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

# TABLE OF CONTENT

DECLARATION ...................................................................................................................... i
DEDICATION ......................................................................................................................... II
ACKNOWLEDGEMENTS ....................................................................................................... III
ABSTRACT ........................................................................................................................... IV
ABSTRAK .............................................................................................................................. V
LIST OF FIGURES ............................................................................................................ IX
LIST OF TABLES ............................................................................................................... XI
LIST OF ABBREVIATIONS ................................................................................................. XII

## CHAPTER 1 INTRODUCTION

1.1. Background .................................................................................................................. 1
1.2. Problem Statement ....................................................................................................... 2
1.3. Research Question ....................................................................................................... 2
1.4. Project Objective ......................................................................................................... 3
1.5. Research Contribution ............................................................................................... 4
1.6. Project Scope ............................................................................................................... 4
1.7. Expected Output ........................................................................................................... 4
1.8 Report Organization ................................................................................................... 5
1.9 Summary ....................................................................................................................... 5

## CHAPTER II LITERATURE REVIEW

2.1 Introduction .................................................................................................................. 6
2.2 Android ........................................................................................................................ 6
   2.2.1 Definition of Android ............................................................................................ 6
   2.2.2 Architecture of Android ....................................................................................... 7
2.3 Malware ....................................................................................................................... 8
   2.3.1 Definition of Malware ........................................................................................... 8
   2.3.2 Type of Malware .................................................................................................. 8
   2.3.3 Type of Trojan Horse .......................................................................................... 10
   2.3.4 Android Malware ............................................................................................... 11
   2.3.5 DroidKungFu Malware ....................................................................................... 11
2.4 Detection Technique ................................................................. 12
  2.4.1 Static Analysis ............................................................... 12
  2.4.2 Dynamic Analysis ......................................................... 13
2.5 Parameter .................................................................................. 13
  2.5.1 System Call ......................................................................... 13
2.6 Summary ..................................................................................... 15

CHAPTER 3 METHODOLOGY ............................................................. 16
3.1 Introduction ............................................................................... 16
3.2 Methodology ........................................................................... 16
  3.2.1 Phase 1: Literature Review ............................................. 17
  3.2.2 Phase 2: Analysis ............................................................. 17
  3.2.3 Phase 3: Design and Development ................................. 19
  3.2.4 Phase 4: Implementation ............................................... 19
  3.2.5 Phase 5: Testing and Evaluation ..................................... 19
3.3 Summary ................................................................................... 19

CHAPTER 4 DESIGN AND ANALYSIS ............................................. 20
4.1 Introduction ............................................................................... 20
4.2 Analysis Approach ................................................................... 20
  4.2.1 Software Requirement .................................................. 21
  4.2.2 Hardware Requirement ................................................. 22
4.3 Design ....................................................................................... 23
  4.3.1 Physical Design .............................................................. 23
  4.3.2 Logical Design ............................................................... 23
4.4 Implementation .......................................................................... 24
  4.4.1 Data Collection ............................................................... 24
4.5 Analysis of Data ........................................................................ 26
  4.5.1 Analysis of captured system call .................................... 26
4.6 Determine Attribute ................................................................. 28
4.7 Generate Attack Pattern ......................................................... 29
  4.7.1 Process Flow of DroidKungFu4 Attack ......................... 29
  4.7.2 Basic Attack Model ....................................................... 30
CHAPTER 5 TESTING AND RESULT ANALYSIS

5.1 Introduction ........................................................................................................... 35
5.2 Test Planning ........................................................................................................... 35
  5.2.1 Test Organization ............................................................................................... 35
  5.2.2 Test Environment .............................................................................................. 36
  5.2.3 Test Schedule .................................................................................................. 37
5.3 Test Strategy .......................................................................................................... 37
  5.3.1 Unit Testing ...................................................................................................... 37
5.4 Test Design ............................................................................................................ 37
  5.4.1 Test Data Set ..................................................................................................... 38
5.5 Test Result .............................................................................................................. 39
  5.5.1 Test Result of System call ................................................................................ 39
5.6 Result Analysis ...................................................................................................... 41
  5.6.1 System Call Analysis ....................................................................................... 41
5.7 Discussion of Result Analysis ............................................................................... 43
  5.7.1 Access tainted file and execution of root abuse command ......................... 44
  5.7.2 General Attack Pattern of DroidKungFu4 ...................................................... 45
5.8 Summary ................................................................................................................. 46

CHAPTER 6 CONCLUSION ....................................................................................... 47
6.1 Introduction ............................................................................................................. 47
6.2 Project Contribution ............................................................................................... 47
6.3 Constrain and Limitation ....................................................................................... 47
6.4 Further Work .......................................................................................................... 48

REFERENCES ............................................................................................................. 49
LIST OF FIGURES

