BORANG PENGESAHAN STATUS TESIS*

JUDUL: INVESTIGATE ANDROID MALWARE'S BEHAVIOUR THROUGH

DYNAMIC ANALYSIS (ANSERVERBOT)

SESI PENGAJIAN: 2012 / 2013

Saya JEEVA A/L KUMAR

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)

Alamat tetap: 138-B, TINGKAT 2,
WISMA SENTOSA, JALAN SULTAN
ZAINAL ABIDIN, K. TERENGGANU

Tarikh:

(TANDATANGAN PENYELIA)

PROF MADYA DR. MOHD
FAIZAL BIN ABDOLLAH
Nama Penyelia

Tarikh:

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

INVESTIGATE ANDROID MALWARE'S BEHAVIOUR THROUGH DYNAMIC ANALYSIS (ANSERVERBOT)

JEEVA A/L KUMAR

This report is submitted in partial fulfillment 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 this project report entitled

INVESTIGATE ANDROID MALWARE'S BEHAVIOUR THROUGH DYNAMIC ANALYSIS

(ANSERVERBOT)

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

STUDENT :______________________________ Date:_____________

(JEEVA A/L KUMAR)

SUPERVISOR:______________________________ Date:_____________

(PROF MADYA DR. MOHD FAIZAL BIN ABDOLLAH

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 the assist and help.

ACKNOWLEDGEMENT

Thanks to Al-Mighty God, who with His willing give me the opportunity to complete this Final Year Project which entitled “Investigating Android Malware (AnserverBot) Behaviour through Dynamic Analysis”. This final year project report was prepared for Faculty of Information and Communication Technology (FTMK), Universiti Teknikal Malaysia Melaka (UTeM), basically for final year students to complete the undergraduate program that leads to the completion of degree of Bachelor of Computer Science.

First of all, it is a honor for me to wish a million of thank you to my supervisor, Prof Madya Dr. Mohd Faizal Bin Abdollah for his technical guidance and valuable time in assisting me in the accomplishing this project. I also would like to convey my sincere thank you wishes to all the lecturers and staffs involved for their full cooperation and moral support when I needed the most in completing my final year project with success.

Lastly, deepest thanks and appreciation to my parents, family, friends, and others for their fruitful support for the report completion start from the beginning till the end of this project. Besides that, I would also like to thank all of my friends and everyone that has being contributing by giving motivating support in completing my final year project with success.

ABSTRACT

Nowadays, the growth of android-based Smartphone's is growing rapidly and the unfortunate issue is that android malware too growing as rapid as well simultaneously. The popularity and adoption of Smartphone's has greatly stimulated the spread of mobile malware, especially on the popular platforms such as Android. Malware or malicious software is software that is residing in a system and cause harm to the system. The most well-known android malwares such as DroidKungFu, Goldream, BeanBot and AnserverBot are the major threats to the users of the Smartphone's. In light of their rapid growth, there is a pressing need to develop effective Therefore, analysis of the behavior of these malware attacks need to be studied in order to control the unwanted growth of android malware. That's what this project is merely all about. Introducingly android malware analysis whereby it is a process in which the malwares' code structure, operational and functionality are being analyzed deeply. The analysis consists of two types namely static analysis and dynamic analysis. The objectives of this project are to investigate the behavior of android malware through dynamic analysis, to identify and profile the behavior of android malware based on the parameter and lastly to differentiate the parameter of android during the infection and normal condition. In order for the project to be conducted and also to be completed in a right manner and correct sequence, there are total of five phases involved in the project methodology. The phases are in ascending sequence which are literature review, analysis, design and development, implementation and lastly testing and evaluation phases. The expected outcomes would be the results from disassembly malwares will varies and gain a clear understanding in identify the android malware's behavior in order to imagine an effective measure that can be practically developed.

