BORANG PENGESAHAN STATUS TESIS*

JUDUL : ANALYSIS OF ANDROID MALWARE (DROIDKUNGFU 2) THROUGH THEIR BEHAVIOR USING STATIC ANALYSIS

SESI PENGAJIAN : 2010 / 2011

Saya ALIAA SYAHIRAH BT ABD RASHID mengaku membenarkan tesis Projek Sarjana Muda ini disimpan di Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dengan syarat-syarat kegunaan seperti berikut:

Tesis dan projek adalah hakmilik Universiti Teknikal Malaysia Melaka.

Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan untuk tujuan pengajian sahaja.

Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.

** 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 Kelompok 5, Block A-2-18, Kuarters KLIA, 71800 Nilai, Negeri Sembilan.	PROF MADYA Dr. MOHD FAIZAL BIN ABDOLLAH Nama Penyelia
Tarikh: ________	Tarikh: ________

CATATAN: * Tesis dimaksudkan sebagai Laporan Projek Sarjana Muda (PSM).
** Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa.

ANALYSIS OF ANDROID MALWARE (DROIDKUNGFU 2) THROUGH THEIR BEHAVIOR USING STATIC ANALYSIS

ALIAA SYAHIRAH BT ABD RASHID

This report is submitted in partial fulfilment of the requirements for the
Bachelor of Computer Science (Computer Networking)

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA
2013

DECLARATION

I hereby declare that this project report entitled

ANALYSIS OF ANDROID MALWARE (DROIDKUNGFU 2)

THROUGH THEIR BEHAVIOR USING STATIC ANALYSIS

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

STUDENT : ALIAA SYAHIRAH BT ABD RASHID
Date : 29 Ogos 2013

SUPERVISOR : PROF MADYA DR. MOHD FAIZAL BIN ABDOLLAH
Date : 29 Ogos 2013

DEDICATION

This project is especially dedicated to my lovely parents who have inspired me all this while. They thought me to solve the entire problem calmly instead of run from it. Without their sincere love and continuous support for me, this research may not be successfully complete. I would like to dedicate this research project work to my family and all my fellow friends for giving me fully encouragement to complete this research project. Not forgotten, I dedicate this work to my supervisor for his guidance, encouragement, and support for the sake of this project completion.

Thanks to Allah SWT for giving me such a good health condition and guidance to accomplish this research project

ACKNOWLEDGEMENTS

First and foremost, we would like to thank to our supervisor of this project, Dr Mohd Faizal Bin Abdollah for the valuable guidance and advice. He inspired us greatly to work in this project. His willingness to motivate us contributed tremendously to our project. We also would like to thank his for showing us some example that related to the topic of our project. Besides, we would like to thank the authority of Technical Malaysia University (UTeM) for providing us with a good environment and facilities to complete this project. Finally, an honourable mention goes to our families and friends for their understandings and supports on us in completing this project. Without helps of the particular that mentioned above, we would face many difficulties while doing this project.

ABSTRACT

Smartphones is now one of the gadgets that widely used; it has greatly stimulated the spread of mobile malware, especially on Android platform. Android phones are one of the smartphones that were and continue to be a main target of hackers. Thus, this research is about analysis of Android Malware DroidkungFu 2 through static analysis. There are two types of analysis can be done which is dynamic analysis and static analysis. But then, these researches focus only on the static analysis. The analysis will be implemented with the use of reverse engineering tools such as apktool, dex2jar, and jdgui. The reverse engineering technique is used to manipulate a legitimate application into a malware. Generally, this research took about six month to complete. At the end of this research, procedure of extracting the attack pattern (script) will be formulated.

ABSTRAK

Telefon pintar kini merupakan salah satu alat komunikasi yang digunakan secara meluas, ia telah banyak merangsang penyebaran malware mudah alih, terutamanya pada sistem operasi Android. Telefon Android adalah salah satu daripada telefon pintar yang telah dan terus menjadi sasaran utama penggodam. Oleh itu, kajian ini adalah mengenai analisis Android Malware DroidkungFu 2 melalui analisis statik. Terdapat dua jenis analisis boleh dilakukan iaitu analisis dinamik dan analisis statik. Tetapi, kajian ini memberi tumpuan hanya kepada analisis statik. Analisis ini akan dilaksanakan dengan penggunaan alat-alat kejuruteraan terbalik seperti apktool, dex2jar, dan jdgui. Teknik kejuruteraan terbalik digunakan untuk memanipulasi aplikasi yang sah ke dalam malware. Secara amnya, kajian ini mengambil masa kira-kira enam bulan untuk disiapkan. Pada akhir kajian ini, prosedur mengeluarkan corak serangan (skrip) akan digubal.

