BORANG PENGESAHAN STATUS TESIS

JUDUL: INVESTIGATING DROIDKUNGFU4 ANDROID MALWARE BEHAVIOR THROUGH DYNAMIC ANALYSIS

SESI PENGAJIAN: SESI 2012/2013

Saya KOAY SOON LEE mengaku membenarkan tesis Projek Sarjana Muda ini disimpan di Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dengan syarat-syarat kegunaan seperti berikut:

1. Tesis dan projek adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. ** Sila tandakan (/)

_____	SULIT	(Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)
_____	TERHAD	(Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan)
____/_____	TIDAK TERHAD	

_____ _____

(TANDATANGAN PENULIS) (TANDATANGAN PENYELIA)

Alamat tetap : 4D-02-19,
Lorong Semarak Api 1, 11500
Pulau Pinang, Malaysia

DR. SITI RAHAYU
Nama Penyelia

Tarikh : _____ Tarikh: _____

INVESTIGATING DROIDKUNGFU4 ANDROID MALWARE BEHAVIOR THROUGH DYNAMIC ANALYSIS

KOAY SOON LEE

This report is submitted in partial fulfillment of the requirement for the Bachelor of Computer Science (Computer Networking)

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA
2013

DECLARATION

I hereby declare this project report entitled

INVESTIGATING DROIDKUNGFU4 ANDROID MALWARE BEHAVIOR THROUGH DYNAMIC ANALYSIS

is written by me and is my own effort and that no part has been plagiarized without citations.

STUDENT :_____ Date:_____

(KOAY SOON LEE)

SUPERVISOR:_____ Date:_____

(DR. SITI RAHAYU SELAMAT)

DEDICATION

This work is dedicated to my beloved family and siblings, who passed on a love of reading and respect for education.

To my supportive friends, my supervisor and all lecturers, thank you so much for assist and help.

ACKNOWLEDGEMENTS

I would like to show my gratitude and appreciation to my supervisor, Dr. Siti Rahayu Selamat for all the advices in guiding me throughout the project.

I would also like to thank my parents because they have given me the greatest support in all sorts of materials throughout my years of studying in this university.

Last but not least, I would like to thanks to all my friends and course mates for their kindness in sharing knowledge and resources.

Thanks a lot.

ABSTRACT

This project identifies the behaviours of Android malware and generates attack pattern through dynamic analysis. In the end of this project a script is created to verify the malware, DroidKungFu4 by the attack pattern of this malware. In this project, a step by step on configuring and carry out the dynamic analysis is provided as a guide for Android users so that they could protect their properties by carrying out the analysis following the guide. The behaviour of malware is difficult to identify and detect as the behaviour of each malware are varies. The objective of this project is to investigate the parameter, generate attack pattern of malware and develop a script to detect DroidKungFu4 malware. The project started with a literature review on malware then follow by plan on how to capture data of the malware for analysis. After the analysis on captured data has been done, then a script is designed. The main tools used in this project are Android SDK, and NetBeans. From the analysis result, DroidKungFu4 malware is a rootkit malware, which will try root the dhost device and scan for tainted file create by other variant of DroidKungFu malware. As it fails to root the host device, thus it can said that it is not a very harmful malware. Meanwhile, this project is to help end-user from being exploited by malware and to provide a prevention knowledge.

ABSTRAK

Projek ini mengenal pasti tingkah laku Android malware dan menghasilkan corak serangan melalui analisis dinamik. Pada akhir projek ini skrip yang dicipta untuk mengesahkan malware, DroidKungFu4 oleh corak serangan malware ini. Dalam projek ini, satu langkah demi langkah mengkonfigurasi dan menjalankan analisis dinamik disediakan sebagai panduan untuk pengguna Android supaya mereka boleh melindungi harta benda mereka dengan menjalankan analisis mengikuti panduan ini. Tingkah laku malware adalah sukar untuk mengenal pasti dan mengesan sebagai tingkah laku setiap malware adalah berbeza-beza. Objektif projek ini adalah untuk menyiasat parameter, menjana corak serangan malware dan membangunkan skrip untuk mengesan DroidKungFu4 malware. Projek ini bermula dengan kajian literatur mengenai malware kemudian diikuti dengan rancangan bagaimana untuk menangkap data daripada malware untuk analisis. Selepas analisis ke atas data yang ditangkap telah dilakukan, maka skrip yang direka. Alat utama yang digunakan dalam projek ini adalah Android SDK, dan NetBeans. Dari hasil analisis, DroidKungFu4 malware adalah malware rootkit, yang akan cuba akar peranti dhost dan mengimbas fail tercemar mencipta oleh varian lain DroidKungFu malware. Kerana ia gagal untuk akar peranti tuan rumah, oleh itu ia boleh berkata bahawa ia bukan malware sangat berbahaya. Sementara itu, projek ini adalah untuk membantu pengguna akhir daripada dieksploitasi oleh malware dan menyediakan pengetahuan pencegahan.

