Jurnal E-Komtek
Vol. 8 No. 1 (2024) pp. 137-143
https://jurnal.politeknik-kebumen.ac.id/index.php/E-KOMTEK
p-ISSN : 2580-3719 e-ISSN : 2622-3066

Android Phishing Analysis with the Reverse Engineering Method Using MT Manager

Ika Mei Lina[1], Gilang Ryan Fernandes
[1-2]Department of Informatics Engineering, Universitas Indraprasta PGRI, Indonesia, 12530

ikameilina.24@gmail.com

https://doi.org/10.37339/e-komtek.v8i1.1677

Published by Politeknik Piksi Ganesha Indonesia

Artikel Info
Submitted:
26-02-2024
Revised:
04-06-2024
Accepted:
11-06-2024
Online first :
26-06-2024

Abstract

People spend a lot of time with gadgets every day, and it cannot be denied that gadgets can facilitate people's activities in various fields. However, even though gadgets are very helpful, there are digital crimes that we must be aware of. One case that has received a lot of attention is the method of providing online invitations and package delivery receipts in the form of malware spread via the WhatsApp chat application. This has caused many losses, such as losing money in banking and also confidential data being accessed by criminals. The aim of this research is so that the public can anticipate this crime. Researchers use the Reverse Engineering method to find out the process, patterns, design, and how a program works in detail. The results obtained from this research are that there are many hacker attacks in the form of malware applications. This malware application will run when the victim downloads, installs, and grants access permission to the application. So people should always be alert and careful when using gadgets in everyday life.

Keywords: Malware; Analysis; Hacking; Android; Reverse Engineering

Abstrak

Masyarakat menghabiskan banyak waktu dengan gadget setiap harinya, dan tidak dapat dipungkiri bahwa gadget dapat memudahkan aktivitas masyarakat di berbagai bidang. Namun, meskipun gadget sangat membantu, ada kejahatan digital yang harus kita waspadai. Salah satu kasus yang banyak mendapat sorotan adalah modus pemberian undangan online dan resi pengiriman paket berupa malware yang disebarkan melalui aplikasi chatting WhatsApp. Hal ini menyebabkan banyak kerugian, seperti kehilangan uang di perbankan dan juga data-data rahasia yang diakses oleh penjahat. Tujuan dari penelitian ini adalah agar masyarakat dapat mengantisipasi kejahatan ini. Peneliti menggunakan metode Reverse Engineering untuk mengetahui proses, pola, desain, dan cara kerja suatu program secara detail. Hasil yang didapatkan dari penelitian ini adalah banyaknya serangan hacker yang berupa aplikasi malware. Aplikasi malware ini akan berjalan ketika korban mengunduh, menginstal, dan memberikan izin akses terhadap aplikasi tersebut. Sehingga masyarakat harus selalu waspada dan berhati-hati ketika menggunakan gadget dalam kehidupan sehari-hari.

Kata-kata kunci: Malware, Analisis, Peretasan, Android, Teknik Membalik

1. Introduction

Currently, people feel comfortable with increasingly developing technology, this can all be seen from people's activities which cannot be separated from gadgets, starting from work, entertainment, and family matters. People spend a lot of time with gadgets daily, and it cannot be denied that gadgets can help in various fields. Gadgets have various forms, such as laptops, computers, and smartphones **[1]**. Even though gadgets are very helpful, behind it all there is digital crime that we should be aware of. The public must also understand every type of crime in the digital world. Crime in the digital world is growing along with the rapid development of technology **[2]**. Many people only use gadgets without realizing that evil lurks in our every carelessness. The number of crime cases, such as providing online invitations and package delivery receipts in the form of applications spread across chat applications such as WhatsApp has resulted in many victims, such as losing money in banking and having confidential data on smartphones taken by hackers. Hackers are individuals or groups who misuse IT skills to commit crimes in cyberspace **[3]**. This attack technique is called phishing, and the perpetrator will act as a relative to be trusted and install malware that is packaged in such a way that it becomes an online invitation or package delivery receipt. In this study, researchers will dissect online invitation malware to see what coding is dangerous and to find out the flow of how this malware works. The aim of this research is so that the public can avoid and better anticipate this crime. Researchers used the MT manager application to view and dissect the malware application.

2. Method

The author used the Reverse Engineering method to analyze Android APK malware in this research. This method will dismantle the malware application with the help of the MT Manager tool. By using this method, we can see how dangerous the malwar is.

