BORANG PENGESAHAN STATUS TESIS*

JUDUL : Investigating Android Malware (Droidkungfu 4) Behavior Through Static Analysis

SESI PENGAJIAN : 2010 / 2011

Saya SITI NUR ATIKAH BT SHEIKH ABDUL HADI

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 hak milik 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 manapenyelidikan dijalankan)
_____	TIDAK TERHAD	

(TANDATANGAN PENULIS)	(TANDATANGAN PENYELIA)
Alamat tetap 174 Jln Kemuning 4, Taman Kemuning Senawang, 70450 Seremban, 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 atau TERHAD, sila lampirkan surat daripada pihak berkuasa.

INVESTIGATING ANDROID MALWARE (DROIDKUNGFU 4) BEHAVIOR THROUGH STATIC ANALYSIS

SITI NUR ATIKAH BT SHEIKH ABDUL HADI

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

INVESTIGATING BEHAVIOR OF ANDROID MALWARE (DROIDKUNGFU 4)

THROUGH STATIC ANALYSIS

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

_____

STUDENT : SITI NUR ATIKAH BT SHEIKH ABD HADI

Date : 28 OGOS 2013

_____

SUPERVISOR : PROF MADYA DR. MOHD FAIZAL BIN ABDOLLAH

Date : 28 OGOS 2013

DEDICATION

This paper is especially dedicated to my lovely and respective parents who have inspired me all this while. They thought me to face 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, Prof Madya 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

As 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 prime target of hackers. Thus, this research is about analysis of Android Malware DroidkungFu 4 through static analysis. There are two types of analysis can be done which is static analysis and dynamic analysis. But then, these researches focus on the static analysis only. The analysis will be carried out with the use of reverse engineering tools such as apktool, dex2jar, and jdgui. The reverse engineering technique is used to renovate 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

2.0 CHAPTER II: LITERATURE REVIEW

3.0 CHAPTER III: METHODOLOGY

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

1.1 Introduction

Nowadays, androids are the leading smartphone as well as outselling every other brand by a huge majority. Based on Linux and Java, users download applications from Google's Play Store (formerly Android Market), the Amazon Appstore and other online sources (see Google Play and Amazon Appstore). Android is a Linux-based OS specially design for touchscreen mobile phone developed by Google. Android is quite different and special because Google is actively developing the platform but giving it away with no charge to hardware manufacturers and phone carriers who want to use Android on their mobile devices.

Malware is short for malicious software, or a software used or created by attackers to disturb computer operation, collect sensitive information as well as trying to gain access to private computer systems. Malware takes the form of code, scripts, content and even legal software to obtain access to your computer and the personal information it houses. General term used by malware often referred as a variety of forms of hostile or intrusive software. Malware analysis is a process in which we take apart the malware for studying its code structure, operation and functionality.

This project will use static analysis to analyze the malware which will focus more on the behavior of the malware as well as the generated attack pattern of the android malware and the formulated procedure of extracting the attack pattern.

The goal of this project is to understand the behavior of an android malware. Android OS is now a popular environment or platform for mobile malware. Thus, we need to overcome it before it getting more serious. However, we need to understand how it works before we can overcome it.

An android environment of this project is conducted by using emulator. The network is purposely infected by sample of (DroidKungFu4) malware. Then, collect and analyze the sample. 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 Problem Statement

Table 1.1: Research Problems

No	Research Problem
1	Lack of understanding about how to formulate the procedure of extracting the attack pattern as well as lack of clear evidence on the malware behavior.

Table 1.2: Research Question

RP	RQ	Research Question
RP1	RQ1	What is the behavior of android malware?
RP2	RQ2	How to differentiate behavior of android during infected and normal condition?
RP3	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 1.1. This RQ1 is the primary guides to formulate the research objectives (RO1) of this project.

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

This research question is formulated by considering the malware's behavior issue which is epidemic as highlighted in RP2 in Table 1.1. 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 RP3 in Table 1.1. This RQ3 is the primary guides to formulate the research objectives (RO3) of this project.

