INVESTIGATE MALWARE BEHAVIOR ON ANDROID PLATFORM

LOH KE LIH

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA
2014

BORANG PENGESAHAN STATUS TESIS

JUDUL: INVESTIGATE MALWARE BEHAVIOR ON ANDROID PLATFORM

SESI PENGAJIAN: SESI 2013/2014

Saya LOH KE LIH mengaku membenarkan tesis (PSM/Sarjana/Doktor Falsafah) 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 : 18, Jalan Khalidi,
84000 Muar,
Johor, Malaysia
Tarikh : _____

Nama Penyelia : En. Zulkiflee Muslim
Tarikh: _____

INVESTIGATE MALWARE BEHAVIOR ON ANDROID PLATFORM

LOH KE LIH

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
2014

DECLARATION

I hereby declare this project report entitled

INVESTIGATE MALWARE BEHAVIOR ON ANDROID PLATFORM

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

STUDENT :_____ Date:_____

(LOH KE LIH)

SUPERVISOR:_____Date:_____

(EN ZULKIFLEE BIN MUSLIM)

DEDICATION

To my beloved parents…

ACKNOWLEDGEMENTS

I would like to show my gratitude and appreciation to my supervisor, En Zulkiflee bin Muslim for all the ideas and advices in guiding me throughout the project.

I would also like to thank my family members especially 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, BaseBridge through dynamic analysis. Scope to be conducted in this project are using only one specific type of android malware and focusing on behaviour of android malware. Tcpdump will be used in this project to sniff the network. This research will be contributed in identifying the behavior of BaseBridge in respective network traffic by using Santoku Linux operating system which contains several tools such as Android SDK emulator, Wireshark and Tcpdump. In the end of this project, behaviour of BaseBridge will be concluded. However, there are several constraints and limitations on this project which is not fully fit for other android malwares' behaviours. For future works, a script can be generate and conducted into a complete software system, so that the processes of capture data can be done automatically by the system thus enhances the system fit for other android malwares.

ABSTRAK

Projek ini mengenal pasti tingkah laku malware Android, BaseBridge melalui analisis dinamik. Skop yang akan dijalankan dalam projek ini menggunakan hanya satu jenis tertentu Android malware dan memberi tumpuan kepada tingkah laku Android malware. Tcpdump akan digunakan dalam projek ini untuk mengesan rangkaian BaseBridge. Kajian ini akan menyumbang dalam mengenal pasti tingkah laku dalam BaseBridge trafik rangkaian masing-masing dengan menggunakan sistem operasi Linux Santoku yang mengandungi beberapa peralatan seperti Android SDK emulator, Wireshark dan tcpdump. Di akhir projek ini, tingkah laku BaseBridge akan dibuatkan kesimpulan. Walau bagaimanapun, terdapat beberapa kekangan dan batasan projek ini, iaitu tidak cergas sepenuhnya untuk tingkah laku lain malwares Android. Bagi kerja-kerja masa depan, skrip yang boleh dijana dan dijalankan ke dalam sistem perisian yang lengkap, supaya proses menangkap data boleh dilakukan secara automatik oleh sistem itu bagi meningkatkan sistem untuk malwares Android lain.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

FIGURE **TITLE** **PAGE**

LIST OF ABBREVIATIONS

ALPHABET	WORDS	EXPLANATION
A	APK	Android Application Package File
	ARP	Address Resolution Protocol
H	HTTP	Hypertext Transfer Protocol
T	TCP	Transmission Control Protocol
U	UDP	User Datagram Protocol
	URL	Uniform Resource Locator

LIST OF ATTACHMENTS

CHAPTER I

INTRODUCTION

1.1 Introduction

Nowadays, the mobile platforms and applications are increasing in popularity. However, the popular platform such as Android has greatly stimulated the spread of mobile malware. In order to identify the problem that cause mobile malware spread rapidly, we will discuss about the background of the project which is Android and malware. The research problem will be formulated into three research questions. Based on the research questions, the current problem that faced by the Android user will be clearly shown. After that, the research objective can be generated and all works done in this project will be based on the research objective.

Firstly, for the purpose to do this project, project background will be discussed. The background of Android platform and malware will be described. Secondly, the research problem will be summarised. After that the research question and objective will be conducted. Project scope and contribution will also be discussed. Lastly, the report organization will be described to make sure the project is carry out in correct flow.

1.2 Project Background

In recent year, the using of smart phone is increasing. There are several of operating system used in smart phone such as Android, IOS, Window, Blackberry and Symbian. Android is the most popular platform used in smart phone which is 79.0% compare to Apple IOS (14.2%), Windows Phone (3.3%), Blackberry (2.7%) and other (0.9%) (mobiThinking, 2014). Android is the largest installed platform and growing fast which placed first among others smart phone operating systems (Micheal Oleaga, 2014, Guru, 2014).

As more and more smart phones come out, the amount of people accessing the Internet greatly increases. So, there is a rapid increase in the amount of malware targeting Android smart phones since it is the most popular operating system used in smart phone. 99% of mobile malware targeted Android devices last year (Brad Reed, 2014).