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVATIONS

API	Application Programming Interface
ARM	Acorn RISC Machine
C&C	Command & Control
DoS	Denial of Service
DS	Data Set
FTP	File Transfer Protocol
GPS	Global Positioning System
IOS	Internetwork Operating System
ID	Identifiers
DKF4P	DroidKungFu4 Prevention
OS	Operating System
RATC	Rage Against The Cage

CHAPTER 1

INTRODUCTION

1.1 Background

Malware, short for malicious (or malevolent) software, is software used or created by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. The type of malware that would like to analyze in this project would be android malware.

Smartphones has become popular from one year to another year in these few years. In this growing market of smartphones, Android, an open source platform of *Google* has become one of the most popular Operating Systems. Android is mainly used in smartphones and tablets. As Smartphone are able to provide services likes social networking, banking and so on, thus it become a primary choice of phone by a lot of people now a day. It comes with a lot features that are needed in our daily life likes Wi-Fi and GPS. There are a number of factors that help Android achieve this, the main reason is that a lot mobile phone companies will manufacture smartphones with Android operating system and has support from Google.

Recently, malwares has been spread through a lot kind new propagation medium. For example, through links of twitter tweet, permission while installing android applications (Sanzgiri,. Joyce & Upadhyadya 2011). Permission based malware will appears while the user trying to install the application and asked permission from user to get sensitive information likes get location of user, access internet and access bluetooth devices.

For twitter, it is choose as the propagation medium by as it can provide a high propagation rate for the malware. Those malwares are hidden in the link that have in the twitter. Thus, the malware can be easily infect or attack on those user who clicked on those links and it will help the hacker to get more sensitive information of those user in shorter before the malware is being detected. Furthermore, some malware is set and hide by the hacker inside popular programs name likes MatLab and Adobe Creative Suite.

This project is going to analyze the behaviour of malware using reverse engineering. Reverse engineering is the process of discovering the technological principles of a device, object, or system through analysis of its structure, function, and operation.

1.2 Problem Statement

Malware, as it is a software which will affect the parameter on android and thus it is difficult to analyse as the variety of malware is increasing rapidly nowadays. Somehow, the function of each malware might slightly different from each other. The Research Problem (RP) is summarized into Table 1.1.

Table 1.1 Summary of Research Problem

No.	Research Problem
RP1	Difficulty on identifying and detecting behavior of android malware

1.3 Research Question

Thus, one Research Questions (RQ) is constructed to identify the research problem as discussed in previous section is depicted in Table 1.2.

Table 1.2 Summary of Research Question

RP	RQ	Research Question
RP1	RQ1	What is the parameter use to study the behaviour of android malware?
	RQ2	What is the behaviour of android malware
	RQ3	What is the procedure of extracting the behaviour

RQ1: What is the parameter use to study the malware?

This research question is to find out the suitable parameter to be use to study on the behaviour of android malware. It is important to determine which parameter to be use as each type of malware infect on different parameter.

RQ2: What is the behaviour of android malware?

This research question is to find out the behaviour of android malware and identify suitable techniques to use to collect the data.

RQ3: What is the procedure of extracting the behaviour?

This research question is to find out the step used to identify the behaviour of the android malware.

1.4 Project Objective

From the research problem and question, the project objective has been determined. The project objective is depicted in Table 1.3.

Table 1.3 Summary of Project Objective

RP	RQ	RO	Objectives
RP1	RQ1	RO1	To investigate the parameter of android malware behaviour
	RQ2	RO2	To generate the attack pattern of malware
	RQ3	RO3	To formulate the procedure of extracting the attack pattern(script)

RO1: To find suitable parameter to study the behaviour of malware

Parameter is something that must be have in order to start an analysis. As malware might behave in different way due to its purpose, thus, a lot parameter might involve in the analysis.

RO2: To generate the attack pattern of malware

After the parameter used to analyse the malware is determined, thus the next step is to collect data and analyse the data to generate the attack pattern of malware.