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

CHAPTER I

INTRODUCTION

1.1 Introduction

In recent years, there is an explosive growth in smartphone sales and adoption. Unfortunately, the increasing adoption of smartphones comes with the growing prevalence of mobile malware. Malware is short for “malicious software” as that is precisely what it is. Malware defines an entire class of malicious software. Malware includes computer viruses, worms, Trojans, adware, spyware, crimeware, scareware, rootkits and other unwanted programs. Malware can not only be annoying to a computer user, but it can also end up being costly (What is Spyware).

Even programs that aren’t gathering a user’s personal data will most likely end up causing damage to the system that could be costly to fix. Smartphones is a mobile phone that offers more advanced computing ability and connectivity than a feature phone. Android is the world’s most popular mobile platforms, is also an operating system developed by Google. Android is based on Linux and offers a great deal operating system customization in widgets and over millions of apps. As the most popular mobile platform, Google’s Android overtook others to become the top mobile malware.

This project will use static analysis to analyse the malware where will focus on the behaviour of the malware by using the parameter such as network traffic through HTTP connection, TCP flag, DNS, payload, system call, storage, memory utilization and processor utilization will be inspect.

The goal of this project is to understand the working of an android malware. It needs to overcome it before it getting serious. However, we need to identify the behaviour and understand how it works before we can defend it.

As a result, an android environment of this project is conducted by using the emulator. The network is purposely infected by malware (DroidKongfu2) then, collect and analyze The network traffic is captured by using tcpdump tool. Tcpdump is a powerful command line interface packet sniffer and has ability to analyze network behavior by reading the detail of packets . The worm attack pattern is important in order to provide a clear view on how the attack has performed and from the result of it ,the attacker and victim also can be identified which will help how the crime is being committed.

1.2 Research Problem

Malware can spread fast, rapidly and will embed in other software. This characteristic cause the difficulty to detect and identify the malware. The Research Problem (PR) is summarized into Table 1.

Table 1.1: Research problem

No	Research Problem
1	Less understanding about the behaviour of malware and how the malware will affect the parameter

1.3 Research Question

Table 1.2 shows the research problems and research questions in this project.

Table 1.2: Research question

RP	RQ	Research Question
RP1	RQ1	What is the behaviour of android malware?
	RQ2	How to differentiate behavior of android during infection and normal condition?
	RQ3	What is the formulated procedure of extracting the attack pattern

RQ1: What is the behaviour of android malware?

This research question is formulated by considering the malware's parameter issue which is epidemic as highlighted in RP1 in Table 1.2. This RQ1 is the primary guides to formulate the research objectives (RO1) of this project.

RQ2: How to differentiate behavior of android during infection and normal condition?

This research question is formulated by considering the malware's behavior issue which is epidemic as highlighted in RP1 in Table 1.2. This RQ2 is the primary guides to formulate the research objectives (RO2) of this project.

RQ3: What is the formulated procedure of extracting the pattern?

This research question is formulated by considering the android's parameter issue which is epidemic as highlighted in RP1 in Table 1.2. This RQ3 is the primary guides to formulate the research objectives (RO3) of this project.

1.4 Research Objective

Based on the research questions founded in previous section, appropriate research objectives (RO) are developed as shown in Table 1.3.

Table 1.3: Research objective

RP	RQ	RO	Research Objective
RP1	RQ1	RO1	To identify the behavior of android malware
	RQ2	RO2	To differentiate behavior of android during infection and normal condition
	RQ3	RO3	To formulate the procedure of extracting the attack pattern (script)

RO 1: To identify the behavior of android malware.

While doing the analysis of android malware, we must investigate the behavior of DroidKongfu2 malware.

RO 2: To differentiate behavior of android during infection and normal condition.

Behavior of android durinf infection and normal condition will be differentiated.

RO3: To formulate the procedure extracting the attack pattern (script).

The procedure for extracting the attack pattern of Droidkungfu2 will be formulated.

1.5 Scope

Scope of project is going to be conducted as follows:

i. Analyzes only on one specific type of android malware – DroidKongfu2
ii. Focusing on generating the attack pattern of android malware.
iii. Focusing on static analysis which is analyzes the behavior of malware.
iv. Focusing on the formulating the procedure of extracting the attack pattern**.**

1.6 Expected Output

The clear evident and behavior of DroidKongfu2 will help in developing a method orsoftware toprotect the system from DroidKongfu2 malware and to minimum the risk of the malware to thesystem.

1.7 Research Contribution

For now, Android malware has become a major issue recently, by identifying patterns of behavior and generate android malware attacks will be of great assistance for people to understand how malware functional on Android. Therefore, the measures necessary precautions should be taken to avoid Android smartphone from malware attacks.