2.1 Reverse Engineering

Reverse Engineering is a technique used to understand a program's process, pattern, design, and workings in detail. In the scope of cyber security, testing is carried out to find a security gap or vulnerability in a program, and not infrequently, this technique is also used to replicate a program. This technique is commonly used in security penetration to look for

loopholes in a program. Reverse Engineering allows software to convert binary files that are initially only readable by machines into files that programmers can read **[4]**.

2.2 Phishing

Phishing is a method used for cybercrimes by pretending to be another person, company or relative to deceive the target via e-mail, website, and short message/chat. Phishing is aimed at online banking users, because the user enters a username and password, and does not rule out the possibility that this phishing is aimed at other online users **[5]**. Phishing is an activity that threatens or traps someone with the concept of fishing or deceiving so that the target indirectly provides the information the perpetrator needs **[6]**.

2.3 Malware

Malware is categorized as a virus, where this malware is a collection of codes created by hackers to damage the system, gain access to the system by force, or steal the target's valuable data. In the cyber world, malware is a frightening attack because it is specifically created to be hidden so that it can remain in a system without the antivirus and the system owner realizing it **[7]**.

2.4 Android

Android is a Linux-based operating system for mobile devices that we often encounter on various brands of smartphones and tablets. Android is an open-source operating system where developers can develop applications **[8]**.

2.5 MT Manager

MT Manager is a file management tool with a wide set of features such as file management, APK editing, and many more **[9]**. The MT manager application is an application used for application editors such as dissecting applications and modifying applications with app extensions.

3. Results and Discussion

In the following chapter, the author will analyze and dismantle the malware application used to break into the victim's Android smartphone. The author dismantled the malware for analysis and education for the public so that people know how dangerous this malware is.

3.1 Analysis

Before carrying out the analysis, the author will download the application sent by the perpetrator to the author's WhatsApp on behalf of a relative and send a wedding invitation attachment. After that, the application is decompiled to look like **Figure 1.**

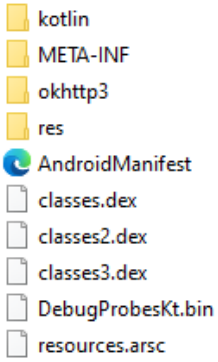

Figure 1. Decompiler Malware Application

Here the author has carried out the decompile and obtained the material to be analyzed. In the picture above there are folders and files, where if you see that the language used to create this malware is the Kotlin programming language. Kotlin is a programming language developed by JetBrains and this language is based on Java Virtual Machine, so the Kotlin programming language is pragmatic for Android which combines object-oriented and functional programming **[10]**. **Figure 2** decompiles the first classes.

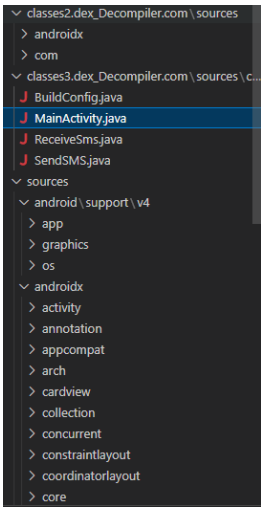

Figure 2. Decompiler File Classes

To analyze the malware, you must decompile the files again with the dex extension, namely the classes, classes2 and classes3 files. It can be seen in Figure 2 that the author has decompiled the files and after that, the author will search for and understand how the coding in the malware works. **Figure 3** is permission malware.

