BORANG PENGESAHAN STATUS TESIS*

ANALYSIS OF ANDROID MALWARE (DROIDKUNGFU 2)

JUDUL: THROUGH THEIR BEHAVIOR USING STATIC ANALYSIS

SESII PENGAJIAN: 2010 / 2011

Saya ALIA 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.

Tarikh: Tarikh:

PROF MADYA Dr. MOHD FAIZAL BIN ABDOLLAH

Nama Penyelia

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 MADA YA 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 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 him 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

TABLE OF CONTENT

<table>
<thead>
<tr>
<th>CHAPTER</th>
<th>SUBJECT</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>DECLARATION</td>
<td>i</td>
<td></td>
</tr>
<tr>
<td>DEDICATION</td>
<td>ii</td>
<td></td>
</tr>
<tr>
<td>ACKNOWLEDGEMENT</td>
<td>iii</td>
<td></td>
</tr>
<tr>
<td>ABSTRACT</td>
<td>iv</td>
<td></td>
</tr>
<tr>
<td>ABSTRAK</td>
<td>v</td>
<td></td>
</tr>
<tr>
<td>TABLE OF CONTENT</td>
<td>vi</td>
<td></td>
</tr>
<tr>
<td>LIST OF FIGURES</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>LIST OF TABLES</td>
<td>xiii</td>
<td></td>
</tr>
</tbody>
</table>

1.0   CHAPTER I: INTRODUCTION

1.1   Introduction                      1
1.2   Research Problem                  2
1.3   Research question                 3
1.4   Research Objective                4
1.5   Scope                             5
1.6   Expected output                   5
1.7   Research contribution             5
1.8   Report Organization               6
1.9   Conclusion                        7

2.0   CHAPTER II: LITERATURE REVIEW

2.1   Introduction                      8
2.2   Related work                      9
      2.2.1 Android                     9
2.2.2 Malware 11
2.2.3 Trojan 13
2.2.4 Trojan classification 13
2.2.5 DroidKungFu 2 14
2.2.6 DroidKungFu 2 characteristic 15
2.3 Attack pattern analysis 16
2.3.1 Definition attack pattern 16
2.3.2 Importance of attack pattern 17
2.4 Malware analysis 17
2.4.1 Static analysis 17
2.4.2 Dynamic analysis 18
2.5 Conclusion 19

3.0 CHAPTER III: METHODOLOGY

3.1 Introduction 20
3.2 Categories analysis 21
3.2.1 Phase I: Literature review 21
3.2.2 Phase II: Requirement analysis 22
3.2.3 Phase III: Design and development 22
3.3 Categories system development 23
3.3.1 Phase IV: Implementation 23
3.3.2 Phase V: Testing and evaluation 23
3.4 Milestone 24
3.5 Gantt chart 25
3.6 Conclusion 25
4.0 CHAPTER IV: DESIGN AND IMPLEMENTATION

4.1 Introduction 26
4.2 Hardware and software requirement 27
  4.2.1 Hardware 27
  4.2.2 Software 28
  4.2.3 Tools 30
4.3 Design 32
  4.3.1 General Flow chart 33
  4.3.2 Flow chart for script 1 34
  4.3.3 Flow chart for script 2 35
4.4 Implementation 36
  4.4.1 Installation of software and tools 36
  4.4.2 Installation of malware(DroidKungFu2) 40
  4.4.3 Installation of malware in emulator 43
4.5 Conclusion 45

5.0 CHAPTER V: TESTING AND ANALYSIS

5.1 Introduction 46
5.2 Testing 46
  5.2.1 Design 46
  5.2.2 Sample 49
5.3 Analysis Result 59
  5.3.1 Script 59
  5.3.2 Comparison between normal and abnormal 61
  5.3.3 General malware attack pattern 62
5.4 Conclusion 65
6.0 CHAPTER VI: CONCLUSION

6.1 Introduction 66
6.2 Research Summarization 66
6.3 Limitations 67
6.4 Contributions 68
6.4.1 Behavior Profiling 68
6.5 Future Works 68
6.6 Conclusion 68

