Summary report on Dissecting Android Malware: Characterization and Evolution

Siva Chintapalli

February 06, 2016

Dissecting Android Malware: Characterization and Evolution

Over the years smartphone usage has been increased tremendously and became vulnerable for malware attackers, especially on popular platforms like Android, IOS and windows etc. Among all the platforms Google Android overtook other platforms with 46percent share of mobile malware and still growing. As Android is most adaptive mobile platform which should provide best defense system and get not exploited easily. According to the report 400percent of Malware has been increased in Android since 2010.

In this paper author mainly focus on Android malware characteristics and its existence.

1. In Android platform 1260 android malware Samples are identified and grouped them in to 49 families from 2010 2011.

2. After analyzing the Malware samples, it has been characterized based on its behavior.

   (a) Malware Installation Installation of malware is analyzed carefully and grouped in to four categories:

      i. Repacking: These is one of the most common technique. In this technique an existing application in the market has been dissemble and add payload (malicious content) and repacked and released in to the market as original application. Among 1260 samples 1083 are repackaged samples.

      ii. Update attack: In this technique app will be repackaged with update component. Once the user download application and started using update component will fetch payload and install without user knowledge.

iii. Drive-by Download: In this technique malware authors make legitimate app like games or some fake social accounts and attract the user to download and install them. These are hard to identify by normal users and which are used to steal the sensitive information such as bank details.

(b) Activation: Once the user has been download and install the application in mobile payload will trigger events and start attacking the system or before the application installation payload will trigger the Bootstrap.

(c) Malicious Payloads: Based on the payload Malware is characterized in to four groups

   i. Privilege Escalation
   ii. Remote Control
   iii. Financial Charge
   iv. Information Collection

Evolution: Among 1260 Sample of Malware, 473 sample are from DroidKungFu and 187 samples are from AnswerBot. Which give clear view of the Malware growth.

In June 2011 first version of DroidKungFu was detected and second, third and fourth versions are identified in July, August and October 2011 respectively. Many of these are encrypted for root exploits which are looks like normal files. Ever version of DroidKungFu payloads are used to communicate with the CC server and receive commands from them. It also carries Shadow Payloads, when the root exploits are successfully, payloads will install automatically without user aware.

AnswerBot was first discovered in September 2011. These Malware look like legitimate apps which are released on the Android third party Apps. These Malware mainly present on Chain Based Android Platform.

Author test four antivirus to detect Malware in the infected mobile and the results as follow.

AntiVirus	Malware Detection
AVG	54.7
LookOut	79.6
Norton	20.2
Trend Micro	76.7

Due to rapid growth of malware many Antivirus Organizations face serious challenges to provide better security.