ICIBA 2014, the Third International Conference on
Information Technology and Business Applications
Palembang-Indonesia, 20-21 February 2014

Malware Analysis on Android System With Forensic Computer Techniques

Rahmat, Prihambodo Hendro Saksono, Yesi Novaria Kunang

Master of Information Technology
Bina Darma University
e-mail:rahmat.novrianda.d@gmail.com

Abstract

The purpose of this study to determine the stages for android malware analysis, malware detection android, knowing how to determine the impact of the entry of malware as well as malware android to the android system. There are 3 sample android application android malware infected material to be used in this study, namely: iCalendar, Live wallpapers live prints and SMS Hippo. The analysis carried out by making use of several computer forensics tools, such as: WinRAR, Dex2jar and JD-GUI. The first stage is to analyze malware android rename APK extension of android apps into ZIP extension, then extract with WinRAR generate DEX file format. Using tools Dex2jar, DEX files converted into a JAR file. Final step, decompile JAR file using JD-GUI and analyzed java source code from android application. The results of analysis shows android malware make device to send SMS to premium number and android malware can steal information private information.

Keywords : *Malware, Android, Computer Forensics, java source code*

1 INTRODUCTION

The development of technology also trigger the development of new malware, so the more injured party due to the presence of this malware. The advantages of android operating system is open access, which provided an open platform for developers (user) that is intended to allow users to create and develop their own applications that can be used on a variety of mobile devices. However, this has raised the ease in which the parties are not responsible for the build and develop malware applications that can be entered into the android system. Researchers took three samples that contain malware android application android, android application which iCalendar (Android.raden.A), Live live wallpaper prints (Hongtoutou) and Hippo (Hippo SMS).

1.1 Malware

Malware is a software that can infiltrate into the operating system so that it can damage the system and can also steal important files on the system. Also called malware or

destructive software include Computer Viruses, Trojan Horse, the surveillance (spyware), the ads (adware) dishonest, malicious software (crimeware) software and other malicious and unwanted.

1.2 Android System

Android system is a Linux-based operating system for mobile phones such as smartphones and tablet PCs. Android system has advantages, such as the operating system is open source, multitasking, ease of notification to the number of applications or software that can dinikimati using android system.

1.3 Forensic Computer

Forensic computer is simply the application of computer investigation and analysis techniques in the interests of determining potential legal evidence. Evidence might be sought in a wide range of computer crime or misuse, but not limited to theft of trade secrets, theft or destruction of intellectual property, and fraud. CHFI can draw a variety of methods to find data residing within a computer system, or recovering that have been removed, encrypted or damaged file information. Forensic Computer in recent years began to bloom in Indonesia, the experts are still limited. This science should really be accounted for. Forensic Computer expert in Indonesia is still very rare because it may not be too many IT people who pursue this field. The second, perhaps still a lot of people are afraid that IT is associated with the law.

1.4 Tools Required

In a research and analysis would certainly require some supporting tools that can do a problem analysis. In the present study related to the analysis of malware on android system, while the tools it needs is some software on the computer forensics. As for some of the software are as follows:

- WinRAR
- Dex2jar
- JD-GUI

2 RESEARCH METHODOLOGY

In one study, there are several things that must be considered in order to run properly research, ie research methods and methods of analysis.

2.1 Research Methods

Each study requires a research method that reached a final conclusion. Here is the method in this study:

1. Preparation tools and tool-support tools.
2. Hardware and software testing. Hardware and software that will be used should go well.

3. Searching and collecting some android malware samples that will be used as research material.

4. Android malware analysis with computer forensic techniques that can be detected and analyzed the workings and influence of malware on the android system.

5. Preparation of the data collected in a single unit and then the final conclusions drawn.

2.2 Methods of Analysis

Of Figure 1 . The first thing to do is select or search for android application which will be studied , in this case android applications downloaded from the mobile contangio forum . Detect malware on android app using the total virus service . Android apps android analyzed contained malware detected by means of static analysis . Android apps infected with malware android extension - rename APK in ZIP extension , which is then extracted by using WinRAR . This is done because the APK files can be illustrated as an archive (ZIP file) containing Dalvix Executable files (extension DEX) . The results of the extraction contains several files , which are files berektensi DEX . Then , DEX files be converted into a JAR format using Dex2jar and will generate a JAR file extension .

The final step , decompile JAR file using JD - GUI that can be seen all java source code to be studied and analyzed to achieve the purpose of this study.

3 RESULTS AND DISCUSSION

The results of this study were obtained from 3 samples examined were infected with malware android application android, namely: iCalendar, Live live wallpaper prints and Hippo (kuis.com).

3.1 iCalendar

In iCalendar application that serves as an electronic calendar on android device with some additional features are also inserted a suspected malware can send an SMS to a premium number so that the pulse of android devices infected is reduced without being noticed by the user.

From the analysis of the total virus detected using a service that there is malware on iCalendar.apk applications and also contained some irregularities in the required permissions.

