Security News
2013-40005 Remote Access Tool AndroRAT Inject Into Android APK Risk

1. Affected Version

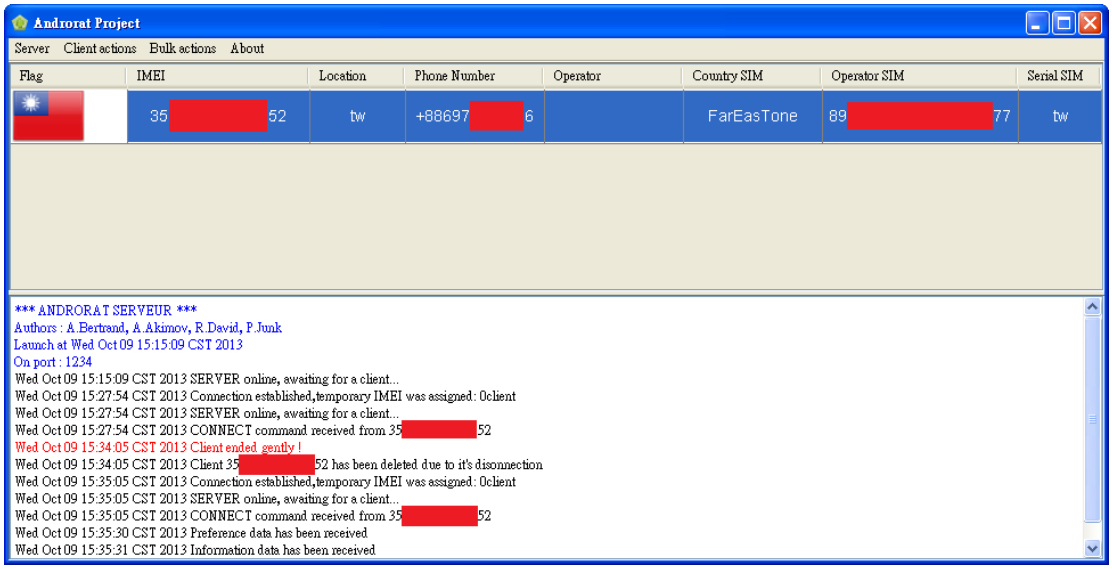
Android OS

2. Description

AndroRAT is an open-source tool that was created and published on the Internet, it is a RAT (Remote Access Tool) for Android OS and exactly as any other RATs, and it allows a remote attacker to control the victim.

3. Vulnerability Analysis

The RAT comes in the form of an APK which is the standard application format for Android. When used in conjunction with the AndroRAT APK binder, it easily allows an attacker with limited expertise to automate the process of infecting any legitimate Android application with AndroRAT, thus Trojanizing the app.



AndroRAT C&C panel

4. Recommendation

1. AegisLab IDP signature database can prevent this attack since 2013/10/3.
2. Installing a security app, such as AegisLab Antivirus
3. Avoid clicking links that lead to third-party sites advertising free apps
4. Enable app verification: go to your device's apps menu and touch Google Settings > Verify apps. Touch the box next to verify apps; the setting turns on when the check mark appears. If your device is running Android 4.2 and higher, you can also go to Settings > Security > Verify apps.

5. Reference

http://securityaffairs.co/wordpress/17038/cyber-crime/androrat-drives-the-rise-for-diy-android-hacking-tools.html
http://securityaffairs.co/wordpress/15759/cyber-crime/android-botnets-on-the-rise-case-study.html
https://support.google.com/accounts/answer/2812853?hl=en

About Lionic: Lionic Corporation is an innovative network security chip and IP design company. It provides optimal cost-performance solutions for network security products from 30Mbps SOHO devices to 4Gbps enterprise-level appliances.
For more information, please visit Lionic website and contact our sales representatives.
Web site: www.lionic.com e-mail: sales@lionic.com Tel: 886-3-578-9399 Fax: 886-3-578-0707