Malware, short for malicious software, is software used to damage or control the computer operation, gather with sensitive information, or gain access to private computer systems. It can be emerged as a collection of code, script, active content and embedded in other application (McMahon, 2013). Therefore, a script can be generating in order to detect the android malware that found in the smart phones.

Examples of android malware such as DroidKungFu, BeanBot, BaseBridge are the major threats to the security of the android mobile. However, there are some malware will re-implementing some of their malicious functionalities in native code. The changes are possibly to make their detection and analysis harder. (Yajin Zhou, 2012). So, the parameter will be analyzing to know the attack pattern of the malware.

The malware are grows rapidly, some effectively defend should take against the malware. In order to create a method to defend against the malware, we need to study, analysis and investigate about the malware. We need to how the malware behaves when executed, how it got here, what is the purpose and how it runs (Kris Kendall, 2007).

Therefore, dynamic analysis will be using in this project to analyse the android malware. It will focuses on the behaviour of attack, determine how and what it gets installed, how it run, what files have been added or modified, who they are communicate to, etc (Dennis Distler, 2007). So, the parameter such as system call and network traffic will be investigate in this project.

1.3 Problem Statement

Nowadays, malicious code is reportedly infecting Android devices at a rapid speed. Therefore, Android phone users are advised to take extra precautions on this situation. However, the malware characteristics cause difficulty for users to identify and detect their behaviours. The Research Problem (PR) is summarized into Table 1.1.

Table 1.1 Summary of Problem Statement

No	Research Problem
RP1	Difficult to detect the appearance of android malware inside the smart phone because most of the anti-virus software is low accuracy.

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

Table 1.2 Summary of Research Question

No	Research Question
RQ1	What is the behaviour of different android malware?
RQ2	What is the parameter used to detect the android malware's behaviour?
RQ3	How to detect the android malware using parameter?

RQ1: What is the behaviour of different android malware?

This research question is used to study the behaviour of malware by identify which techniques is suitable to use for collecting data for different type of malware.

RQ2: What is the parameter used to detect the android malware's behaviour?

This research question is formulated by considering the android malware's behaviour issue because there are many different type of malware and that may infect to different parameter. Thus, it is important to identifying which parameter is suitable to use for study the malware's behaviour.

RQ3: How to detect the android malware using parameter?

This research question is formulated by considering the way to extract the behavior of the android malware using parameter and generate the attack pattern dynamically.

1.4 Objective

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

Table 1.3 Summaries of Research Objectives

RP	RQ	RO	Research Objective
RP1	RQ1	RO1	To classify the android malware's behaviour.
	RQ2	RO2	To identify the parameter used to detect the android malware's behaviour.
	RQ3	RO3	To detect the android malware using parameter.

RO1: To classify the android malware's behaviour.

Firstly, we need to classify the type of android malware and the behaviour of android malware in order to find out the feature of malware. Different type of malware may have different type of behaviour.

RO2: To identify the parameter used to detect the android malware's behaviour.

We need to investigate the suitable parameter used to identify the behaviour of android malware in order to generate the attack pattern of malware and do the detection

RO3: To detect the android malware using parameter.

After identify the parameter, we need to develop a script to detect the android malware automatically using its parameter.

1.5 Scope

Scope of project is going to be conducted as follows:

1. Using only one specific type of android malware.
2. Focusing on behaviour of android malware in order to generate the attack patterns of android malware by using network traffic.
3. Tcpdump and Wireshark will be used in this project to sniff the network.

1.6 Project Contribution

The contribution of this project are summarized in Table 1.4

Table 1.4 Summary of project contributions

RP	RQ	RO	RC	Research Contribution
RP1	RQ1	RO1	RC1	The classification of android malware's behaviour.
	RQ2	RO2	RC2	The parameter of android malware's behaviour.
	RQ3	RO3	RC3	Detecting the malware’s attack pattern using parameter.

Table 1.4 shows the project contributions based on the research problem, research questions and research objective.

1.7 Report Organization

Chapter 1: Introduction

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

Chapter 2: Literature Review

This chapter will study about the related works such as android, malware, malware attack pattern, malware analysis technique, parameter and operating system used. The related works will be contribute to the next chapter.

Chapter 3: Methodology

This chapter will explain the method used to analyse android malware and project methodology. Project schedule and milestones will discuss in this chapter to finish the project in time.

Chapter 4: Analysis and Design

This chapter will introduce the problem analysis, requirements of software and hardware. The experimental design such as logical design and physical design will also conduct in this chapter. Environment will setup based on the requirements.

Chapter 5: Implementation and Testing

This chapter will describe the method to implement and test the collected data in order to carry out the graph to support the evidence. The test result and analysis will conclude in this chapter.

Chapter 6: Conclusion

This chapter will summarize all chapters as a conclusion. Project summarization, limitation and future work will discuss.

1.8 Summary

As a conclusion, this project will identify the behaviour of Android malware using dynamic analysis. The problem statement, research questions, research objectives and scope are discussed in this chapter to identify and solve the problem. Besides that, report organization also carried out in this chapter to make sure the project runs in sequence. In the next chapter, more research and related works about Android malware and malware detection technique will be discussing.