In the application there iCalendar Android malware Raden A, which resulted in the presence of this malware activity to and from the premium SMS number.

Class files SmsReceiver.class look at when decompile with JD-GUI. In the class file, there are a premium destination number is ”1066185829” SMS ”921X1”. In addition, there is also broadcast an abort command, which is intended as a rejection of the premium sms notification activity. This causes the user is not aware of any SMS activity.

3.2 Live prints live wallpaper

Live prints live wallpaper is a live wallpaper app for android devices with a live display prints. This prints a live model’s great for the live wallpaper on the android device, but it also contains malware application android called Hongtoutou.

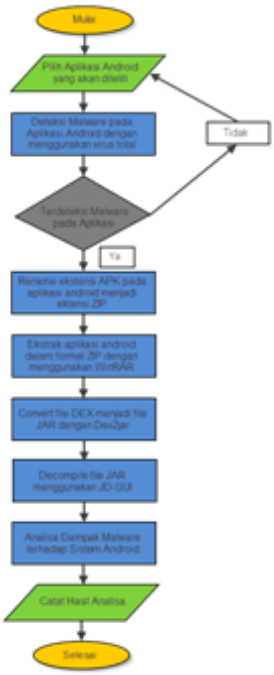

Figure 1: Android Malware Analysis Method Flowchart

In this application there Hongtoutou android malware, malware which is able to read and steal IMEI and IMSI dijangkitinya android devices.

Java source code on android application, the researchers found a command "TelephonyManager" which is meant to be read IMEI and IMSI android devices. Then in class the other file contained a "get" the IMEI and IMSI and sent to the address of the site "http://adrd.taxuan.net/index.aspx".

3.3 Hippo (kuis.com)

In the Hippo application android application which is connected with kuis.com site. This application is a quiz which normally provide services also include chat media, search engines and others. However, this android application android suspected of containing malware called ANDROIDOS_HIPPOSMS.A and more popularly known as SMS Hippo.

In this application there is a malware known as Hippo android SMS. There is a class file java source code MessageService.class on this android application. In the class file, there are the "sendsms" to the premium number "1066156686" with the text "8". This causes premium SMS subscription android devices from a variety of premium Chinese number. In class the other files, there is a command to delete the original text from numbers starting with "10" using the text "ddddddddddddddddssssssssssssssss ssddddddddd".

4 CONCLUSION

From the research results obtained, the researcher took some conclusions as follows:

1. In this study, the android malware analysis techniques require multiple computer forensic tools, namely: WinRAR, Dex2jar and JD-GUI.

2. ICalendar android apps containing malware (Trojans) that can send SMS to a premium number "1066185829", so the user unwittingly receive sms premium of the premium number.

3. Applications prints live wallpaper live android hongtoutou containing malware (Trojans and spyware) that can steal information about IMEI and IMSI from android device.

4. Malware android SMS Hippo Hippo contained in the application making android device to send sms to any number of premium Chinese ("1066156686") and resulted in the android devices from a variety of premium SMS subscription premium Chinese number without the user in mind.

References

Afrianto, D.S., (2007), *Jurnal Antisipasi Cybercrime Menggunakan Teknik Komputer Forensik.* Universitas Islam Indonesia : Informatika Teknologi Industri.

Burguera.I, Nadijm, Tehrani.U.Z., (2011), *Crowdroid: Behavior- Based Malware Detection System for Android.* In: SPSM11. ACM.

Eko.P.U., (2009), *Panduan Mudah Mengenal Bahasa Java.* Bandung : Yrama Widya.

Garfinkel, S.L., (2010), *Digital forensics research: The next 10 years. Digital Forensics Research Conferences (DFRWS).*

Gursimran, K., Bharti, N., (2012), *Malware Analysis & its Application to Digital Forensic. Ambedkar Institute of Advanced Communication Technologies & Research* : Department of Computer Science & Engineering.

Kriti, S., William, S., (2013), Malware Analysis for Android Operating. *8th Annual Symposium on Information Assurance (ASIA 13).*

Kruse, W.G., Heiser, J.G., (2001), *Computer Forensics.* Addison-Wesley : Incident Response Essentials.

La, P.M., Martinelli, F., Sgandurra, D., (2012), *A survey on security for mobile devices.* IEEE PP(99) : Communications Surveys Tutorials.

Rangsang, P., (2002), *Tuntunan Pemrograman Java.* Jakarta : Prestasi Pustaka Publisher.

Rijalul, F., Ipam, F.A., (2005), *Pemrograman Java.* Yogyakarta : Andi Offset.

Singgih, S., (2003), *Jurnal Forensik Komputer Sebuah Penanganan Kejahatan Komputer.*

Vibha, M., (2011), *Reverse Engineering of Malware on Android. University of Essex: The SANS Institute*

Yudi, P., (2011), *Makalah Pengantar Digital / Komputer Forensik. Universitas Islam Indonesia : Informatika Teknologi Industri.*

Zarni, A., Win, Z., (2013), Permission-Based Android Malware Detection. *International Journal of Scientific & Technology Research.*