beazley nodatabreach.com

Data Security Alert

iOS Security Alert: iPhones/iPads at Risk

Internet security firm FireEye has reported a significant new iOS security flaw dubbed “Masque Attack”. The vulnerability allows malicious replacement apps, installed through enterprise/ad-hoc (non App Store) provisioning, to overwrite genuine apps previously installed through Apple’s official App Store. The replacement can occur as long as both malicious and genuine apps use the same bundle identifier. The vulnerability has been verified for both jailbroken and non-jailbroken devices that use iOS 7.1.1, 7.1.2, 8.0, 8.1 and 8.1.1.

All apps are susceptible for such replacement except iOS preinstalled apps, e.g. Mobile Safari. In practice an attacker could lure a victim to install a replacement app with a deceiving name such as “New Angry Bird”, which is actually a malicious replacement for an email or online banking app. Using a well-designed interface to mimic the original app, the replacement app could steal sensitive information including logon credentials.

Further, the replacement apps have been shown to be able to access the original app's local data - for example cached emails or login-tokens - which the malware can then use to log into the user's account directly. Such attacks could result in compromising bank, email, or other sensitive accounts and information that users access on their mobile devices, including sensitive corporate emails.

Attackers can trick a user into downloading a Masque Attack app from outside the Apple-approved App Store, usually through a prompt via text message, email, or hyperlink.

Mitigations

iOS users should protect themselves from Masque Attacks by following these steps:

1. DO NOT install apps from third-party sources other than Apple's official App Store or the user's own organization.
2. DO NOT click "Install" on pop-ups from third-party web pages, regardless of what description the pop-up uses for the app.
3. When opening an app, if the iOS shows the alert "Untrusted App Developer", click on "Don't Trust" and uninstall the app immediately.
4. If using iOS 7, check the profile section by navigating to Settings - General - Profiles. Any profiles used to install a non-App Store will be shown here and can be deleted. Apple has removed the ability to see these profiles on the devices using iOS 8.
5. Suspicious applications can be removed by deleting them, and re-installing cleanly from the App Store.

If you suspect that your App was subject to this attack, change all passwords on your business/banking accounts accessed on mobile Apple devices.

This information is provided by ePlace Solutions, Inc. which is solely responsible for its content. ePlace Solutions, Inc. is not engaged in rendering legal or other professional services. Federal and state laws are more complex than presented here. This information is simplified for the sake of brevity and is not a substitute for legal advice. ePlace Solutions, Inc. disclaims any liability, loss or risk incurred as a consequence, directly or indirectly, of the use and application of any of the contents of this information.