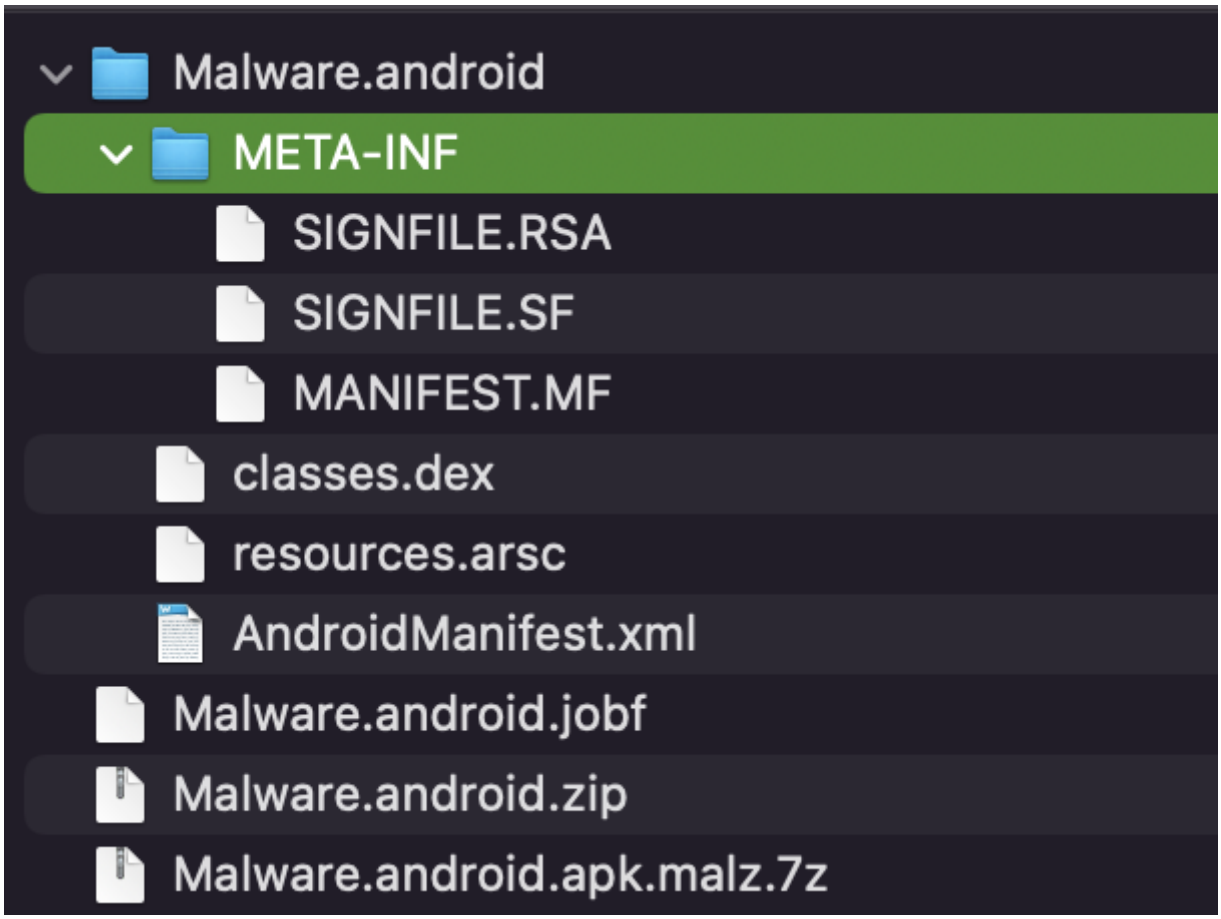
Mobile Malware

> https://github.com/HuskyHacks/PMAT-labs/blob/main/labs/3-6.Mobile-Malware/Android/Malware.android.apk.malz.7z

In this section, we are going to analyze the Mobile Malware. The APK file is provided on the mentioned URL.

APK files are basically zip files and we can change their extension from .APK to .ZIP and can unzip them.



