Smartphone Users Should be Aware of Malware Targeting Mobile Devices and Safety Measures to Help Avoid Compromise

– Bryon Gross

The FBI has recently been made aware of various malware attacking Android operating systems for mobile devices. Some of the latest known versions of this type of malware are Loozfon and FinFisher. Loozfon is an information-stealing piece of malware. Criminals use different variants to lure the victims. One version is a work-at-home opportunity that promises a profitable payday just for sending out e-mail. A link within these advertisements leads to a website that is designed to push Loozfon on the user's device. The malicious application steals contact details from the user's address book and the infected device's phone number.

FinFisher is a spyware capable of taking over the components of a mobile device. When installed the mobile device can be remotely controlled and monitored no matter where the Target is located. FinFisher can be easily transmitted to a smartphone when the user visits a specific web link or opens a text message masquerading as a system update.

Loozfon and FinFisher are just two examples of malware used by criminals to lure users into compromising their devices.

Safety tips to protect your mobile device:

- When purchasing a smartphone, know the features of the device, including the default settings. Turn off features of the device not needed to minimize the attack surface of the device.
- Depending on the type of phone, the operating system may have encryption available. This can be used to protect the user's personal data in the case of loss or theft.
- With the growth of the application market for mobile devices, users should look at the reviews of the developer/company who published the application.
- Review and understand the permissions you are giving when you download applications.
- Passcode protect your mobile device. This is the first layer of physical security to protect the contents of the device. In conjunction with the passcode, enable the screen lock feature after a few minutes of inactivity.
- Obtain malware protection for your mobile device. Look for applications that specialize in antivirus or file integrity that helps protect your device from rogue applications and malware.
- Be aware of applications that enable geo-location. The application will track the user's location anywhere. This application can be used for marketing, but can also be used by malicious actors, raising concerns of assisting a possible stalker and/or burglaries.
- Jailbreak or rooting is used to remove certain restrictions imposed by the device manufacturer or cell phone carrier. This allows the user nearly unregulated control over what programs can be installed and how the device can be used. However, this procedure often involves exploiting significant security vulnerabilities and increases the attack surface of the device. Anytime an application or service runs in "unrestricted" or

"system" level within an operation system, it allows any compromise to take full control of the device.

- Do not allow your device to connect to unknown wireless networks. These networks could be rogue access points that capture information passed between your device and a legitimate server.
- If you decide to sell your device or trade it in, make sure you wipe the device (reset it to factory default) to avoid leaving personal data on the device.
- Smartphones require updates to run applications and firmware. If users neglect this, it increases the risk of having their device hacked or compromised.
- Avoid clicking on or otherwise downloading software or links from unknown sources.
- Use the same precautions on your mobile phone as you would on your computer when using the Internet.

If you have been a victim of an Internet scam or have received an e-mail that you believe was an attempted scam, please file a complaint at www.IC3.gov.