ABSTRAK

Pada masa kini, pertumbuhan Smartphone android berasaskan adalah berkembang pesat dan isu yang malang ialah malware android juga berkembang sebagai pesat serta pada masa yang sama. Populariti dan penggunaan Smartphone telah banyak merangsang penyebaran malware mudah alih, terutama pada platform popular seperti Android. Perisian malware atau berniat jahat adalah perisian yang tinggal dalam sistem dan menyebabkan kerosakan kepada sistem. Yang paling terkenal android malwares seperti DroidKungFu, Goldream, BeanBot dan AnserverBot adalah ancaman utama kepada pengguna Smartphone ini. Memandangkan pertumbuhan pesat, terdapat satu keperluan mendesak untuk membangunkan berkesan Oleh itu, analisis tingkah laku serangan malware perlu dikaji untuk mengawal pertumbuhan yang tidak diingini android malware. Itulah yang projek ini adalah semata-mata semua tentang. Introducingly android analisis malware di mana ia adalah satu proses di mana struktur kod malwares ', operasi dan fungsi sedang dianalisis secara mendalam. Analisis ini terdiri daripada dua jenis iaitu analisis statik dan analisis dinamik. Objektif projek ini adalah untuk menyiasat tingkah laku android malware melalui analisis dinamik, untuk mengenal pasti dan profil tingkah laku android malware berdasarkan parameter dan akhir sekali untuk membezakan parameter android semasa jangkitan dan keadaan. Dalam usaha untuk projek yang dijalankan dan juga akan selesai dengan cara yang betul dan urutan yang betul, terdapat sebanyak lima fasa yang terlibat dalam metodologi projek. Fasa mengikut urutan menaik yang kajian literatur, analisis, reka bentuk dan pembangunan, pelaksanaan dan akhir sekali ujian dan fasa penilaian. Pencapaian yang dijangka akan menjadi hasil daripada malwares pemasangan akan berbeza dan mendapatkan pemahaman yang jelas dalam mengenal pasti tingkah laku malware android dalam usaha untuk membayangkan satu langkah yang berkesan yang boleh dikatakan maju.

TABLE OF CONTENTS

CHAPTER I INTRODUCTION

CHAPTER II LITERATURE REVIEW

CHAPTER V TESTING AND RESULT ANALYSIS

CHAPTER VI CONCLUSION

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

TERMS	DESCRIPTION
ADT	Android Developer Tools
APK	Application Package File
API	Application Programming Interface
C&C	Command-and-Control
DDMS	Dalvik Monitor Server
DNS	Domain Name Server
DoS	Denial-of-Service
DS	Data Set
HTTP	Hypertext Transfer Protocol
IDE	Integrated Development Environment
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPv4	Internet Protocol Version 4

OS	Operating System
PSM	Projek Sarjana Muda
RP	Research Problem
RQ	Research Question
RO	Research Objective
SDK	Software Development Kit
SIM	Subscriber Identity Module
TCP	Transmission Control Protocol
UA	User-Agent
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VM	Virtual Machine

CHAPTER 1

INTRODUCTION

This chapter basically discusses the project background, problem statements, objectives, scopes, project significance, report organization and the conclusion.

1.1 Project Background

The fast growth of Smartphone's which consists of various types of operating systems has become a trend for mobile phone users at least to own a piece. The most popular platform will be Android which is a linux-based open source operating system that gain the support of Smartphone users in the market nowadays. As to mention our disappointment, as the trend of growth of android-based Smartphone sliding higher nowadays, the growth of malware in the Smartphone is also increasing rapidly at the same time and causing serious concern among Smartphone user about the security breaching and malicious attacks. Malwares that are found on android-based smartphones are known as android malwares which are evolving in a rapid manner and effective measures to stop and control them have become difficult since new signatures and encapsulation have been used in order to prevent them from being detected. In attempt to control or stop the growth of malware, thorough analysis, study and investigation need to be applied. The popularity and adoption of Smartphone has greatly stimulated the spread of mobile malware, especially on the popular platforms such as Android. Malware or malicious software is software which found to be in the form of code and scripts that is residing in a system and causing harm and damage to the system. The most well-known android malwares such as DroidKungFu, Goldream, BeanBot and AnserverBot are the major threats to the users of the Smartphone. Based on the enormous growth of Android malware, an urgent effective prevention and detection technique needed to be developed and executed in order to reduce or even stop the increasing growth. Thus, analysis of the behaviour of these malware attacks needed to be studied in order to control the unwanted growth of android malware. That is what this project is merely all about. Introducingly android malware analysis whereby it is a process in which the malwares' code structure, operational and functionality are being analyzed deeply.