Also, we can load the APK in JADX-GUI, it will decompile the code automatically and will provide us with the calsses and files.

In the below screenshot, we can observe the following.

- The package name is **com.metasploit.stage**
- The application is developed for the Android SDK version targetting `<uses-sdk android:minSdkVersion="10" android:targetSdkVersion="17"/>`
- The application uses the hardware features.
  - Get's access to Camera
  - Camera Autofocus
  - Microphone

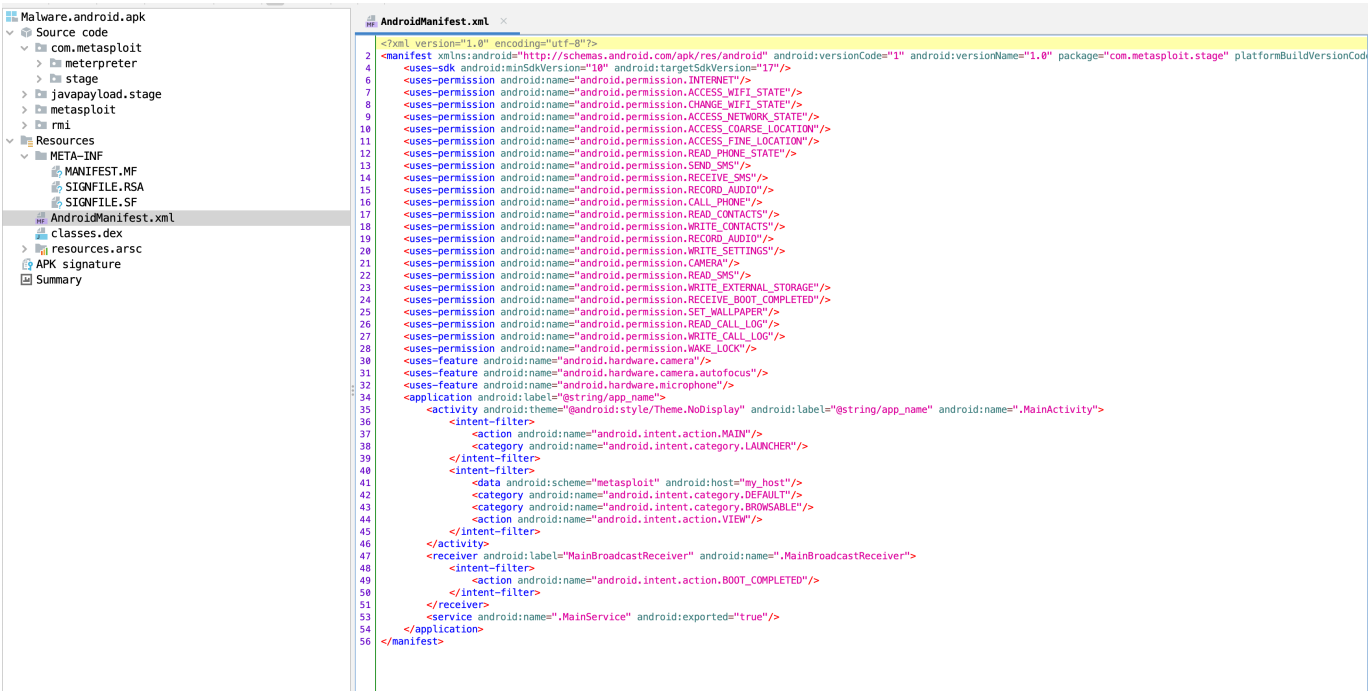
```
 <uses-feature android:name="android.hardware.camera"/>
 <uses-feature
android:name="android.hardware.camera.autofocus"/>
 <uses-feature android:name="android.hardware.microphone"/>
```