RO3: To formulate the procedure of extrating the attack pattern

From the profiled the behavior of malware, thus a will formulate the procedure and develop a script to extract the behaviour fromm the data collected.

1.5 Research Contribution

The research contributions of this project are summarized in Table 1.4.

Table 1.4 Summary of Research Contribution

RP	RQ	RO	RC	Research Contribution
RP1	RQ1	RO1	RC1	The parameter use to analyse the malware behaviour
	RQ2	RO2	RC2	The attack pattern of android malware
	RQ3	RO3	RC3	The script to extract malware attack pattern

1.6 Project Scope

The scopes of this project are as follow:

1. The research only research on one specified malware, named DriodKungFu4.

2. Focus on investigate the parameter on system call to study the behaviour of malware.
3. Focus on dynamic analysis method, which is used to study the behaviour of malware.

4. Develop script from collected data to extract the behaviour of malware.

1.7 Expected Output

The behaviour of malware will be converted into a data form to be used as a further research on new malware. Through the analyze of malware, we can get know how they design the malware in order to take the advantage from the vulnerability of system and from that we can build up some prevention to prevent those black hat hacker exploit on these vulnerability.

1.8 Report organization

i) **Chapter 1: Introduction**

This chapter will discuss about introduction, project background, research problem, research question, research objective, scope, project significant and report organization.

ii) **Chapter 2: Literature Review**

This chapter will explain related work of this project, such as network traffic, system parameter and malware type.

iii) **Chapter 3: Methodology**

This chapter will explain the method use to analyse the malware and organise the sequence of project work in phase by phase.

iv) **Chapter 4: Design and Implementation**

This chapter will introduce the software and hardware use in this project, environment setup. Implementation of script will also include in this chapter

v) **Chapter 5: Testing and Result Analysis**

This chapter will analyse the collected data and carry out the test on malware using the developed script.

vi) **Chapter 6: Conclusion**

This chapter will summarized all chapters as a conclusion.

1.9 Summary

In this chapter, the research objective has been clearly determined as well as the plan to conduct the analysis. Suitable parameters must be selected in order to make the analysis of malware behaviour can be conducted as well as accurate information can be recorded. The behaviour of malware will be study from the information recorded during the analysis.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

In this chapter, a literature review about the types of android as well as malware will be discussed. Techniques and parameter used to conduct the analysis of malware behavior will also be discuss in this chapter as shown in Figure 2.1.

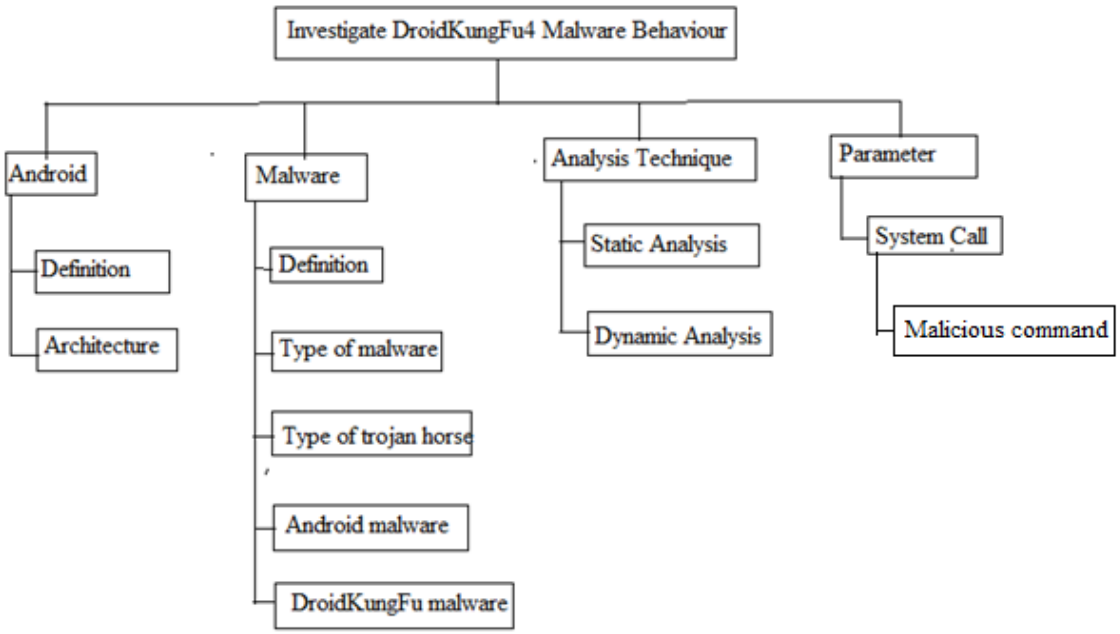

Figure 2.1 Operational framework: Literature review phase

2.2 Android

2.2.1 Definition of Android

Android is an operating system developed by Google. Basically it was started by some other company which was taken by Google and improved by Google to make it a open source platform. It was widely adapted over the world. As it is open source it is so popular amongst the smartphones and tablets PCs.