1.2 Problem Statements

Malware is widespread rapidly and is happened within seconds in network. This characteristic had leaded to difficulty to identify the malware's behavior. The Research Problem (RP) is summarized into Table 1.1.

Table 1.1 Summary of Research Problem

No.	Research Problem
RP1	Malware is an epidemic and leads to difficulty in identifying the behavior of the malware

Thus, one Research Question (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	How can we identify the behavior of the android malware?

RQ 1: How can we identify the behaviour of the android malware?

This research question is formulated by considering the malware's behaviour issue which is epidemic as highlighted in RP1 in Table 1.1. This research question (RQ) is the primary guides to formulate the research objectives (RO) of this project.

1.3 Objectives

Based on the research questions formulated in previous section, appropriate research objectives (RO) are developed as follows:

RO 1: To investigate the parameter of android malware's behaviour

In order to identify the behaviour of malware via dynamic analysis, firstly a study needed to be done to figure out the parameters involved. A sample of approximately 3 variants of the specific malware needed to be run to analyze its behavioural data such as system call, incoming and outgoing network traffic, memory utilization, CPU usage and other types of data during both normal and abnormal condition.

RO 2: To generate the attack pattern of android malware

The behavioural data captured from differentiating the parameter of android malware's behaviour during normal and abnormal condition through the android malware analysis will be gathered to be utilized in generating the attack pattern of the android malware.

RO 3: To formulate the procedure of extracting the attack pattern (script)

The attack pattern of android malware which actually will be in the form of script generated from the behavioural data will be analyzed and studied in order to investigate the malware behaviour through dynamic analysis.

The Research Objectives (RO) are summarized as show in Table 1.3 below.

Table 1.3 Summary of Research Objectives

RP	RQ	RO	Research Objectives
RP1	RQ1	RO1	To investigate the parameter of android malware's behavior
		RO2	To generate the attack pattern of android malware
		RO3	To formulate the procedure of extracting the attack pattern (script)

1.4 Scopes

It is essential to identify the scopes of the project in attempt to specify the path of the project paving to. Therefore, the scopes of the project are specified as follows:

- Only one specific type of malware will be analyzed and studied thoroughly which is the AnserverBot.
- Dynamic type of analysis will be used and focused instead of static type of analysis in analyzing the behaviour of malware.
- Behavioural data collected from the differentiation of the parameters of android malware's behaviour by the measure of various dynamic analysis tools which is the attack pattern of the android malware generated in the form of script that will be analyzed in order to identify and investigate the behaviour of the malware.

1.5 Project Significance

Results from disassembly malwares will vary as soon as the research completed. Thus, a clear understanding is needed to be acquired in identifying the android malware's behaviour in order to imagine an effective measure that can be practically developed. The behaviour and attack pattern of android malware will be much helpful in network security and forensic department to prevent android-based Smartphone from being attacked.

1.6 Report Organization

In attempt to make sure the project is progressing smoothly, report organization is very important as it is arranged accordingly chapter by chapter. The description and summarization of each chapter are been depicted as show below:

i. **Chapter 1: <u>Introduction</u>**

- This chapter will be discussing about introduction, project background, research problems, research questions, research objectives, scopes, project significant and report organization.

ii. **Chapter 2: <u>Literature Review</u>**

- In this chapter, related work or previous work of this project, analysis of current problem or justification and proposed solution for further project.

iii. **Chapter 3: <u>Methodology</u>**

- This chapter will be focusing on the methodology part whereby activities, steps and stages in completing this project are been exposed according to its sequence phase by phase for the category of analysis.

iv. **Chapter 4: <u>Design and Implementation</u>**

- In this chapter, hardware and software requirements will be introduced together with the environment setup, architecture network design, experimental design and simulation design and lastly the implementation of the project methodology along with the sample of output will be covered as well.

v. **Chapter 5: <u>Testing and Analysis</u>**

- This chapter will be explaining the steps and methods in testing and analyzing the collected data and also the comparative analysis of the result will be elaborated.

vi. **Chapter 6: <u>Conclusion</u>**

- In this last chapter of this project, an overall picture of limitations, contributions and future works will be summarized.

1.7 Summary

In conclusion, this project will be subjected to identify and also analyze the behaviour of android malware (AnserverBot) through dynamic analysis. In the next chapter, more research and study about the malware and its behavioural data will be carried out in the form of literature review.