Faculty of Information and Communication Technology

INVESTIGATING GOLDDREAM BEHAVIOR THROUGH DYNAMIC ANALYSIS

Halizah binti Saad

Master of Computer Science (Security Science)

2013

INVESTIGATING GOLDDREAM BEHAVIOR THROUGH DYNAMIC ANALYSIS

HALIZAH BINTI SAAD

A thesis submitted

in fulfillment of the requirements for the degree of Master of Computer Science (Security Science)

Faculty of Information and Communication Technology

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2013

DECLARATION

I declare that this thesis entitle Investigating GoldDream Behavior through Dynamic Analysis is the result of my own research except as cited in the references. The thesis has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature : …….

Name : …….

Prof Madya Dr Mohd Faizal Bin Abdollah

Date : …….

TABLE OF CONTENT

ABSTRACT

Smartphones have become more popular today and along with it Android Operating system also increasing rapidly. The Android OS is very popular because of their design where it is an open source design. So, it attracts people to use it because it is more convenient and easy. However, the openness of Android design also become it flaw because it not only attract Android user but also attacker for Android platform. Their openness design and it is easy to get their application have give advantages to attacker repackaged Android application and can upload the repackage application easily on Android market or any third party market. This brings to the increasing of android malware in the market. So, because of that reason it leads to the execution of this project where this project helps to understand how is the malware behavior and how its work especially about GoldDream malware. The method used to identify the malware behavior is by conducting a dynamic analysis technique. The behavior is being extract from the network traffic log and based on system call function. As conclusion, the behavior of GoldDream that can be identify from this research are the malware will create a database in user device which this database will log all the incoming and outgoing phone call plus with spying the incoming sms. Another behavior is it will upload the victim SIM, IMEI and IMSI information to their C&C server by embedded the information in HTTP URL.

ABSTRAK

Telefon pintar telah menjadi lebih popular hari ini dan bersama-sama dengan itu sistem operasi Android juga meningkat dengan cepat. Android OS adalah sangat popular kerana reka bentuk mereka iaitu menjadikan ia sebagai satu reka bentuk sumber terbuka. Jadi, ini menarik orang ramai untuk menggunakannya kerana ia adalah lebih mudah dan murah. Walau bagaimanapun, keterbukaan reka bentuk Android juga menjadi satu kecacatan kepadanya kerana ia bukan sahaja menarik pengguna Android tetapi juga penyerang untuk platform Android. Reka bentuk terbuka mereka dimana mudah untuk mendapatkan aplikasi mereka telah memberi kelebihan kepada penyerang mempakej semula aplikasi Android dan boleh memuat naik aplikasi yang dipakejkan semula dengan mudah pada pasaran Android atau mana-mana pasaran pihak ketiga. Ini membawa kepada peningkatan android malware di pasaran. Jadi, oleh kerana itu ia membawa kepada pelaksanaan projek ini di mana projek ini membantu untuk memahami bagaimana kelakuan malware dan bagaimana ia berfungsi terutama berkaitan GoldDream malware. Kaedah yang digunakan untuk mengenal pasti tingkah laku malware adalah dengan menjalankan teknik analisis dinamik. Tingkah laku dikenal pasti daripada log rangkaian lalu lintas dan berdasarkan fungsi panggilan system yang dikumpulkan semasa menjalankan ujikaji. Kesimpulannya, tingkah laku GoldDream yang boleh dikenal pasti dari kajian ini adalah GoldDream akan mewujudkan pangkalan data dalam peranti pengguna di mana pangkalan data ini akan log semua panggilan masuk ke telefon dan panggilan keluar ditambah juga dengan mengintip sms yang masuk ke peranti pengguna. Tingkah laku yang lain adalah ia akan memuat naik maklumat mangsa iaitu nombor SIM, IMEI dan IMSI kepada pelayan C & C mereka dengan menyelitkan maklumat tersebut dalam URL HTTP.

ACKNOWLEDGEMENT

First and foremost, praises and thanks to the Almighty God, for His showers of blessings throughout my research work to complete the research successfully.

I would like to express my deep and sincere gratitude to my research supervisor, Profesor Madya Dr Mohd Faizal Bin Abdollah for his encouragement, guidance and patience he demonstrated throughout this research.