- Application get's access to multiple permissions most of which an application should not have.

```
 <uses-permission android:name="android.permission.INTERNET"/>
 <uses-permission
android:name="android.permission.ACCESS_WIFI_STATE"/>
 <uses-permission
android:name="android.permission.CHANGE_WIFI_STATE"/>
 <uses-permission
android:name="android.permission.ACCESS_NETWORK_STATE"/>
 <uses-permission
android:name="android.permission.ACCESS_COARSE_LOCATION"/>
 <uses-permission
android:name="android.permission.ACCESS_FINE_LOCATION"/>
 <uses-permission
android:name="android.permission.READ_PHONE_STATE"/>
 <uses-permission android:name="android.permission.SEND_SMS"/>
```

```
 <uses-permission
android:name="android.permission.RECEIVE_SMS"/>
 <uses-permission
android:name="android.permission.RECORD_AUDIO"/>
 <uses-permission android:name="android.permission.CALL_PHONE"/>
 <uses-permission
android:name="android.permission.READ_CONTACTS"/>
 <uses-permission
android:name="android.permission.WRITE_CONTACTS"/>
 <uses-permission
android:name="android.permission.RECORD_AUDIO"/>
 <uses-permission
android:name="android.permission.WRITE_SETTINGS"/>
 <uses-permission android:name="android.permission.CAMERA"/>
 <uses-permission android:name="android.permission.READ_SMS"/>
 <uses-permission
android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
 <uses-permission
android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
 <uses-permission
android:name="android.permission.SET_WALLPAPER"/>
 <uses-permission
android:name="android.permission.READ_CALL_LOG"/>
 <uses-permission
android:name="android.permission.WRITE_CALL_LOG"/>
 <uses-permission android:name="android.permission.WAKE_LOCK"/>
```

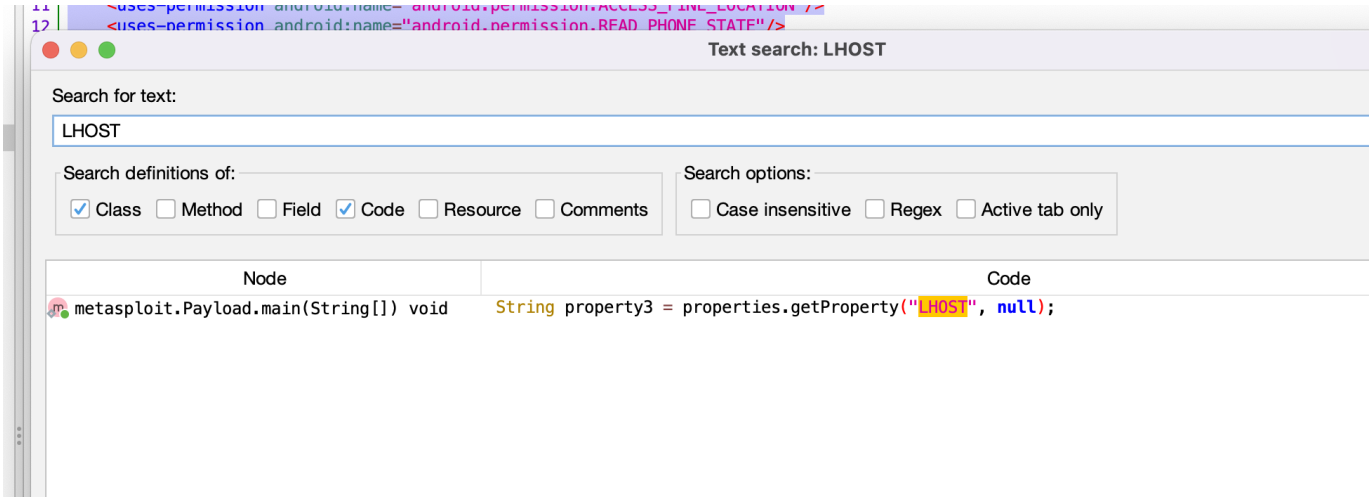
- The APK is generated using MSFVENOM.



