

工具: Apktool、apksign

1. APK 脱壳得到 dex 文件
2. 通过 Apktool 对 APK 解包

命令: java -jar apktool.jar d /xxx/xxx.apk -o /xxx/xxx

```
D:\逆向分析工具箱>java -jar apktool.jar d D:\1\疫苗接种.apk -o D:\1\ym
I: Using Apktool 2.5.0 on 疫苗接种.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: C:\Users\41314\AppData\Local\apktool\framework\1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
```

3. 对解包后的 AndroidManifest.xml 进行修改, 修改程序入口, 删除壳的内容

```
1 <?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android=
"http://schemas.android.com/apk/res/android" android:compileSdkVersion="29" android:compileSdkVersionCodename=
"10" package="com.shanghai.Covid19.vaccine.appointment" platformBuildVersionCode="29" platformBuildVersionName=
"10">
2   <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
3   <uses-permission android:name="android.permission.INTERNET"/>
4   <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
5   <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
6   <uses-permission android:name="android.permission.READ_CONTACTS"/>
7   <uses-permission android:name="android.permission.CAMERA"/>
8   <uses-permission android:name="android.permission.RECORD_AUDIO"/>
9   <uses-permission android:name="android.permission.READ_SMS"/>
10  <application android:appComponentFactory="com.SecShell.SecShell.AP" android:icon="@mipmap/logo"
    android:label="@string/app_name" android:name="com.SecShell.SecShell.AW"
    android:requestLegacyExternalStorage="true" android:roundIcon="@mipmap/logo" android:theme="@style/AppTheme"
    android:usesCleartextTraffic="true">
11    <activity android:name="com.shanghai.Covid19.vaccine.appointment.photoActivity"/>
12    <activity android:label="@string/title_activity_mail" android:name=
    "com.shanghai.Covid19.vaccine.appointment.mailActivity" android:theme="@style/AppTheme.NoActionBar"/>
13    <activity android:name="com.shanghai.Covid19.vaccine.appointment.LoginActivity" android:theme=
    "@style/AppThemeShowAll"/>
14    <meta-data android:name="android.max_aspect" android:value="2.4"/>
15    <activity android:name="com.shanghai.Covid19.vaccine.appointment.IndexActivity" android:theme=
    "@style/AppThemeShowAll">
16      <intent-filter>
17        <action android:name="android.intent.action.MAIN"/>
18        <category android:name="android.intent.category.LAUNCHER"/>
19      </intent-filter>
20    </application>
21 </manifest>
```

application 中

android:appComponentFactory 改回原入口 androidx.core.app.AppCompatActivity

android:name 直接整个删掉

```
1 <?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android=
"http://schemas.android.com/apk/res/android" android:compileSdkVersion="29" android:compileSdkVersionCodename=
"10" package="com.shanghai.Covid19.vaccine.appointment" platformBuildVersionCode="29" platformBuildVersionName=
"10">
2   <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
3   <uses-permission android:name="android.permission.INTERNET"/>
4   <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
5   <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
6   <uses-permission android:name="android.permission.READ_CONTACTS"/>
7   <uses-permission android:name="android.permission.CAMERA"/>
8   <uses-permission android:name="android.permission.RECORD_AUDIO"/>
9   <uses-permission android:name="android.permission.READ_SMS"/>
10  <application android:appComponentFactory="androidx.core.app.AppCompatActivity" android:icon="@mipmap/logo"
    android:label="@string/app_name" android:requestLegacyExternalStorage="true" android:roundIcon=
    "@mipmap/logo" android:theme="@style/AppTheme" android:usesCleartextTraffic="true">
11    <activity android:name="com.shanghai.Covid19.vaccine.appointment.photoActivity"/>
12    <activity android:label="@string/title_activity_mail" android:name=
    "com.shanghai.Covid19.vaccine.appointment.mailActivity" android:theme="@style/AppTheme.NoActionBar"/>
13    <activity android:name="com.shanghai.Covid19.vaccine.appointment.LoginActivity" android:theme=
    "@style/AppThemeShowAll"/>
14    <meta-data android:name="android.max_aspect" android:value="2.4"/>
15    <activity android:name="com.shanghai.Covid19.vaccine.appointment.IndexActivity" android:theme=
    "@style/AppThemeShowAll">
16      <intent-filter>
17        <action android:name="android.intent.action.MAIN"/>
18        <category android:name="android.intent.category.LAUNCHER"/>
19      </intent-filter>
20    </application>
21 </manifest>
```

