is somehow impeded.

[a] An Arduino board is an open-source, programmable and modular microcrontroller board containing input / output (spell out I/O) connections capable of interfacing with various other modules, devices and connectors.

- KeySweeper is hidden within a USB device charger and can be powered directly from an electrical outlet to harvest, decrypt, transmit, and store stolen data. A rechargeable battery serves as optional backup power should the device be removed from the wall.
- According to a Microsoft spokesperson, customers using Microsoft Bluetooth-enabled keyboards are protected against KeySweeper attacks. In addition, users of their 2.4GHz wireless keyboard designs produced after 2011 are also protected because those keyboards use Advanced Encryption Standard (AES) encryption technology.

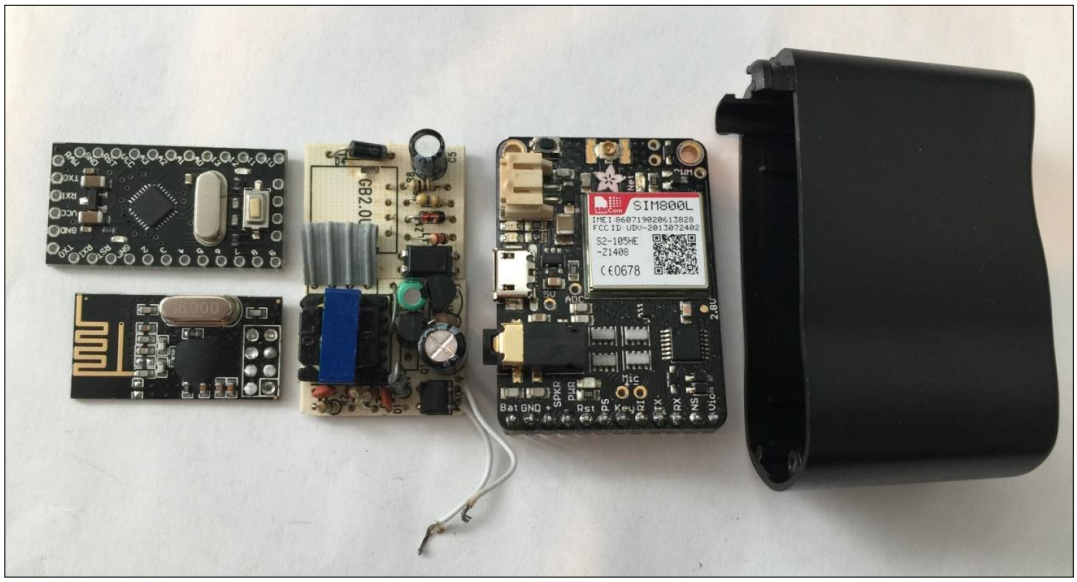
The KeySweeper device in use.

Threat

Since Arduino devices are modular and programmable, an actor could harvest data by capturing and decrypting communications protocols from various other wireless devices, depending on the weakness or exploitability of that protocol's encryption. The device is easy to overlook as it harvests and sends sensitive data to a collector.

- Although KeySweeper was designed to harvest from a particular brand of wireless keyboard, a cyber actor could program the device to conduct reconnaissance against a variety of devices. Given that RF ranges for all wireless devices registered with the FCC are located on the FCC's Web site, discovering the frequency for any registered device is relatively simple. An actor could swap out the RF board for one that matches the frequency of the other device.
- A KeySweeper-like device could be used to harvest data from wireless devices other than wireless keyboards, to potentially include data from Bluetooth, Wi-Fi, or SMS traffic, depending on the difficulty of cracking a protocol's chosen encryption method. Though the data could be collected, decryption depends on the configuration and

protocol.



The KeySweeper device dismantled. The Arduino board is to the top left, the RF monitor is directly below, and the SIM card board is to the far right.

Defense

The primary method of defense is for corporations to restrict the use of wireless keyboards. Since the KeySweeper requires over-the-air transmission, a wired keyboard will be safe from this type of attack. However, if the use of a wireless keyboard cannot be prevented, then ensuring a strong encryption on the keyboard is vital.

- A keyboard using AES encryption makes it more difficult to read keystrokes as there are currently no known practical attacks to read AES encrypted data.
- Keyboards using Bluetooth are also safe from KeySweeper as it listens on a different channel than that which Bluetooth transmits. However, Bluetooth keyboards must have encryption turned on and a strong pairing PIN to protect it from a similar type of data-harvesting attack.

Additional best practices to prevent a compromise could include but are not limited to office policies that address mobile device chargers:

- Limiting which outlets are available for device charging
- Knowing whose chargers are currently being used
- Immediate removal of an unknown charger from the office facility (although the optional backup battery can allow data theft even when unplugged)