# Dissecting Android Malware

Surya Valluri

02/07/2015

In the recent years, there has been a rapid growth in smartphones market with which majority of them having android based operating systems in them. Along with the market android also shares the highest share in mobile malware of 46% and still counting, keeping these number in mind it clearly shows that we need to strengthen the defense system. So that highest share in the market should be an advantage in getting better services, not to get exploited in terms of security.

This paper aims to cover three aspects:
1. Collecting and tabulating all types of android malware samples and categorizing them into different families.
2. Based on the analysis we will characterize them based on their life cycle in the application.
3. Keeping the present scenario, we show that existing solutions for malware attacks are lagging.

| Malware | Count of bugs out of 1260 |
|---|---|
| DroidKungFu3 | 309 |
| AnserverBot | 187 |
| BaseBridge | 122 |
| DroidKungFu4 | 96 |

2. Malware characterization and installation:
Let's take a closer look at how does malware enters the system and they are three major types of intrusions:
a. Repacking: Once the application is released in the market, malware authors disassemble them add their malicious stuff and assemble as it is and upload in the market with such a signature which makes it appear that it is legitimate and a genuine release by the organization.
b. Update Attack: Once the user started using the application, he doesn't use the same version throughout and definitely he would go for an update.Malware authors make sure they added a malicious payload in the update and make it available for the users, opting for an update user is targeted without his knowledge.

c. Drive-by Download: Malware authors advertise their apps in such a way that it shows some feature rich application which lures users to download and install them. A normal user can't figure out if the application has such unreliable stuff and there are chances that he can be easily attacked.

Installation: Once the malicious payload enters the host system through the app it might be installed in two ways. Once the app is running the malware payload triggers its events and attacks the system or it triggers the bootstrap before the host application is launched.

Malicious payload attacks system in different forms and the famous forms of payloads take in control of user privileges escalation, remote control and financial charge. There are some more active payloads which also collect user information and also sensitive bank information.

3.Present Scenario: Such a rapid growth in malware and its criticality challenges many system security organizations regarding their effectiveness. To test the malware detection we selected four different system security software's(AVG ,Lookout,Norton and TrendMicro) and before installing each of them on a phone we have exposed it with a virus database. Then we installed security software's and tried detecting the malware.

| Security Software | Detected Sample Percentage |
|---|---|
| AVG | 54.7% |
| Lookout | 79.6% |
| Norton | 20.2% |
| TrendMicro | 76.7% |

The statistics above show that each software has a different design and implementation in scanning malware, but none does the purpose solely. Which shows that security software's have to update their approach in designing and finding viruses on the system.

This is my github repository link: `https://github.com/suryavalluri1/encryption_engineering.git`