LippesMathias LLP
ATTORNEYS AT LAW

Recently Identified Back Doors on iPhones and iPads May Pose Security Risks

July 29, 2014 | **ARTICLES**

A recent presentation by noted forensic scientist and author Jonathan Zdziarski (https://twitter.com/JZdziarski) recently has identified several undocumented services running on Apple's iOS operating system which powers Apple's iPhone and iPad products. Mr. Zdziarski suggests those undocumented or back door services may make the Apple iOS products susceptible to commercial forensic tools such as those offered by Cellebrite (http://www.cellebrite.com/mobile-forensics), Elcomsoft (http://www.elcomsoft.com/eift.html), and Access Data (http://www.accessdata.com/solutions/mobile-phone-examiner).

Mr. Zdziarski speculates these forensic products may already use these services. These products are sold to law enforcement agencies which use them to obtain data from iOS devices, among other mobile devices. Law Enforcement agencies use these products mostly on phones in their possession but are thought on occasion to pair phones in other circumstances using USB remote protocols where phones of targets do not have USB pairing turned off or even during traffic stops or other custodial situations. Zdziarski also asserts that Apple iOS has a built in packet sniffer and considers that such a sniffer should only be mounted on iOS developer platforms if it is for developer purposes. If not for developer purposes, he questions what other valid use might it serve. Otherwise, Zdziarski credits iOS as being reasonably secure against attacks by routine hacking and criminals.

Zdziarski has posed this and several other security-related questions for Apple to consider and posted them on his blog. Thus far Apple has provided very little meaningful explanation of the purposes of the undocumented services, tersely asserting it designs its iOS "so that its diagnostic functions do not compromise user privacy and security, but still provides needed information to enterprise IT departments, developers and Apple for trouble shooting technical issues."

Zdziarski also notes that these back door services have been in iOS for years and were intentionally programmed by Apple and while he is not asserting any "grand conspiracy" between Apple and any government or security agency, he does believe these services "may" have been used by the NSA to collect data on "potential" targets.[1] The NSA is known to have used iOS security vulnerabilities in the past. In December 2013, security researcher Jacob Applebaum revealed that an NSA program named DROPOUT JEEP reportedly gave NSA almost complete access to the iPhone.

DROPOUT JEEP

Defined as "software implant" for iphones to provide specific SIGINT functionality. This functionality includes the ability to remotely push/pull files from the device. SMS retrieval, voicemail, etc.

NSA claims 100% success rate in installing malware on iphones.

Meanwhile, security consultants, including Zdziarski, are recommending that users of iOS devices set a complex passcode for their device (http://support.apple.com/Kb/HT5949) and install the free Apple Configurator (https://itunes.apple.com/us/app/appleconfigurator/id434433123), set enterprise device management restrictions in the configurator and delete all USB pairing records. While this may not eliminate all security-access vulnerability, it will make any unauthorized access of an iOS device's data more difficult. Zdziarski points out on this subject that iOS devices are, when turned on after rebooting essentially fully authenticated so far as these back door processes operate and most data protection encrypted data can be accessed until the device is again shut down. This is one reason locking down USB is a good idea.

Data privacy rights activists are awaiting further responses from Apple concerning these undocumented services, but Apple will likely stick to its story that these services are intended solely for trouble shooting technical issues.

[1] Androids and even blackberry have been crashed though perhaps not so thoroughly.

Related Team

Michael E. Storck
Partner | Team Co-Leader - Securities