1.3 Objective

Table 1.3: Research Objectives

RP	RQ	RO	Research Objective
RP1	RQ1	RO1	To identify the behavior of android malware.
RP2	RQ2	RO2	To differentiate the behavior of android during infected and normal condition.
RP3	RQ3	RO3	To formulate the procedure 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 DroidKongfu4 malware.

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

Behavior of android during infected and normal condition will be differentiated.

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

The procedure for extracting the attack pattern of Droidkungfu4 will be formulated.

1.4 Scope

Scope of project is going to be conducted as follows:

i. Analyzes only on one specific type of android malware – DroidKongfu4
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**.**

1.5 Expected Output

The clear evident and behavior of DroidKongfu4 will help in developing a method or software to protect the system from DroidKongfu4 malware and to minimum the risk of the malware to the system.

1.6 Research Contribution

As the Android malware has been a big issue recently, identify the behavior and generate attack pattern of android malware will be a big help for us to understand on how the malware works on Android. Thus, precaution step can be taking in order to prevent Android's smartphone from being attack by malware.

1.7 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 output collected.

v) Chapter 5: Testing and Analysis

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

vi) **Chapter 6: Conclusion**

This chapter will summarized all chapters as a conclusion.

1.8 Conclusion

As a conclusion, at the end of this project, the behavior and effect of android malware (DroidKungFu4) 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

2.1Introduction

In this chapter, the project's related work such as an android malware and attack pattern will be discussed. Basically, findings from the literature review about the malware issues will cover the three research objectives (RO1, RO2, and RO3) which is to identify the behavior of android malware, to generate the attack pattern of android malware and as well as to formulate the procedure extracting the attack pattern(script) that have been stated in Chapter 1