Sincere thanks to Dr. Robiah and Dr. Zul Azri for their comment and patience while evaluating this research. I would also like to thank my friend Najiahtul Syafiqah for her motivation and support to complete my research.

Last but not least, I am extremely grateful to my parents for their understanding, prayers and continuing support to complete my study.

CHAPTER I

INTRODUCTION

1.1 Background

These days, there is an explosive growth in Smartphone sales and adoption. The Smartphone is mobile phone which includes functions similar to those found on personal computers but they are compact in size, run complete operating system (OS) software and usually have larger displays and more powerful processors than standard mobile telephones. Besides that, it provides a one-stop solution for information management, mobile calls, email sending, and Internet access. There are many types of Smartphone OS available such as Google's Android, Apple's iOS, Nokia's Symbian, RIM's BlackBerry OS, Samsung's Bada, Microsoft's Windows Phone, Hewlett-Packard's webOS, and embedded Linux distributions such as Maemo and MeeGo.

Unfortunately, the increasing adoption of Smartphone comes with the growing prevalence of mobile malware. Based on PC Advisor (2013), according to a recent report from the security firm Kaspersky, 99 percent of all new malware attacked the Android platform on 2012. That was a continuation of the trend from 2011, which registered an explosive growth in Android malware. During 2011, averages of 800 new types of malicious programs were discovered every month, and this figure rose in 2012 to a whopping 6,300 programs. PC

Advisor (2013) also state a said by a security expert Kevin Freij from MYMobileSecurity which is, "Android is the world's most widely used Smartphone operating system, so it is not surprising that it is also the hacker's favorite goal. But it has probably surprised many people, including myself, that it's as much as 99 percent".

As for this research, the focused of the research is on the Android malware. Malware is a generic term used to describe all kinds of malicious software (e.g., viruses, worms, or Trojan horses). Malicious software not only poses a major threat to the security and privacy of computer users and their data, but is also responsible for a significant amount of financial loss. (Moser, Kruegel, & Kirda, 2007)

1.2 Problem Statement(s)

As Android OS are becoming more popular, they become the targets for potential attacks. Therefore, the research problem for this project is the increasing growth of Android malware where it’s embedded in user devices with intention to harm or damage the system without user’s consent and thus, it is crucial to analyze the malware behavior so that the outcome can be used to plan and implement prevention method for minimizing future malware threat.

1.3 Objective

The objectives for this project are:

- To study about malware behavior and how it works on android
- To identify the parameter for malware analysis using dynamic analysis and to investigate the GoldDream behavior.
- To profile the behavior of GoldDream malware.

1.4 Scope

This research will be focused at the GoldDream malware and android platform to study the behavior of the malware. Plus, the hardware and software that will be involved during the research would be:

a. Hardware
    - PC – The personal computer will be used to install software to create a safe environment for conducting the experiment.

b. Software
    - VM ware – It is a virtual appliance which allows user to run multiple operating systems. It also can be freely downloaded at *https://www.virtualbox.org/wiki/Downloads*
    - Emulator: Android SDK – It's a virtual mobile device that runs on the computer. It can be used to develop and test Android applications without

using a physical device. The Android SDK can be downloaded from *http://developer.android.com/sdk/index.html*.

- Log analyzer: Wireshark – Wireshark is the leading network protocol analyzer. It is used to capture and interactively browse the traffic running on a computer network. The software can be downloaded from *http://www.wireshark.org/download.html.*

1.5 Project Significance

By successfully finishing the research, the significant of this research can be classified as below:

- The understanding about malware android behavior and the effect of malware android.

- Result of profiling the GoldDream Malware behavior.

- Based on both of the benefits discussed, it gives beneficial to understand about the malware characteristic and behavior, and to differentiate normal and abnormal condition as more proficient action can be carry out to solve the problem.

So, from the study that will be conducted hopefully this research is able to brought a sufficient benefits to all Android users. As a result, Android users can be aware of malware attacks.

1.6 Expected Output

The expected output from this project is to achieve all the objectives that have been listed. The benefits that can be gained from objectives achievement are the understanding about android, what is malware, how to analyze it, the behavior and characteristic of the malware, and lastly is the behavior of normal and abnormal condition on android.

1.7 Summary

This chapter basically stated about the research objectives in order to solve the problem faced. The objectives will give an idea how to analyze GoldDream malware, the technique that been choose and related components that necessary to complete the project.