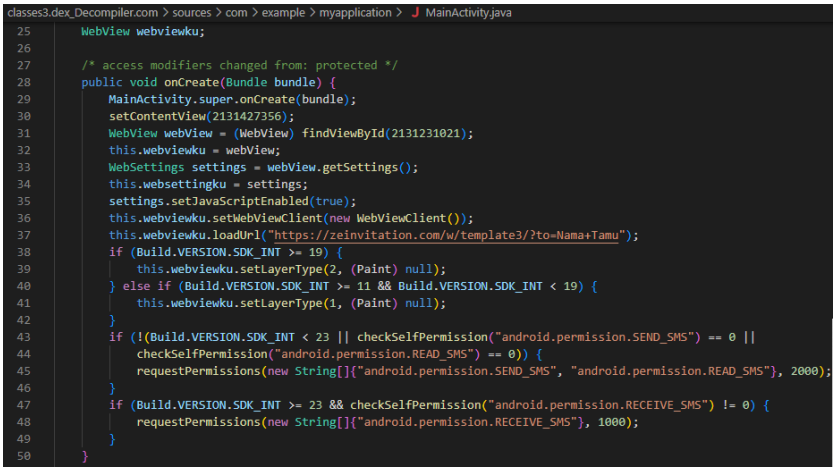

Figure 3. Permission Malware

After searching and understanding the flow of the malware program, we got results in classes3.dex on MainActivity.java, where in the code there is a load URL that leads to an online download web page that the perpetrator or hacker has created; the aim is to make the victim not suspicious of the application. when you have installed it. In the next coding there are android permissions including android. permission.SEND_SMS, android. permission.READ_SMS and android. permission.RECEIVE_SMS, these permissions are related to SMS, where if the victim allows these permissions, then the perpetrator can find out incoming SMS, access SMS history, and what's worse, again the perpetrator can send an SMS. **Figure 4** is receiving message.

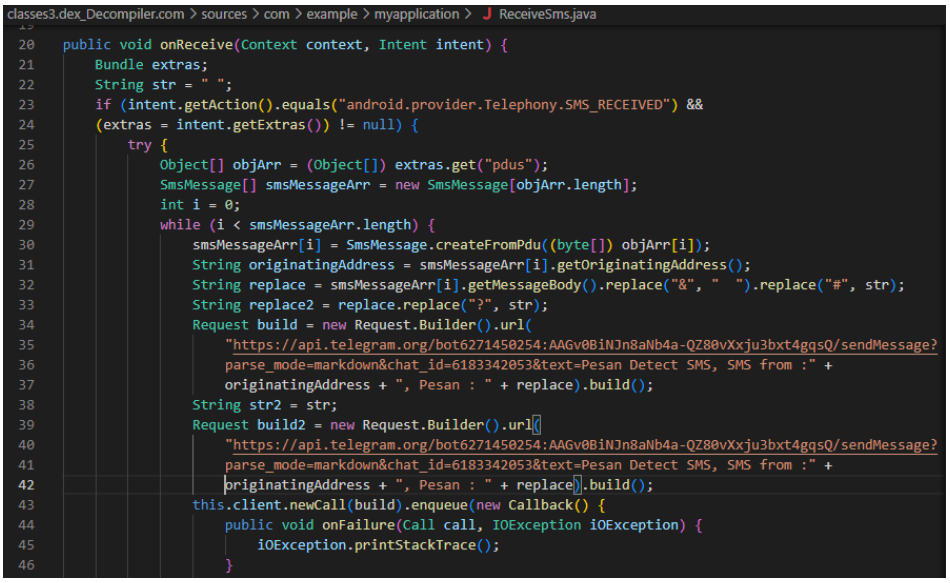

Figure 4. Receive SMS

Figure 4 refers to a file called ReceiveSMS.java. If you look at this coding, it will send all messages on the victim's Android to the perpetrator or hacker via a telegram bot that the

perpetrator has previously set, and this is very dangerous because this malware will send the data in real time, including if there is an incoming message related to the OTP.

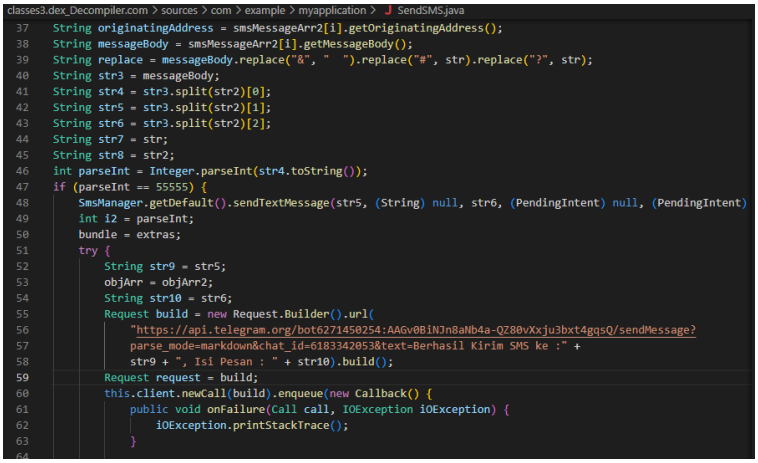

Figure 5. Send SMS

When this malware application has been installed and given access permission, the perpetrator can freely control the victim's Android, one of which can be seen in **Figure 5,** in this picture, there is coding that explains that every time a message is successfully sent, a notification will be sent back to the perpetrator's Telegram bot. This also poses a danger to the victim's mobile banking, especially those who activate SMS banking, because the perpetrator can transfer account balances via SMS banking commands.

