Edward Wu
CS 460
Final Project
Report

Malicious Android Apps

Introduction

The purpose of this project was to explore the security and privacy concerns of Android apps and the process of rooting an Android device. Many smartphone owners root their phones in order to add custom ROMs and themes. However, by rooting their device, these users risk exposure to malware and viruses. In order to highlight this risk, this project will build a malicious Android app that will exfiltrate a user's email and the device's IMEI (International Mobile Equipment Identity) number.

Method

The Android app developed was meant as a proof of concept for a successful exfiltration. Ideally, the malware will be disguised as some sort of game. The app consists of only two views.

An unsuspecting user will initiate the malware by pressing the play button. This will trigger a function that will search the phone for the user's email and the device's IMEI. It will then contact a remote server and log the captured data into a database. For this project, the server is hosted on the University of Illinois's cPanel service. The server code and the code used to create the database are included in the source files as `maliciousServer.php` and `email.sql`.

Discussion

Among the top 5 reasons for not rooting an Android device is the risk of exposure to malicious apps.[1] However, a popular rooting application called SuperSU will actually prompt the user when an app is requesting to use elevated privileges. Unfortunately, the warnings that it gives can desensitize the user causing him to click through the warning. In the malware developed for this project, the app requires several not-so-subtle permissions in order to work. In order to contact the server, the app requires internet permission. In order to read the user's email and IMEI number, another set of permissions must be granted. Android will actually show these permissions to the user before he installs the application. Although these permissions seem strange for a game, they are actually quite common among all applications due to the prevalence of advertising libraries that use these same permissions. Similar to the SuperSU application, these permission requests have the effect of desensitizing users who end up granting the permissions just to get to the game.

Conclusion

Even though Android and rooted Android applications give a fair amount of warnings, users can still end up as victims. As is the case for most security topics, the technology is adequately secured, but ultimately the point of failure lies with the users.

[1] http://betanews.com/2013/10/01/5-reasons-not-to-root-android/