Besides, it gives the indication about the output that will be gained at the end of the project. Last but not least, the scope of the research also been stated as a guideline to ensure that the project in the right path for its completion.

CHAPTER II

LITERATURE REVIEW

2.1 Introduction

In this chapter, related literature reviews will be conducted to get better overview of the project that been conducted. It is important to well understand all information that need to be considered before developing the project. The literature review can be completed by collecting related information from various kinds of resources such as websites, books, journals and other related materials. As a result, the information gathered will be useful for understanding the malware and used as a foundation to provide a suitable test bed to observe their behaviour.

2.2 Android

2.2.1 Definition

Android is a Linux-based open source operating system which design for mobile devices like Smartphone and tablet computers. It is initially developed by Android Inc which founded in 2003 and then it was bought by Google Inc in 2005 (Vangie Beal, 2013). After the acquisition, Android was unveiled in 2007 along with the founding of the Open Handset Alliance. Iland, Pucher and Timm Schauble (2011) stated, Android is becoming the prevalent

platform for Smartphone today, with over 190 million activated devices in use in 130 countries and the software can be downloaded from official Android market, third party app stores, or by direct download and install of an APK file.

On the other hand, the most attractive feature of Android is that it provides an open platform for developers to create their own applications. It also provides an SDK and NDK for the developer to create various applications unlike the Apple iPhone applications that need to be downloaded from the Apple Appstore.

2.2.2 Architecture

According to Lin et.al (2013), android is basically a stack of software which can be divided into four major layers which are Linux kernel, running environment layer, application framework layer and application layer. Figure 2.2 shows the Android architecture.

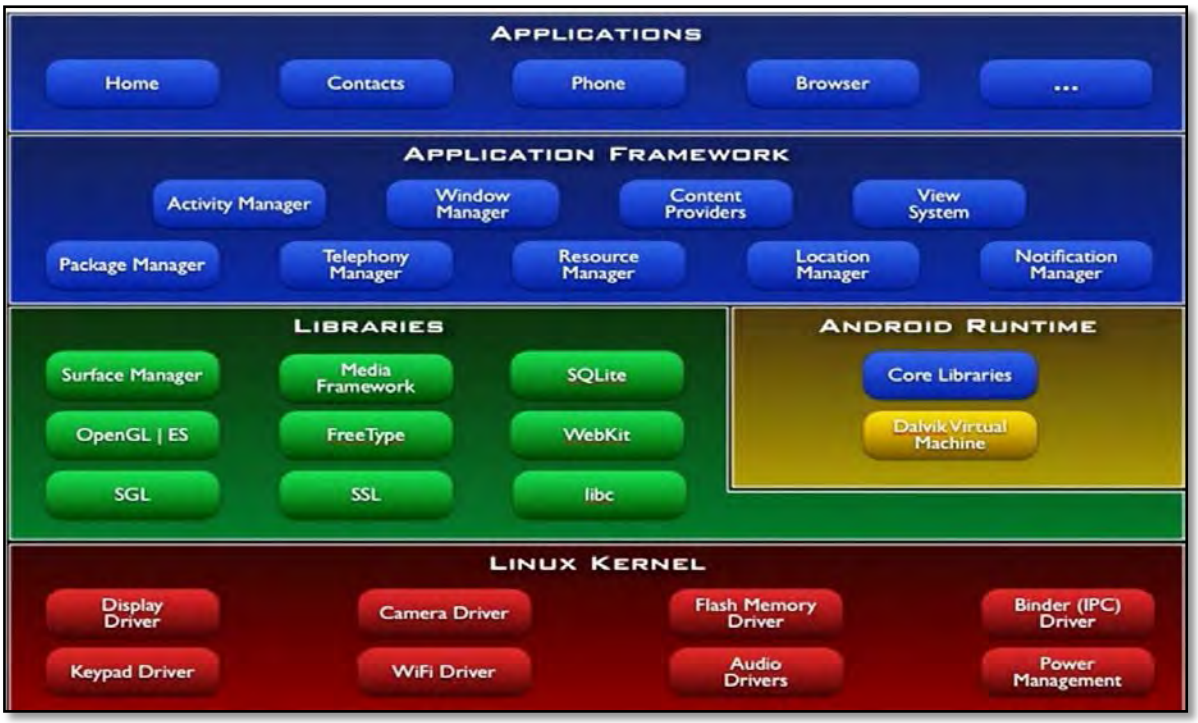

Figure 2.1 Architecture of Android Operating System (Min & Cao,)

Based on Figure 2.2, the layers are written in three different language which is green components is written in native code (C/C++), while blue items are Java components that interpreted and executed by the Dalvik Virtual Machine. Lastly, the red layer represents the Linux kernel components and runs in kernel space.

