The anonymous Attaker Dissecting Android Malware Characterization and Evolution

Sudheer Mandava

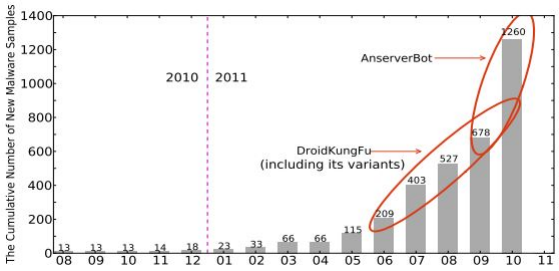
February 6,2016

1 Introduction

Android malware on the raise infact the number malware app on google store itself increased drastically it's quiet scary what this malware programme can get up to in your phone from record your conversation taking full control of your handset taking your personal data such as email address and contact details even tracking your gps data. In this paper these people present a systematic characterization of existing Android malware. The characterization is made possible with one-year effort in collecting 1260 Android malware samples in 49 different families,these are different types of android malware depends on effects what they costs. on their one year effort they come across almost all existing Android malware, where studies runs from August 2010 to recent ones in October 2011.

2 Theory

The figure shows the monthly data of Yajin Zhou, Xuxian Jiang collected, here we can clearly see the way malware samples in their data set drastic changes in every month. infact datasets doubled every month from april to october, where they highlighted two most dangerous and most evolving malware DroidKungFu (starting June, 2011) and AnserverBot (starting September, 2011) these can easily escape from existing anti-virus software



DroidKungFu is the most unwanted malware in entire dataset In total there are 473 DroidKungFu malware samples they are many ways it can escape from detection there are root exploits where some of the files encrypted they look like healthy files thus it avoid from detection. they also escape through C and C Servers , Shadow Payloads, Obfuscation, JNI, and Others .AnserverBot these entirely third party application from china deals with tracking card details and files with these malware they sneak through all the personal data it cannot be detected because of its dynamic behaviour we must be aware of the malware

3 Summary

This paper shows the types of andriod mallware and classified them on there properties they also mention how poor performance our anti virus are functioning and ellabrated how malware escaped from being detected and A variety of findings has been shown in terms of characterization including malware installation, activation, malicious payloads, and permission use, which provides useful insight to identify Android malware in the near future when deciding if an application is suspicious and they also suggesed where we have to focus on to avoid these malware and also provided some soloutions to detect malware they almost coverd all the mallware It would be great the study could be carried out in a regular basis, making a comparison in changes.