Malware Analysis-Lab-10

Virus Total Score: 39/60

Permissions:

- INTERNET
- WAKELOCK
- READ SMS
- RECEIVE SMS
- Read External Storage
- Write External Storage
- Read PHONE State
- Send SMS
- Receive Boot Complete
- READ Contact
- Access Fine Location
- Access Mock Location
- Access Location Extra Commands
- Bind Device Admin
- Get Tasks
- Access Network State

Java packages that look peculiar in `AndroidManifest.xml`:

- MainActivity
- Browser
- BrowserActivity
- Lock
- Google CC
- Inject
- BankApp
- Run Script

Res folder's stuff:

1. Bootscriptnet.js:
   - Writing SMS and sending to an unknown phone number
   - There's some kind of locking taking place as well
   - A service enabling injection
2. App can reset password, delete data and watch logins without user's consent

Some URLS I found:

I tried using cat and grep and then finally ended up using jd-gui.

1. http://23.227.163.110/locker.php
   Virus Total Detection ratio: 2/67

2. http://192.227.137.154/request.php
   Virus Total Detection ratio: 2/67

3. 81.94.205.226
   Virus Total Detection ratio: 1/67

A brief Synopsis:

It seems like the application is a trojan that tries to steal the information of users and then can be used as a ransomware by locking the users' phones and encrypting their information. The functionality of the app is present in the RunService.class file and it receives commands from an unknown server aided by an external library called KryoNet (https://github.com/EsotericSoftware/kryonet).