2.3 Definition Android Malware

Smartphones have become very popular today because it is very convenient with today lifestyle where it offer many services like social engineering, GPS system, web browser and it also offer Office application like word editor and power point application. However, with the increasing of smartphone adoption this also makes the malware developer become interested to infect them with malware. Securelist (2012) has proved it by the statistic shown in their website and the static is shown in Figure 2.2 below:

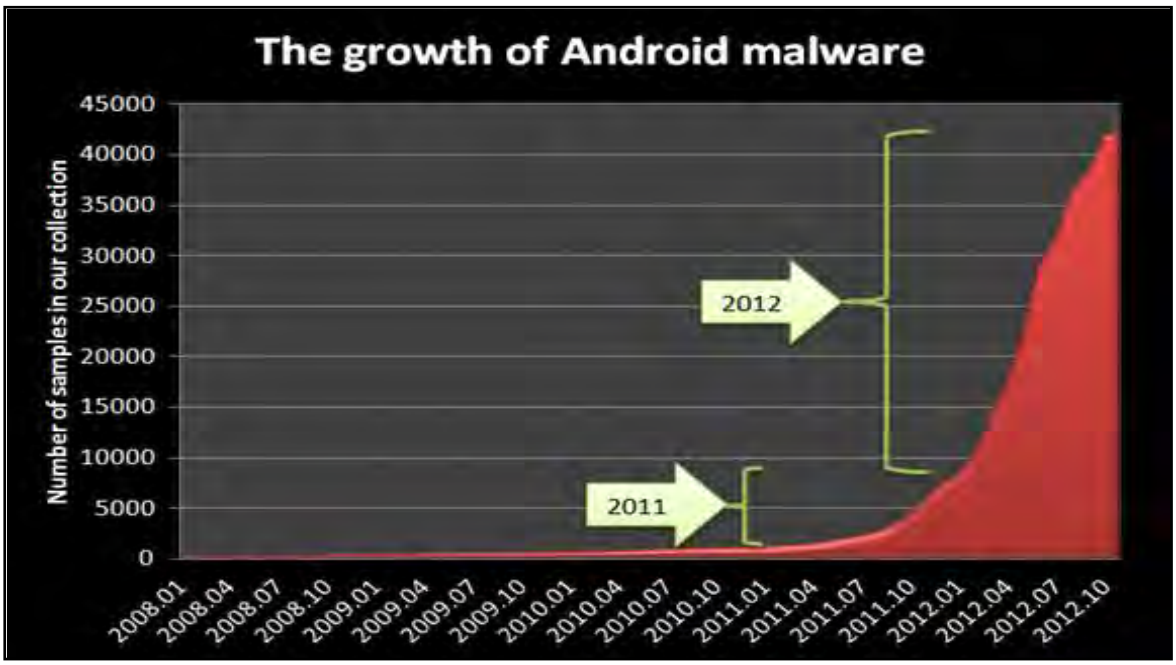

Figure 2.2 The growth of Android Malware (Securelist)

There are various definition of malware have been offered from previous researcher. Table 2.1 show the summarization of malware definition defines from previous researcher.

Table 2.1 Malware definition summary

Researcher	Paper Title	Definition
McGraw & Morrisett (2000)	Attacking malicious code - A report in the Infosec Research Council (2000)	Malicious code is any changed, coded, or removed from a software system to purposely cause harm or threaten the intended function of the system.
Christodorescu *et.al* (2005)	Semantics-Aware Malware Detection (2005)	This paper defines malware as a program that has malevolent intent.
Vasudevan and Yerraballi (2006)	SPiKE : Engineering Malware Analysis Tools using Unobtrusive (2006)	Researcher defines malware as a generic term that encompasses viruses, Trojans, spywares and other intrusive code.
Rutkowska (2006)	Introducing Stealth Malware Taxonomy (2006)	Rutkowska define malware as a part of code which change the behavior of either the operating system kernel or security sensitive applications, without user permission and it is difficult to detect the changes using documented features of the operating system or application (e.g.API).
Dai *et. al* (2010)	Behavior-Based Malware Detection on Mobile Phone	Researcher identifies it as a class of new forms malware seeking at mobile devices.