2.2.2 Architecture of Android

This section will explain the architecture of android as shown in Figure 2.2.

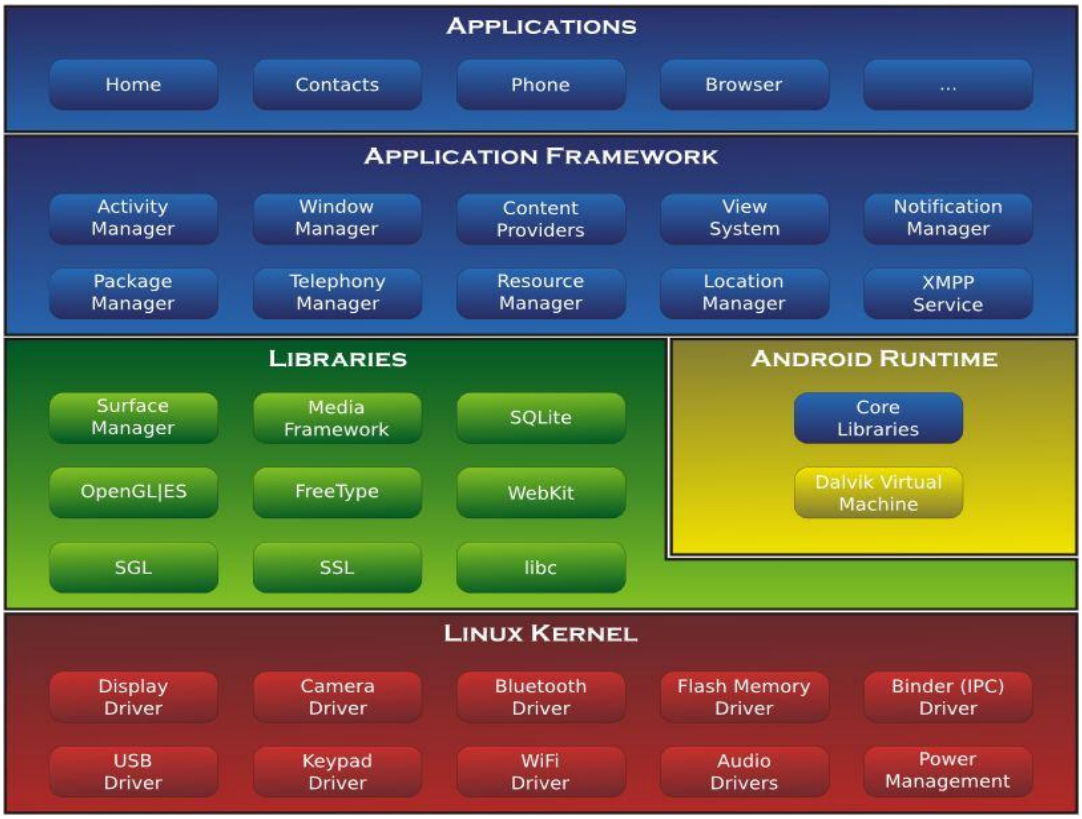

Figure 2.2: Architecture of android

Figure 2.2 shows that Android consists of a kernel based on Linux Kernel, libraries and APIs written in C. The central component of Android is a Linux-based kernel that provides a bridge between the hardware of the device and the rest of the software components of the system. For this reason, it is possible to access an Android device using a remote Linux-based shell and execute commands to list the contents of a current directory in the system. Also, it is possible to port some tools commonly used in Linux to execute them in Android but, to accomplish that, it is necessary to generate an executable code for an ARM platform, which is the principal processor for Android devices (Carios, 2011).

2.3 Malware

2.3.1 Definition of malware

From the research paper and previous works of other related research, malware is define as a software that "deliberately fulfils the harmful intent of an attacker" is commonly referred to as malicious software or malware (Moser, 2007).It is a code which interrupt the kernel of operating system or security sensitive application without the user assent and in a stealthy way which hard to detect those changes by using the documented features of the application or operating system.