3.2 Anticipation

From the explanation above, this malware application is very dangerous if installed on our Android, so we need to take precautions so that we don't become victims of this attack. Anticipations that need to be taken include, do not downloading and install suspicious applications provided via WhatsApp or any social media, downloading and install applications only on Play store, always update devices such as the operating system, software or firmware regularly to increase Android security, it is best not to open links provided by unknown people, carefully and study every time you give permission for the installed application and use updated antivirus and security tools.

4. Conclusion

Based on the analysis above, it can be concluded that in the current digital era, there are many hacker attacks that we need to know about and be aware of. One of these attacks is a phishing or malware application which can be dangerous for the security of our data. This malware application will run when the victim downloads, installs, and gives access permission

to this application. This malware uses SMS access to attack its victims, especially mobile banking which uses the SMS feature and OTP codes.

The author carried out this analysis based on news circulating that several victims lost their money in banking after installing this application and to date there are still many new perpetrators who have emerged using techniques like this. On this basis, the author analyzes and dismantles circulating malware applications to educate the public about the dangers of this malware.

References

[1] D. Wulandari and T. Lestari, "Pengaruh gadget terhadap perkembangan emosi anak," *J. Pendidik. Tambusai*, vol. 5, no. 1, pp. 1689–1695, 2021, [Online]. Available: https://jptam.org/index.php/jptam/article/view/1162?articlesBySameAuthorPage=2

[2] A. Dermawan, "Urgensi Perlindungan Hukum Bagi Korban Tindak Pidana Kejahatan Teknologi Informasi," *J. Sci. Soc. Res.*, vol. 4307, no. 2, pp. 39–46, 2019, [Online]. Available: http://jurnal.goretanpena.com/index.php/JSSR

[3] A. C. Wardaya, "Akibat Hukum Bug Hunter yang Melakukan Illegal Access Terhadap Aplikasi," vol. 3, pp. 2274–2285, 2023.

[4] M. Ziadia, J. Fattahi, M. Mejri, and E. Pricop, "Smali+: An operational semantics for low-level code generated from reverse engineering android applications," *Inf.*, vol. 11, no. 3, 2020, doi: 10.3390/info11030130.

[5] A. S. Gulo, S. Lasmadi, and K. Nawawi, "Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik," *PAMPAS J. Crim. Law*, vol. 1, no. 2, pp. 68–81, 2021, doi: 10.22437/pampas.v1i2.9574.

[6] M. H. Wibowo and N. Fatimah, "Ancaman Phishing Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime," *JOEICT(Jurnal Educ. Inf. Commun. Technol.*, vol. 1, no. 1, pp. 1–5, 2017, [Online]. Available: https://www.jurnal.stkippgritulungagung.ac.id/index.php/joeict/article/view/69

[7] Fatmawati and Raihana, "Analisis Yuridis Terhadap Artificial Intelligence Pada Tindak Pidana Penyebaran Malware Di Indonesia," *Innov. J. Soc. Sci. Res.*, vol. 3, no. 20, pp. 12190–12201, 2023.

[8] E. Maiyana, "Pemanfaatan Android Dalam Perancangan Aplikasi Kumpulan Doa," *J. Sains dan Inform.*, vol. 4, no. 1, pp. 54–65, 2018, doi: 10.22216/jsi.v4i1.3409.

[9] M. Manager, "Official MT Manager Pro Apk Download for Android - MT Manager Apk." https://mtmanager.app/ (accessed Feb. 22, 2024).

[10] A. T. Hidayat, R. Rio, and I. G. O. Santosa, "Membershipplication Berbasis Android Dengan Penerapan Kotlin Programming Language Di Wijaya Fitness Center (Wfc)," *JUSIM (Jurnal Sist. Inf. Musirawas)*, vol. 8, no. 1, pp. 8–15, 2023, [Online]. Available: https://jurnal.univbinainsan.ac.id/index.php/jusim/article/view/1952