	(2011)	
Zolkipli and Jantan (2011)	An Approach for Malware Behavior Identification and Classification (2011)	Malware is a malicious program designed to harm the computer on which it execute or the network over which it communicate.
Chandramohan (2012)	Detection of Mobile Malware in the Wild (2012)	Malware is identified as software that exhibits malicious behavior which is categorized to include viruses, botnets, worms, and Trojan horses.

Based on Table 2.1, it shows that malware is referred to several of names such as malicious software or malevolent software, and malicious code. Plus, from the summary of earlier research, plenty information which describe about malware can be gained. As conclusion, malware generally is a bad program. However, Android malware can be defined as a program that been embedded in Android platform application with intent to breach user privacy and confidentiality by impose as legitimate application.

2.3.1 Android Malware Characteristics

As been discussed earlier, basically malware can be defined as a bad program that has personal agenda to steal information from affected user. The malware can be categorized in several type based on their activities and Manjunath (2004) in his report has classified it as below:

i. **Virus:** A virus is defined as a harmful or malicious program that lacks the ability to self-reproduce
ii. **Worm:** This is a malevolent code that can control system vulnerability or a network in order to automatically duplicate to another system.
iii. **Trojan:** A Trojan allows an invader to obtain illegal access or remote access to a system while it acts to be executing a required operation.
iv. **Spyware:** This destructive application disguises itself from the user while it collects information about the user without the user's consent.

Meanwhile, Pieterse and Olivier (2012) determine that the characteristic of malware are as below:

i. **Repackaged Application:** The allocation of malicious code to instigate a botnet usually takes the form of well-known and legitimate application. A user is unaware of the additional configurations taking place on the device. It is similar to Trojan horse and is the most common method to distribute botnet code.
ii. **Receiving Commands:** The capability to either receive command automatically or to prompt a remote server for the commands and it is the current techniques used by Android botnets. There are several options which are to send the

commands directly from a C & C server to the Android bot as needed, and to allow the Android bot to contact the C & C server at normal intervals and enquire whether new commands are available. If there is any contact with a remote server it is indication that obviously Android botnet is at work.

iii. **Messaging:** Current Android botnets are exploiting SMS messages to gather money by sending messages to premium-rate numbers. These premium-rate numbers are phone numbers, used for a certain service and are charged at a higher rate than normal phone calls. By sending SMS messages at regular.

iv. **Steal Information:** Android botnets do not only obtain information from a C & C server but also upload information about the infected device to the server. This type of activity occurs usually after the installation of the malicious application.

v. **Third Party Application Markets:** Before this, malevolent applications only appeared on unofficial third party application markets but lately it appears on the Official Android Market such as DroidDream malware.

vi. **Additional Content Downloaded:** Android botnets has the ability to download additional content which generally malicious in nature, supports and improves the performance of the botnet. The additional content is either downloaded dynamically by the application or a prompt asks the user to perform the required download.

Besides that, Chandramohan (2012) also have classified the malware based on their behaviour. The classification is shown in Table 2.2

Table 2.2 Behavioral classification overview for mobile malware in the wild (Chandramohan, 2012)

Malware Behaviour	Description	Example
Offers novelty and amusement	Initially developed for fun or to show off the author's technical expertise, less serious, generates useless destruction	Android.Walkinwat
Sells user information	Confidentially collect user details, like contact list, download history, installed applications, and location, and all these details are then sold to advertisers and marketers.	DroidDreamLight
Manipulates content delivery	Generates premium-rate phone calls and sends text messages, possibly to deliver content such as technical support, adult services, or stock quotes.	FakePlayer
Sends SMS spam	Spams multiple messages to mobile phones that usually contain advertisements and phishing links.	Geinimi
Manipulates search engine optimization	Improves website rankings in search engine results.	Hong Tou Tou
Steals user credentials	Captures user credentials like bank account details by secretly snooping on text message, capturing key-strokes by key logging,	Ikee.B