Faculty of Information and Communication Technology

INVESTIGATING DROIDKUNGFU1 ANDROID MALWARE BEHAVIOUR THROUGH STATIC ANALYSIS

Najiahtul Syafiqah Binti Ismail

Master of Computer Science (Security Science)

2013

INVESTIGATING DROIDKUNGFU1 ANDROID MALWARE BEHAVIOUR THROUGH STATIC ANALYSIS

NAJIAHTUL SYAFIQAH BINTI ISMAIL

A thesis submitted

In fulfilment of the requirements for the degree of Master of Science Computer (Security Sciences)

Faculty of Information and Communication Technology

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2013

DECLARATION

I declare that this thesis entitle Investigating Droidkungfu1 Android Malware Behaviour through Static Analysis is the result of my own research except as cited in the references. The thesis has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature :

Name : Najiahtul Syafiqah Binti Ismail

Date :

APPROVAL

I hereby declare that I have read this thesis and in my opinion this thesis is sufficient in terms of scope and quality for the award of Master of Computer Science in Security Science.

Signature	**:**	
Supervisor's Name	**:**	**Prof. Madya Dr Mohd Faizal Bin Abdollah**
Date	**:**	

DEDICATION

I would like to dedicate this project to my beloved dad, Haji Ismail Bin Salim (1954-2005), and my beloved mom, Hajah Samidah Binti Ab Samad for instilling the importance of hard work, patience and having higher education in life.

ABSTRACT

Rapid growth on smartphone user nowadays gives the view that this device becomes necessity on human's life. Smartphone user expectations is to stay connected with their social networking, managed their daily schedule and also for entertainment purposes. The user friendly interface, ease to use, and offer many sources to download fancy and interesting application from official or alternative market make Android one of the most popular smartphone operating system in this 21st century. The pervasive download application that available in the market without any quality or security control exposed Android user to the malware threat which then will reveal their personal information without user permission. This paper focuses on analysis the behavior of DroidKungFu1 malware by using reverse engineering process to define requirement parameter and find the suspicious permission and risky API flaws of Android application through static analysis technique. At the end of this project, the data collected will used to produce state diagram of DroidKungFu1 and generate attack pattern of DroidKungFu1. This result will help future researcher or student to study on DroidKungFu1 behavior in depth and also give awareness sign to illiterate IT user smartphone on how the malware can affect their personal information.

Keywords: Reverse Engineering, Static Analysis, DroidKungFu1, Malware Behaviour, Smartphone.

ABSTRACT

Peningkatan mendadak bilangan pengguna telefon pintar pada masa kini memberi gambaran bahawa peranti ini menjadi satu keperluan hidup manusia. Jangkaan bagi pengguna telefon pintar adalah untuk terus berhubung melalui rangkaian sosial, menguruskan jadual harian mereka dan juga untuk tujuan hiburan. Memberikan kemudahan mesra pengguna, mudah digunakan dan menawarkan pelbagai sumber untuk memuat turun aplikasi menarik daripada pasaran rasmi atau alternatif menjadikan Android salah satu sistem operasi telefon pintar yang paling popular pada abad ini. Kemudahan memuat turun aplikasi tanpa kawalan kualiti dan keselamatan menyebabkan pengguna Android terdedah kepada ancaman menyebabkan maklumat peribadi penggun digunakan tanpa kebenaran. Kertas ini memberi tumpuan kepada analisis tingkah laku DroidKungFu1 malware dengan menggunakan proses Reverse Engineering bagi menentukan parameter dan mencari bukti kelemahan API dan permintaan kebenaran melalui teknik analisis statik. Pada akhir projek ini, data yang dikumpul akan digunakan untuk menghasilkan gambar rajah keadaan DroidKungFu1 dan menghasilkan corak serangan DroidKungFu1. Keputusan ini akan membantu penyelidik di masa depan atau pelajar untuk belajar pada tingkah laku DroidKungFu1 mendalam dan juga memberi tanda kesedaran kepada buta huruf IT telefon pintar pengguna bagaimana malware boleh memberi kesan kepada maklumat peribadi mereka.

Kata Kunci: Reverse Engineering, Statik Analisis, DroidKungFu1, Tingkahlaku Malware, Telefon Pintar.