Figure 2.1 Operational framework: Literature review phase.................................6
Figure 2.2 Architecture of android..................................................................7
Figure 2.3 Type of Trojan horse.................................................................10
Figure 2.4 Distribution of malware by platform...........................................11
Figure 3.1 Phases of malware analysis.........................................................16
Figure 4.1 Analysis approach........................................................................20
Figure 4.2 The spec of the workstation..........................................................22
Figure 4.3 Physical Design...........................................................................23
Figure 4.4 Logical Design............................................................................23
Figure 4.5 Flow chart of data collection on system call.................................24
Figure 4.6 Execution of root abuse command of malware..............................26
Figure 4.7: Sequence of directories involved in root abuse commands.............27
Figure 4.8 Scanning for tainted file..............................................................27
Figure 4.9 Malware fail to find tainted file......................................................27
Figure 4.10 Flow of attack process of DroidKungFu4......................................29
Figure 4.11 Basic Attack Model of DroidKungFu4..........................................30
Figure 4.12 Attack Pattern of DroidKungFu4..................................................31
Figure 4.13 Design of the script....................................................................32
Figure 4.14 DKF4P module..........................................................................32
Figure 4.15 Sample output of script...............................................................33
Figure 5.1 Test result of DS1........................................................................39
Figure 5.2 Test result of DS2........................................................................40
Figure 5.3 Test result of DS3.................................................................40
Figure 5.4 Sequence of execution of root abuse command..........................44
Figure 5.5 Data of root access command in system call log of DS2....................45
Figure 5.6 General attack pattern of DroidKungFu4........................................45
LIST OF TABLES

Table 1.1 Summary of Research Problem.................................................................2
Table 1.2 Summary of Research Question.................................................................2
Table 1.3 Summary of Project Objective.................................................................3
Table 1.4 Summary of Research Contributions.......................................................4
Table 2.1 Type of Trojan horse and function.........................................................10
Table 2.2 Rules and Signatures detection of Android Malware using dynamic analysis.....15
Table 4.1 Attribute for System Call........................................................................28
Table 5.1 Test Organization.....................................................................................36
Table 5.2 Software Requirement.............................................................................36
Table 5.3 Hardware Requirement.............................................................................36
Table 5.4 Test Schedule...........................................................................................37
Table 5.5 Description of data sets (DS1-DS3) .....................................................38
Table 5.6: Comparison of output of manual analysis and output of script (DS1) ..........41
Table 5.7: Comparison of output of manual analysis and output of script (DS2) ..........42
Table 5.8: Comparison of output of manual analysis and output of script (DS3) ..........42
Table 5.9 Comparison of result between different Data set....................................43
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>ARM</td>
<td>Acorn RISC Machine</td>
</tr>
<tr>
<td>C&amp;C</td>
<td>Command &amp; Control</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>DS</td>
<td>Data Set</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>IOS</td>
<td>Internetwork Operating System</td>
</tr>
<tr>
<td>ID</td>
<td>Identifiers</td>
</tr>
<tr>
<td>DKF4P</td>
<td>DroidKungFu4 Prevention</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>RATC</td>
<td>Rage Against The Cage</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>No.</th>
<th>Research Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>RP1</td>
<td>Difficulty on identifying and detecting behavior of android malware</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>RP</th>
<th>RQ</th>
<th>Research Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>RP1</td>
<td>RQ1</td>
<td>What is the parameter use to study the behaviour of android malware?</td>
</tr>
<tr>
<td></td>
<td>RQ2</td>
<td>What is the behaviour of android malware</td>
</tr>
<tr>
<td></td>
<td>RQ3</td>
<td>What is the procedure of extracting the behaviour</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>RP</th>
<th>RQ</th>
<th>RO</th>
<th>Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>RP1</td>
<td>RQ1</td>
<td>RO1</td>
<td>To investigate the parameter of android malware behaviour</td>
</tr>
<tr>
<td></td>
<td>RQ2</td>
<td>RO2</td>
<td>To generate the attack pattern of malware</td>
</tr>
<tr>
<td></td>
<td>RQ3</td>
<td>RO3</td>
<td>To formulate the procedure of extracting the attack pattern(script)</td>
</tr>
</tbody>
</table>

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 extracting 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>
<thead>
<tr>
<th>RP</th>
<th>RQ</th>
<th>RO</th>
<th>RC</th>
<th>Research Contribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>RP1</td>
<td>RQ1</td>
<td>RO1</td>
<td>RC1</td>
<td>The parameter use to analyse the malware behaviour</td>
</tr>
<tr>
<td></td>
<td>RQ2</td>
<td>RO2</td>
<td>RC2</td>
<td>The attack pattern of android malware</td>
</tr>
<tr>
<td></td>
<td>RQ3</td>
<td>RO3</td>
<td>RC3</td>
<td>The script to extract malware attack pattern</td>
</tr>
</tbody>
</table>

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](image)

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](image)

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

<table>
<thead>
<tr>
<th>Type</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Access Trojan</td>
<td>Designed to provide the attacker with complete control of the victim's system.</td>
</tr>
<tr>
<td>Proxy Trojan</td>
<td>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.</td>
</tr>
<tr>
<td>Denial of Service (DoS) Trojan</td>
<td>This type of trojan attack and bring down the network by flooding the entire network with unnecessary traffic.</td>
</tr>
<tr>
<td>Destructive Trojan</td>
<td>Designed to delete, erase the data on the victim’s computer</td>
</tr>
<tr>
<td>Data sending Trojan</td>
<td>Designed to collect and send sensitive data from the victim’s computer to its server.</td>
</tr>
<tr>
<td>FTP Trojan</td>
<td>Designed to open port 21 to allow the hacker to connect to the victim’s computer using FTP.</td>
</tr>
<tr>
<td>Security Disable Trojan</td>
<td>Kill or stop computer security software to operate which have in the victim’s computer likes firewall and antivirus software.</td>
</tr>
</tbody>
</table>