Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

September 30, 2014

Alert Number
I-093014-PSA

STEALTHGENIE MOBILE DEVICE SPYWARE APPLICATION

The Internet Crime Complaint Center (IC3) has received reports related to the fraudulent advertisement and selling of StealthGenie, a mobile device spyware application ("app") that is alleged to illegally intercept wire and electronic communications made using mobile phones. The indictment and arrest of StealthGenie's CEO for selling the spyware coincides with disabling the website hosting StealthGenie and its associated online portal.

WHAT ARE MOBILE DEVICE SPYWARE APPS?

Mobile device spyware apps are developed for smart mobile phones and may allow a purchaser of the app to, amongst other things, surreptitiously monitor a phone user's communications and whereabouts.

The purchaser must generally have physical access to a target mobile phone to install a mobile device spyware app, which is usually downloaded to the phone. Each phone software platform, such as Apple Inc.'s ("Apple") iOs (for iPhones) and Google Inc.'s ("Google") Android, require specific steps to complete the installation process.

HOW DOES STEALTHGENIE WORK?

The StealthGenie app works in so-called "stealth" mode and is undetectable by most individuals. It is advertised as being untraceable. According to the indictment, StealthGenie's capabilities include the following:

- Call Recording: Records all incoming/outgoing voice calls or those specified by the purchaser of the app
- Call Interception: Allows the purchaser to intercept calls on the phone to be monitored while they take place, without the knowledge of the monitored smartphone user
- Recorded Surroundings: Allows the purchaser to call the phone and activate it at any time to monitor all surrounding conversations within a fifteen (15)-foot radius without the knowledge of the user
- Electronic Mail: Allows the purchaser to monitor the incoming and outgoing e-mail messages of user, read their saved drafts, and view attachments
- SMS: Allows the purchaser to monitor the user's incoming and outgoing SMS messages
- Voicemail: Allows the purchaser to monitor the incoming voicemail messages
- Contacts: Allows the purchaser to monitor the entries in the user's address book
- Photos: Allows the purchaser to monitor the photos on the user's phone
- Videos: Allows the purchaser to monitor the videos on the user's phone
- Appointments: Allows the purchaser to monitor the user's calendar entries

The purchaser can review information transferred from the target mobile phone via an online portal. These intercepted communications are stored on the StealthGenie website. For example, a purchaser can log-in to the online

portal to access information pulled from the user's phone such as messages, e-mail, photos, and phone calls.

CAN A PERSON TELL IF A MOBILE DEVICE SPYWARE APP IS ON HIS OR HER PHONE?

Mobile device spyware apps are developed and advertised as being invisible to targets and act in an undetectable manner. For example, an app can be installed to look like another type of app or file, such as a digital photo application. Therefore, it will be difficult for the non-expert user to determine whether or not spyware is on his or her phone.

Certain companies market apps and other products that will scan a phone for malicious software. Private computer forensic companies can physically perform similar scans. Federal law enforcement is not in position to determine the effectiveness of products and services from individual private vendors or entities. If a user is concerned about the potential presence of a mobile device spyware app on their phone, the only way to ensure that any app is permanently removed from the phone is to perform a "factory reset," as described immediately below.

HOW CAN A MOBILE DEVICE SPYWARE APP BE REMOVED?

If you believe your phone may contain a mobile device spyware app, the best option is to conduct a "factory reset" of the phone. When a reset takes place, the phone is restored to its original condition (i.e., the condition at the time of purchase).

Please be advised that this means any and all data and apps installed after purchase will be removed from the phone, including all stored information. Please make sure to back-up any data you want to save from your phone before conducting a factory reset. Please note that performing a factory reset of a phone will not delete any information that has already been already collected from the phone by the mobile device spyware app from a vendor's website.

Apple has provided information concerning how to perform a factory reset of an iPhone running the latest version of their mobile device operating system at http://support.apple.com/kb/HT1414 . Because Google's Android operating system is customizable by a phone manufacturer, please contact your phone's manufacturer for instructions on how to factory reset your phone, or take it to the store from which you purchased the phone. Similar action should be taken to determine how to factory reset a non-iPhone or non-Android phone.