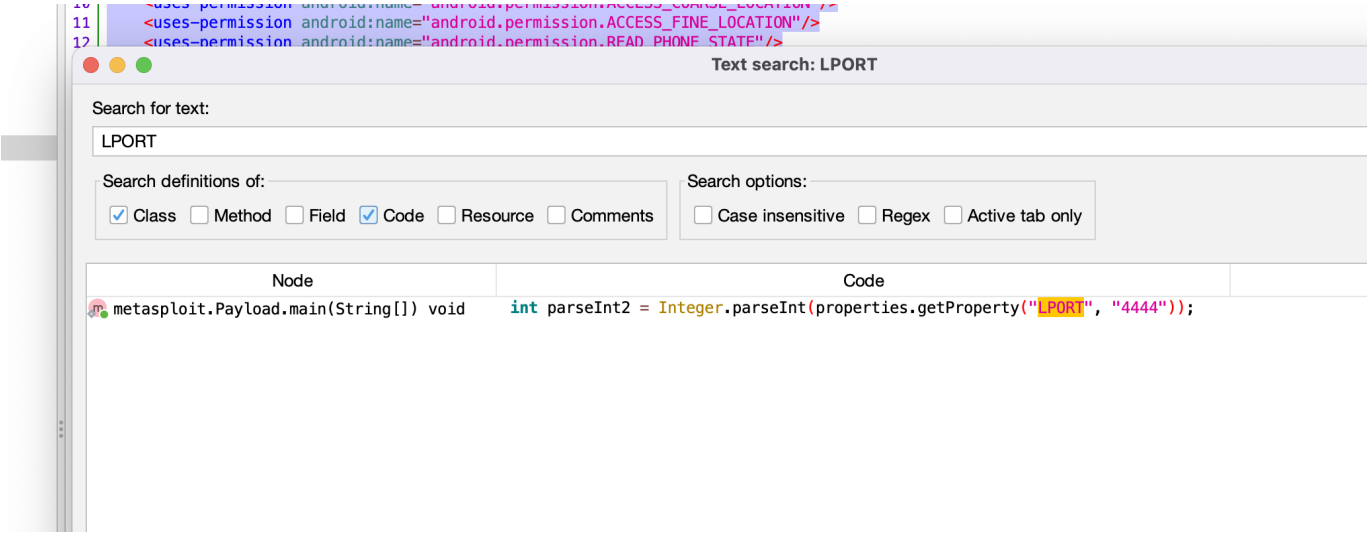
We can also scan the Android App using MobSF.

- In simple words, this APK is malicious i.e. when it will get installed on the Android Device, it will send back a meterpreter session back to the attacker IP Address and Listening Port.

In the below screenshot we can see that LHOST has not been defined.



In the below screenshot we can see that LPORT is set to 4444.



MobSF gives us a loads of information related the the calls an application can make. In the below screenshot we can observe that this particular APK includes fucntions which can make commands to be executed via SHELL.

Execute OS Command	com/metasploit/meterpreter/stdapi/stdapi_sys_process_execute_V1_3.java com/metasploit/meterpreter/android/stdapi_sys_process_get_processes_android.java com/metasploit/meterpreter/Utils.java com/metasploit/meterpreter/stdapi/stdapi_sys_process_execute.java com/metasploit/meterpreter/android/android_check_root.java javapayload/stage/Shell.java metasploit/Payload.java com/metasploit/meterpreter/stdapi/stdapi_sys_process_get_processes.java

Android Location, Audio Mode, Cell Information Collection and many more.

Get System Service	com/metasploit/stage/Payload.java com/metasploit/meterpreter/android/android_geolocate.java com/metasploit/meterpreter/WifiCollector.java com/metasploit/meterpreter/android/webcam_start_android.java com/metasploit/meterpreter/android/android_set_audio_mode.java com/metasploit/meterpreter/android/android_wlan_geolocate.java com/metasploit/meterpreter/android/android_wakelock.java com/metasploit/meterpreter/CellCollector.java com/metasploit/meterpreter/android/appapi_app_list.java com/metasploit/meterpreter/GeolocationCollector.java com/metasploit/meterpreter/ClipManager.java
GPS Location	com/metasploit/meterpreter/android/android_geolocate.java com/metasploit/meterpreter/GeolocationCollector.java

Follow Me

Twitter: https://twitter.com/deFr0ggy

GitHub: https://github.com/deFr0ggy

LinkedIn: https://linkedin.com/in/kamransaifullah