2.3.2 Type of malware

Malware is classified into 6 major types as discussed in, (Egele, Scholte, Kirda, & Kruegel, 2012), which are:

a) Computer virus

Computer virus is a malicious program which is able to duplicate itself. Virus can infect computer from one to another if the infected file is copied to another computer. The purpose of virus is mainly to destruct on the target victim. Virus also spread through internet download. It can be mask by any files type such as graphic, video and audio. Virus will delete the data on the infected computer and spread itself to other using e-mail.

b) Worms

Worm is an malicious program which also able to duplicate itself, like virus. But worms have something that different from viruses is that it is able to spread through network, unlike virus which need to directly interact with the devices then only can infect on it.

c) Trojan

Trojan horse is a type of destructive program or virus which most of the time release by an email attachment. It will steal sensitive information such as account and pin numbers from the infected computer then send these information back to theft's database. Trojan horse itself is destructive but unlike worm and viruses, it does not duplicate itself.

d) Spyware

Spyware is normally correlative with advertisement in the web. Sometimes, spyware is installed into while the user clicks on the fake options on pop windows of a page or implemented inside a shareware or freeware. Most of time, spyware is to theft data, change configuration of the infected computer and trace activities of the user.

e) Bot

A bot is a piece of software which allows the developer of the bot, the bot master to gain control on the infected system. Bots are commonly instructed to send spam emails
or perform spyware activities.

f) Rootkit

Rootkit is a piece of software, which used to hide malware from being detected. It allows virus and malware to hide as an disguising as an necessary files which would not be suspect by the antivirus software. As rootkit is activated before operating system even boots up, therefore it is very hard to detect and thus provide a powerful way for attackers to access and use the targeted computer without the owner's notice.

2.3.3 Type of Trojan Horse

Trojan Horse is divided into 7 big types (OWASP, 2009). Figure 2.3 shows the type of Trojan Horse.

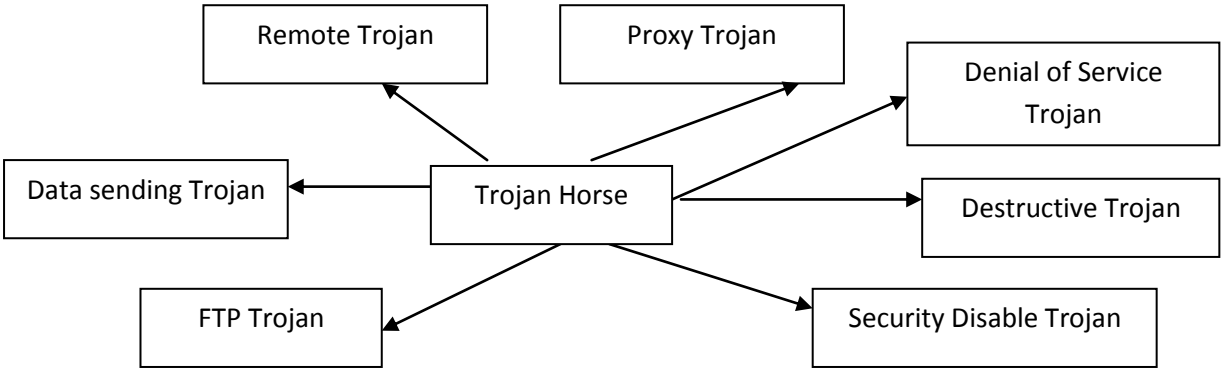

Figure 2.3 Type of Trojan horse

Table 2.1 summarized the functions of each type of Trojan Horse malware is shown respectively.

Table 2.1 Type of Trojan horse and function

Type	Function
Remote Access Trojan	Designed to provide the attacker with complete control of the victim's system.
Proxy Trojan	Designed to allow the hacker to use the victim's computer as an proxy server. This might use by the hacker to turn the victim's computer into zombie to attack other computers.
Denial of Service(DoS) Trojan	This type of trojan attack and bring down the network by flooding the entire network with unnecessary traffic.
Destructive Trojan	Designed to delete, erase the data on the victim's computer
Data sending Trojan	Desgined to collect and send sensitive data from the victim's computer to its server.
FTP Trojan	Designed to open port 21 to allow the hacker to connect to the victim's computer using FTP.
Security Disable Trojan	Kill or stop computer security software to operate which have in the victim's computer likes firewall and antivirus software.