ACKNOWLEDGEMENT

Alhamdulillah. Thanks to Allah SWT, whom with His willing giving me the opportunity to complete my Projek Master entitle Investigating DroidKungFu1 Android Malware Behavior through Static Analysis. I would like to express my sincere gratitude to my supervisor, Prof. Madya Dr. Mohd Faizal Bin Abdollah, for the continuous support to complete my project, for his assist, sound advice, patience and immense knowledge. His guidance helped me in all the time of final year project and writing of this report. Deepest thank and appreciation to my beloved mother and siblings for giving me support and motivation throughout my study years. Last but not least, my thank goes to my friends for the stimulating discussions, for the sleepless nights we were working together before the deadlines, and for all the fun we had together.

LIST OF FIGURE

LIST OF TABLES

LIST OF ABBREVIATIONS

1.	**API**	**Application programming interface**
2.	**APK**	**Android Package Kit**
3.	**APP**	**Application**
4.	**CMD**	**Command**
5.	**DVM**	**Darvik Virtual Machine**
6.	**GPS**	**Global Positioning System**
7.	**IMEI**	**International Mobile Equipment Identity**
8.	**IMSI**	**International Mobile Subscriber Identity**
9.	**MMS**	**Multimedia Messaging Service**
10.	**SD. CARD**	**Secure Digital Memory Card**
11.	**SMS**	**Short Messaging system**

TABLE OF CONTENTS

LIST OF APPENDICES

CHAPTER I

INTRODUCTION

1.1 Background

Nowadays, smartphone is getting increasingly popular and become a trend. Everyone keep in alert to follow the trend and it becomes a necessity device that everyone must have. Beside the basic phone activity such as short messaging system (SMS) and calling, they are using smartphone for capturing and recording important moment, organizing their daily schedule, managing their email, and socializing in social network site and playing game. User expectation by using the smartphone to stay connects connected in their social network world and as manager of their daily life.

There are many types of smartphone operating system platforms such as IOS from Apple, Android from Google (originally founded by Android Corp.), Blackberry and Windows. However, since Android compatible with many brands of smartphone and have variety range of price from the cheapest to the most expensive price, Android become the main choice for the user. Now, Android is one of the world's most popular mobile platforms because it is user friendly operating system and many choices of free applications on store. It uses a Linux-

based operating system. It is an open source platform which can be used by any phone manufacturers in the world. Android Inc. was founded by Andy Rubin (2011), Rich Miner (2007), Nick Sears (2011) and Chris White (2005) at Palo Alto, California on October 2003. However, on August 2005, Google Inc. have bought Android Inc. and making it as a Google subsidiary and user can get all the latest application at Google Store. The first version of Android mobile operating system is on 2007 where Android released a beta version and follow on 2008 where Android release the first commercial mobile operating system which is Android 1.0. Until today, there are seventeen version of android commercial mobile operating system excluded the two alphas and beta version. The latest version of android mobile operating system is Android 4.2 Jelly Bean which release in November 2012 (Nahrstedt, K., 2011).

Since Android is one of the biggest mobile platform operating system, many attackers had continuously focus on improve or design their program to gain access from Android user. This make Android user exposed to mobile threat which also known as malicious program or malware category. Android user must aware that the effect of this threat will expose their privacy to another bad people. The threat will get their personal device information such as IMSI and IMEI number. Mostly, the motive of malware threat is more on to make monetary profit from Android mobile which has been infected with the malware.

This project will cover the development and implementation of an appropriate simulation network for android mobile and also tools for doing the static analysis on android malware. A simulator of android smartphone and the malware analysis will be done in Virtual Machine to avoid the host pc, other device or files gets infected by the malware. To gain this project objective which is to

profile the malware behavior, I need to analyze the parameters that have been selected using a specific tool to get an accurate result.

The main focus on in this project is to analyze the android malware. Droidkungfu1 has been chosen for this project. The DroidKungfu1 is one of the sophisticated android malware found in 2011 by North Carolina State University researcher, Associate Professor Xuxian Jiang and his research team (X. Jiang, 2011). The DroidKungFu1 malware was found included in repackaged apps which available through a number of alternative apps markets or black-markets. The malware will change the structure of the infected app with a new service and a new receiver. The malware will automatically launch the service once the receiver notified when the system finishes booting. It does not ask for user permission (Y.Zhou and X. Jiang, 2012).

