1. **Scan the APK file using VirusTotal. What is the detection ratio as returned by VirusTotal?**

   27/62, where 27 security vendors flagged this as malicious

2. **Using apktool on Kali Linux, extract the contents of the APK file via `apktool d <name_of_app.apk>`. Take a look at the `AndroidManifest.xml` file. What permissions do the app have access to? Do any of the permissions look peculiar?**

   Some of the permissions:
   android.permission.ACCESS_FINE_LOCATION
   android.permission.SEND_SMS
   android.permission.READ_PHONE_STATE
   android.permission.ACCESS_COARSE_LOCATION
   android.permission.INTERNET
   android.permission.READ_CONTACTS
   android.permission.RECEIVE_BOOT_COMPLETED
   android.permission.ACCESS_NETWORK_STATE
   android.permission.FOREGROUND_SERVICE
   android.permission.ACCESS_WIFI_STATE

   Peculiar permissions:
   android.permission.SEND_SMS
   android.permission.READ_PHONE_STATE
   android.permission.ACCESS_COARSE_LOCATION
   android.permission.INTERNET
   android.permission.READ_CONTACTS

3. **Take a further look at the `AndroidManifest.xml` file, are there any peculiar activities or Java packages referenced?**

These activities/packages are mostly based out of com.jadhalno.goplotu

com.jadhalno.goplotu.Alt
com.jadhalno.goplotu.Fini
com.jadhalno.goplotu.Special
com.jadhalno.goplotu.login
com.jadhalno.goplotu.MainActivity
com.startapp.sdk.adsbase.consent.ConsentActivity
com.startapp.sdk.ads.list3d.List3DActivity
com.startapp.sdk.adsbase.activities.OverlayActivity
com.startapp.sdk.adsbase.activities.FullScreenActivity

4. **Take a look at all the files in the resources folder `res`. Are there any files look suspicious?**

Below are the folders in res that has suspicious files. They are images/pictures of TikTok logo. Some of the pictures are blurry and also there is a space/gap in some of the pictures between 'Tik' and 'Tok'. In addition, these images come in various sizes (circle or square border shape) and background (black vs white), which doesn't seem to correlated with real TikTok brand. As a sophisticated company, there shouldn't be any branding or logo issues and this is clearly a mistake of a fraudster.

drawable
mipmap-hdpi-v4
mipmap-mdpi-v4
mipmap-xhdpi-v4
mipmap-xxhdpi-v4
mipmap-xxxhdpi-v4

5. **Find and list any suspicious HTTP and/or HTTPS URLs used in `.smali` files. In which `.smail` file(s) did you find suspicious HTTP and/or HTTPS URLs? If you find any suspicious URLs, send them to VirusTotal for analysis, and provide the VirusTotal detection ratio for each URL.**

Path	file	URL	Ratio
Smali/com/jadhalno/goplotu	Act.smali	https://www.jio.com/api/jio-recharge-service/recharge/submitNumber	0/82
Smali/com/jadhalno/goplotu	Act.smali	www.jio.com	1/83
Smali/com/jadhalno/goplotu	Act.smali	https://www.jio.com/JioApp/index.html?root=primeRecharge/	0/79

6. **What does this app really do, or what do you think this app really do? Provide a brief synopsis. Show all evidence including lines of code in question, and cite any references.**

It looks like a TikTok app by looking at various folder in rec (directory), which means a social engineering technique. Attack strategy starts with a SMS or messaging where a tiny URL is sent to direct such users to another website (weebly.com) owned by an fraudster/attacker. In this case, the website is for the app TikTok to download. The SMS spread is happening via SMS on phone service company name JIO.

https://www.zscaler.com/blogs/security-research/android-apps-targeting-jio-users-india