REFERENCES 69
APPENDIX A 71
APPENDIX B 79
## LIST OF FIGURES

<table>
<thead>
<tr>
<th>FIGURES</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 2.1</td>
<td>Literature review phase</td>
<td>9</td>
</tr>
<tr>
<td>Figure 2.2</td>
<td>Android Architecture</td>
<td>10</td>
</tr>
<tr>
<td>Figure 2.3</td>
<td>Malware distribution</td>
<td>11</td>
</tr>
<tr>
<td>Figure 3.1</td>
<td>Five phase of methodology</td>
<td>21</td>
</tr>
<tr>
<td>Figure 3.2</td>
<td>Milestone of research project</td>
<td>24</td>
</tr>
<tr>
<td>Figure 3.3</td>
<td>Gantt chart of research project</td>
<td>25</td>
</tr>
<tr>
<td>Figure 4.1</td>
<td>Components in ApkTool</td>
<td>30</td>
</tr>
<tr>
<td>Figure 4.2</td>
<td>Components in Dex2jar</td>
<td>31</td>
</tr>
<tr>
<td>Figure 4.3</td>
<td>Example of JD-GUI</td>
<td>32</td>
</tr>
<tr>
<td>Figure 4.4</td>
<td>Process of extracting the .apk file</td>
<td>33</td>
</tr>
<tr>
<td>Figure 4.5</td>
<td>Process of script on extracting the .apk file using netbean</td>
<td>34</td>
</tr>
<tr>
<td>Figure 4.6</td>
<td>Process of script in searching malware</td>
<td>35</td>
</tr>
<tr>
<td>Figure 4.7</td>
<td>VMware Workstation 8</td>
<td>36</td>
</tr>
<tr>
<td>Figure 4.8</td>
<td>Windows 7</td>
<td>37</td>
</tr>
<tr>
<td>Figure 4.9</td>
<td>SDK manager</td>
<td>37</td>
</tr>
<tr>
<td>Figure 4.10</td>
<td>ApkTool .zip file</td>
<td>38</td>
</tr>
<tr>
<td>Figure 4.11</td>
<td>Command prompt to install apktool</td>
<td>38</td>
</tr>
<tr>
<td>Figure 4.12</td>
<td>Dex2jar .zip file</td>
<td>39</td>
</tr>
<tr>
<td>Figure 4.13</td>
<td>Command prompt to install dex2jar</td>
<td>39</td>
</tr>
<tr>
<td>Figure 4.14</td>
<td>JD-GUI</td>
<td>40</td>
</tr>
<tr>
<td>Figure 4.15</td>
<td>Decode malware using apktool</td>
<td>40</td>
</tr>
<tr>
<td>Figure 4.16</td>
<td>Folder malware after decode process</td>
<td>41</td>
</tr>
</tbody>
</table>
Figure 4.17  File for ‘test 1’ malware  42
Figure 4.18  Convert to .jar file using dex2jar  42
Figure 4.19  ‘test 1.jar’ file appeared at desktop  42
Figure 4.20  Open ‘test 1.jar’ file using JD-GUI  43
Figure 4.21  SDK platform-tools  43
Figure 4.22  Interface to launch the emulator  44
Figure 4.23  Menu screen for emulator  44
Figure 4.24  Adb install using command prompt  45
Figure 4.25  Malware appeared in menu screen  45
Figure 5.1  Process of script on extracting the .apk file using netbean  47
Figure 5.2  Process of script in searching malware parameter  48
Figure 5.3  Mobile Sandbox overview  50
Figure 5.4  “com.eguan.state” in jd-Gui  50
Figure 5.5  URLs found in code  51
Figure 5.6  Code for Root exception  51
Figure 5.7  Code malicious get the data  52
Figure 5.8  Update information function  52
Figure 5.9  Mobile Sanbox overview  53
Figure 5.10  “com.eguan.state” in jd-Gui  53
Figure 5.11  URLs found in code  54
Figure 5.12  Code for Root exception  54
Figure 5.13  Code malicious get the data  55
Figure 5.14  Update information function  55
Figure 5.15  Mobile Sanbox overview  56
Figure 5.16  “com.eguan.state” in jd-Gui  56
<p>| Figure 5.17 | URLs found in code | 57 |
| Figure 5.18 | Code for Root exception | 57 |
| Figure 5.19 | Code malicious get the data | 58 |
| Figure 5.20 | Update information function | 58 |
| Figure 5.21 | First script output | 59 |
| Figure 5.22 | Second script output | 60 |
| Figure 5.23 | Abnormal apk folder | 61 |
| Figure 5.24 | Components assest folder in jd-gui | 61 |
| Figure 5.25 | Normal .apk folder | 61 |
| Figure 5.26 | Code normal .apk | 62 |
| Figure 5.27 | Overview from Virus Total system | 62 |
| Figure 5.28 | DNS network traffic | 63 |
| Figure 5.29 | Http network traffic | 64 |
| Figure 5.30 | Root-kit exploit in emulator | 64 |</p>
<table>
<thead>
<tr>
<th>TABLE</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 1.1</td>
<td>Research problem</td>
<td>2</td>
</tr>
<tr>
<td>Table 1.2</td>
<td>Research question</td>
<td>3</td>
</tr>
<tr>
<td>Table 1.3</td>
<td>Research objective</td>
<td>4</td>
</tr>
<tr>
<td>Table 2.1</td>
<td>Definition of Malware</td>
<td>12</td>
</tr>
<tr>
<td>Table 2.2</td>
<td>Classificition of Trojan</td>
<td>14</td>
</tr>
<tr>
<td>Table 4.1</td>
<td>Hardware requirement for PC</td>
<td>27</td>
</tr>
<tr>
<td>Table 4.2</td>
<td>Hardware requirement for Laptop</td>
<td>28</td>
</tr>
<tr>
<td>Table 5.1</td>
<td>Sample .apk file used</td>
<td>49</td>
</tr>
<tr>
<td>Table 5.2</td>
<td>Parameters uses in script</td>
<td>60</td>
</tr>
</tbody>
</table>
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>
<thead>
<tr>
<th>No</th>
<th>Research Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Less understanding about the behaviour of malware and how the malware will affect the parameter</td>
</tr>
</tbody>
</table>
1.3 Research Question

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

Table 1.2: 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 behaviour of android malware?</td>
</tr>
<tr>
<td></td>
<td>RQ2</td>
<td>How to differentiate behavior of android during infection and normal condition?</td>
</tr>
<tr>
<td></td>
<td>RQ3</td>
<td>What is the formulated procedure of extracting the attack pattern</td>
</tr>
</tbody>
</table>

**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>
<thead>
<tr>
<th>RP</th>
<th>RQ</th>
<th>RO</th>
<th>Research Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>RP1</td>
<td>RQ1</td>
<td>RO1</td>
<td>To identify the behavior of android malware</td>
</tr>
<tr>
<td></td>
<td>RQ2</td>
<td>RO2</td>
<td>To differentiate behavior of android during infection and normal condition</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>

**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 during 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 or software to protect the system from DroidKongfu2 malware and to minimize the risk of the malware to the system.

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.
In the literature review phase, more information on malware, attack pattern and malware analysis issues will be 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 advanced 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.