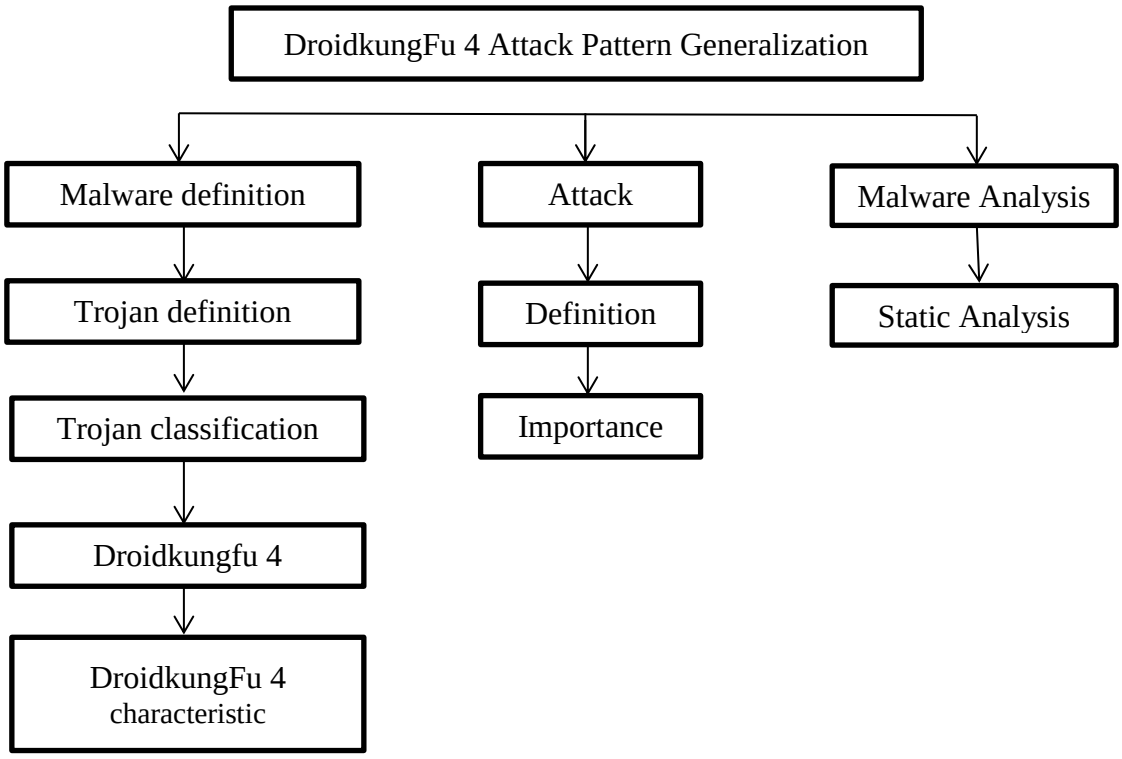

Figure 2.1: literature review phase

In the literature review phase, further discussion on malware, attack pattern and malware analysis issues will be discussed in details. In addition, all the relevant literature sources like articles, journals, thesis, websites and other sources are reviewed.

2.2 Related Work

2.2.2 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 includes 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.

Android is a operating system that designed for touch screen mobile devices and delivers full set of software. Android is an open source and all application can be used by any manufactures of device except for smartphone like iOS because they have their own operating sytem to operate. It's also give a world-class platform for fast and easy creating applications for Android user everywhere. Android is continuously pushing the boundaries of hardware and sofware forward to bring new capabilities to users.

Android is the best power device from some of the best smartphone and tablet manufactures in the world, like Samsung,HTC,Sony and more. Some local manufactures such as Micromax, Karbon, Hawai also use android phones on their portable devices.

Android is one the hottest and popular mobile operating systems for mobile devices available today. Samsung is the Largest Manufacturer of android phones and tablets. LG, HTC, Sony, are other top manufacturers of android phones and tablets. Some other local manufacturers such as Micromax, Karbon, Hawai, also use android Phones on their portable devices.

2.2.2 *Malware*

Malwares are evolving in a rapid manner and combat measures to stop them have become difficult because they use new signatures, encapsulation which prevents it from being detected. Anti-Virus products have been releasing daily updates which detect almost all the attacks,

some of them narrowly escape. It is essential that a reverse engineer must analyze such malwares which change the registry values, tamper data, and download payloads in short which shows unusual behavior. Reverse Engineer must analyze malware of that particular Operating system and study the environmental variables and activity performed by that malicious software.

According to (Panda Labs, 2013) Panda Security's anti malware laboratory had published its Quarterly Report for Q1 in which it analyzed the IT security events and incidents from January through March 2013. From the report published, trojans continue to dominate the threat landscape, representing nearly three out of every four new malware samples in circulation and almost similar numbers to those of in 2012. Panda Lab's reports come out with the graph of malware distribution as shown in the Figure 2.2 and Figure 2.3 below.

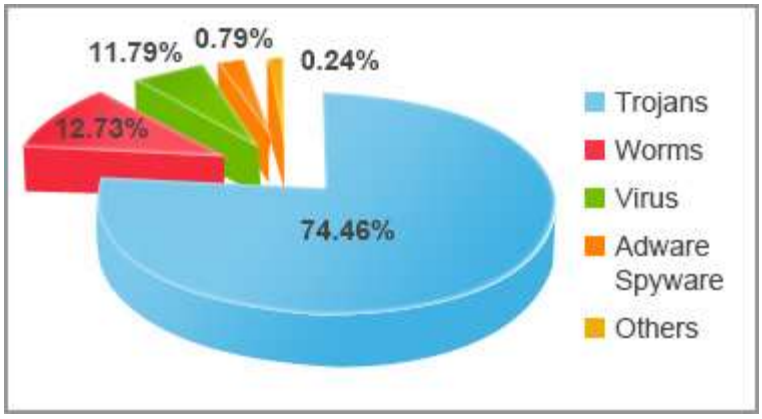

Figure 2.2: New Malware Distributions (Panda Labs, 2013)