1.2 Problem Statements

Nowadays, Android applications are used widely in range of area which make it surrounds with very sensitive information and can lead to serious security risks if there are fall into unauthorized persons. According to A. Gahalaut (2010), since Android market does not have any prior security check, irresponsible person tend to spread malicious application especially in free apps market. Malware author tend to write application that seems legitimate application but there are contain with risky APIs and tricky permission to confuse the user.

1.3 Objectives

- To study about DroidKungFu1 malware behavior and investigate the information it infected in smartphone.
- To identify parameter in malware analysis through static analysis.
- To analyze the comparison behavior during normal and infection condition.
- To produce the state diagram of DroidKungFu1 malware.

1.4 Scope

The scope of this project is more on study the behavior of DroidKungfu1 malware and how its affect information in smartphone. Besides, this project also analyze about the comparison of DroidKungfu1 malware behavior during normal and infection condition.

- Analyze the malware behavior with the selected parameters.
- Analyze the result to get the final finding.
- Applied on two scenario; normal and infected environment.

1.5 Project Significance

The significance of this project is to analyze the malware behavior with the selected parameters. Two scenarios will be test in testbed on a virtual machine to discover the behavior when infected or normal condition. From this project, it will get the malware behavior profile at final finding. All information about the malware profiling behavior and its result will be store for future review.

1.6 Expected output

This research project expected to give lots of benefits to researcher and also help educate user not to easily install any application available in market. It is also expectantly could help user to reach their satisfaction on using the save application that does not exploit their personal information. At the end of this research, it will get overall droidKungfu1 behaviour profile and how it exploits in user smartphone.

1.7 Summary

As a conclusion, this chapter reviews on the description of the project and some related background information on the project. This chapter has clearly defined the objectives and scopes of the project. Besides, as a guideline for the implementation, all the problem statements have been listed with the project significance. As, it still earlier to mention or discuss about the result, this chapter is just only describe what the expected output will be derived from this project.

This project seems to be very helpful for the media streaming provider to enhance their service. Besides, it will help the students who will do the same research as this project. This chapter will become the guideline and future review to all the work that is to be carried out in the next phase.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

Literature review is aimed to review the critical points of current knowledge on a specific topic. Thus, the intention of the literature review is to discover, interpret and investigate the literature or any works or studies related to this system. It is important to recognize and considered all related information before implement this project research.

For this project, few research and analysis on previous or related research papers have been done to understand the concept, purpose and the way of implementation regarding this project.

2.2 Related Work

The motive or development of this research is not self-developed but based on the theory or ideas from previous research. This research is more on proof-of – concept or to accomplish the theory or hypothesis that had been state before by previous researcher. Besides, this research project also improves by focus on specific

or added new features of chosen parameter and malware to analyze. Below is the summarization of similar research from year 2009-2013.

Table 2.1: Similar previous related work.

	Researchers	Title	Technique/ Method	Specific Approach	Output
1.	Khyati R.; Vinod D.	Performance Base Static Analysis of Malware on Android (2013)	Reverse Engineering: • Static Analysis	• To explore a study of static analysis on Android. • To give an overview for user about how malware can harm their personal information by providing real case malware attack scenarios. • To explore the permissions file of the Android applications.	• Proven that malicious application decides the activity without user knowledge. • Permission files give a hint for any suspicious activity however most users do not aware the permissions of the applications.
2.	Peffer, A. et al.	Malware Analysis And Attribution Using Genetic Information (2012)	Reverse Engineering: - Header Analysis - Dynamic Analysis - Semantic Analysis	• To develop an understanding of malware features by using biological analogy & linguistic analogy. It's compared the malware sample with the living organisms.	Malware features based on two main analogy: • Attackers often reuse pattern code & techniques to hide the attack similarities for avoiding detection. • Malware's function plays the main role to understand the reuse code pattern.
3.	Xuetao W. et al.	Profiledroid: Multi-Layer Profiling Of Android Applications (2012)	Static Analysis	To measure & develop malware profile at four different layers: • Static layer • User interaction layer • Operating system layer • Network layer	Produce a monitoring & profiling system that evaluate Android malware characteristic with systematic approach which are: • Generate cost-effective but comprehensive Android App profiles