1.8 Report Organization

i. **Chapter 1: Introduction**

This chapter will discuss the 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 organize the sequence of project work 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 malware as well as the sample data collected.

v. **Chapter 5: Testing and Analysis**

This chapter will analyse the collected data and carry out the scripting proposed to support the evidence.

vi. **Chapter 6: Conclusion**

This chapter will summarized all chapters as a conclusion.

1.9 Conclusion

As a conclusion, at the end of this project, the behavior and effect of android malware (DroidKungFu2) will be identified, as well as the attack pattern of android malware that had been generated. For the next chapter which is literature review, will explain the related work of this project.

CHAPTER II

LITERATURE REVIEW

2.1 Introduction

In this chapter, the project will discuss about the literature review on android malware, system parameter and network traffic depends on the project's related work. From the literature review, the results of the literature review on issues of malware will cover three research objectives (RO1, RO2, and RO3), which is to recognize android malware behaviors, to generate the android malware and attack patterns as well as to develop procedures produce patterns of attack (script) that mentioned in Chapter 1.

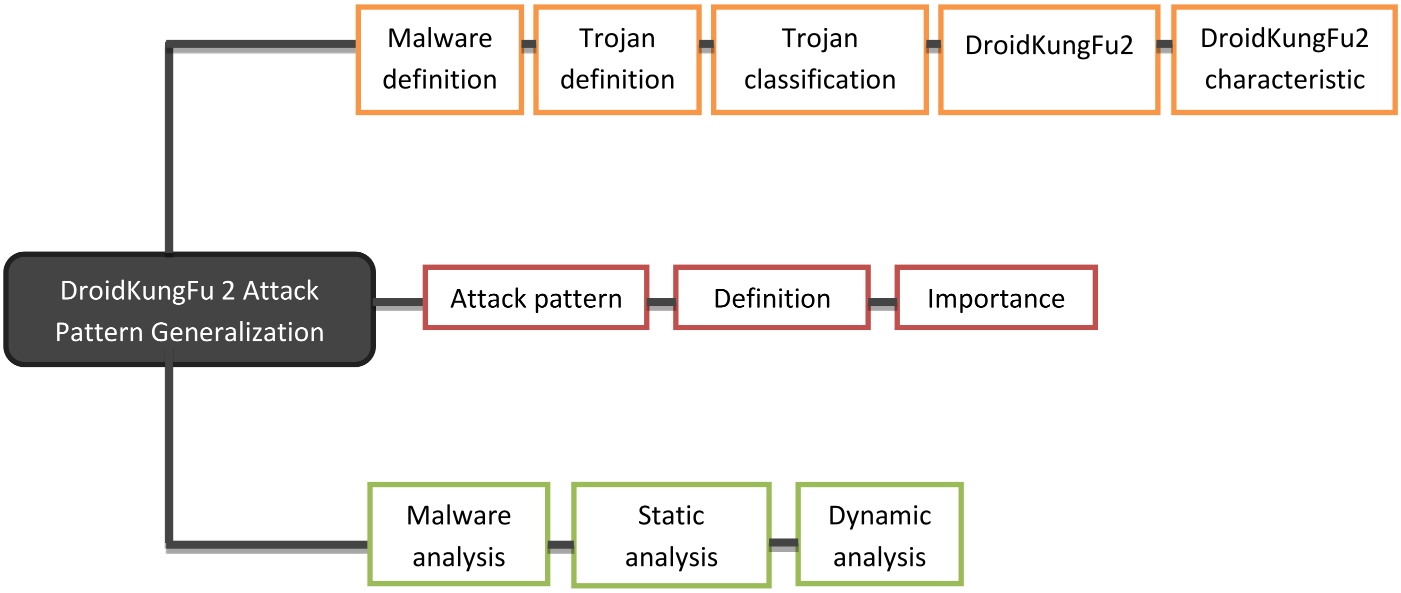

Figure 2.1: Literature review phase

In the literature review phase, more information on malware, attack pattern and malware analysis issues will discussed as shown in Figure 2.1. Other than that, all related literature like journals, websites, articles, book references and other sources are reviewed.

2.2 Related work

In this section, all the related work will be reviewed and discussed in detail.

2.2.1 Android

In recent years, there is an explosive growth in smartphone sales and adoption. Smartphone is a mobile phone that offers more advance computing ability and connectivity than a conventional phone. The mobile operating system for smartphone include Android, iOS, Microsoft's Windows Phone and others. It can be used for many different smartphone models, unless for the the iOS because the operating system by Apple for iPhone, iPad and other iDevices only.