ABSTRACT

The popularity of Android smartphones has increased the number of security threats that target mobile devices. Current mobile device offer a large amount of mobile applications and services. These days, mobile banking, confidential mailing and other influential and confidential activity can be done in an Android device. Those activities can be exploited to get user personal data (phishing). In this final project we analyze data theft attack (kleptodata) on Android 2.3 operating system and implementing it using malware application. The malware is exploiting several of Android security weaknesses.

We exploit several Android weaknesses where an already installed Android application can get the permission to download and installing another application, which then can be run on the background. More so, the permission-based security system on Android differs from other mobile operating system, where the user was unable to review the permissions asked by application. User may accepting or ignoring all of the permission asked. These weaknesses is combined with the inter-application communication feature on Android. Those weaknesses is implemented using a pair of applications to stole SMS data from the phone, keeping it in the database, and sending the stolen data to server. Both applications detecting each others' presence, therefore even if one of the applications is being uninstalled, it will download the uninstalled part and continuing the process.

Our finding is that the malware application used to perform kleptodata attack run as intended, with the SMS logs being sent into server. At the time of testing in May 2014, several commonly used antivirus on the Market did not detected the application as a malware. However, the masquerade system used by the application still not good enough, since it didn't totally comply with the permission needed by the applications.

Key words: Android, Security, Kleptodata, Malware