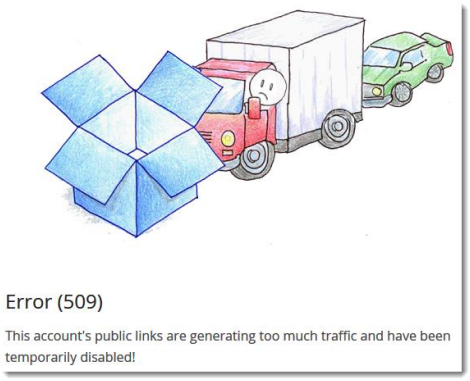
A significant vulnerability has been discovered by FireEye mobile security researchers and reported to Apple on July 26, 2014. Named "Masque Attack" by FireEye, the vulnerability has been verified to affect all users of Apple iOS versions 7.1.1, 7.1.2, 8.0, 8.1 and 8.1.1 and can lead to significant compromise of user information on affected devices.

This vulnerability exists because iOS doesn't enforce matching certificates for apps with the same bundle identifier which is created during installation. This allows an attacker to lure a victim to install an app with a deceiving name crafted by the attacker and the iOS system will use it to replce a legitimate app with the same bundle identifier.

Security Implications

1. Attackers could mimic the original app's login interface to steal the victim's login credentials. This has been confirmed through multiple email and banking apps, where the malware uses a UI identical to the original app to trick the user into entering real login credentials and upload them to a remote server.
2. FireEye also found that data under the original app's directory, such as local data caches, remained in the malware local directory after the original app was replaced. The malware can steal these sensitive data. FireEye confirmed this attack with email apps where the malware can steal local caches of important emails and upload them to a remote server.
3. The MDM interface couldn't distinguish the malware from the original app, because they used the same bundle identifier. Currently there is no MDM API to get the certificate information for each app. Thus, it is difficult for MDM to detect such attacks.



FireEye has created a video which may not be accessible as shown in the accompanying graphic. The link to the video is: https://www.dropbox.com/s/iy538vlb4dqpgee/ios_masque_monitor.mp4?dl=0.

Mitigation (Risk Avoidance)

1. Don't install apps from third-party sources other than Apple's official App Store or the user's own organization
2. Don't click "Install" on a pop-up from a third-party web page, as shown in Figure 1(c), no matter what the pop-up says about the app. The pop-up can show attractive app titles crafted by the attacker
3. When opening an app, if iOS shows an alert with "Untrusted App Developer", click on "Don't Trust" and uninstall the app immediately

You can read the complete FireEye blog post here: http://www.fireeye.com/blog/technical/cyber-exploits/2014/11/masque-attack-all-your-ios-apps-belong-to-us.html

[20141110]