4. 如有其他输入壳的东西, 如壳的 provider, 直接删掉, 保留原 provider

```

16 <intent-filter>
17 <action android:name="android.intent.action.MAIN"/>
18 <category android:name="android.intent.category.LAUNCHER"/>
19 </intent-filter>
20 </activity>
21 <activity android:name="com.shanghai.Covid19.vaccine.appointment.MainActivity" android:theme=
22 "@style/AppThemeNoTitle"/>
23 <activity android:name="com.shanghai.Covid19.vaccine.appointment.PayActivity" android:theme=
24 "@style/AppThemeNoTitle"/>
25 <activity android:name="com.shanghai.Covid19.vaccine.appointment.PayTempActivity"/>
26 <activity android:name="com.yalantis.ucrop.UCropActivity" android:screenOrientation="portrait"
27 android:theme="@style/Theme.AppCompat.Light.NoActionBar"/>
28 <provider android:authorities="com.shanghai.Covid19.vaccine.appointment.fileProvider" android:exported=
29 "false" android:grantUriPermissions="true" android:name="androidx.core.content.FileProvider">
30 <meta-data android:name="android.support.FILE_PROVIDER_PATHS" android:resource="@xml/file_path"/>
31 </provider>
32 <service android:enabled="true" android:exported="true" android:name=
33 "com.shanghai.Covid19.vaccine.appointment.service.MsgService" android:permission=
34 "android.permission.BIND_NOTIFICATION_LISTENER_SERVICE" android:priority="1000">
35 <intent-filter android:priority="1000">
36 <action android:name="android.service.notification.NotificationListenerService"/>
37 </intent-filter>
38 </service>
39 <provider android:authorities="com.shanghai.Covid19.vaccine.appointment.CP" android:exported="false"
40 android:initOrder="2147483647" android:name="com.secneo.apkwrapper.CP"/>
41 </application>
42 </manifest>

```

```

15 <activity android:name="com.shanghai.Covid19.vaccine.appointment.IndexActivity" android:theme=
16 "@style/AppThemeShowAll">
17 <intent-filter>
18 <action android:name="android.intent.action.MAIN"/>
19 <category android:name="android.intent.category.LAUNCHER"/>
20 </intent-filter>
21 </activity>
22 <activity android:name="com.shanghai.Covid19.vaccine.appointment.MainActivity" android:theme=
23 "@style/AppThemeNoTitle"/>
24 <activity android:name="com.shanghai.Covid19.vaccine.appointment.PayActivity" android:theme=
25 "@style/AppThemeNoTitle"/>
26 <activity android:name="com.shanghai.Covid19.vaccine.appointment.PayTempActivity"/>
27 <activity android:name="com.yalantis.ucrop.UCropActivity" android:screenOrientation="portrait"
28 android:theme="@style/Theme.AppCompat.Light.NoActionBar"/>
29 <provider android:authorities="com.shanghai.Covid19.vaccine.appointment.fileProvider" android:exported=
30 "false" android:grantUriPermissions="true" android:name="androidx.core.content.FileProvider">
31 <meta-data android:name="android.support.FILE_PROVIDER_PATHS" android:resource="@xml/file_path"/>
32 </provider>
33 <service android:enabled="true" android:exported="true" android:name=
34 "com.shanghai.Covid19.vaccine.appointment.service.MsgService" android:permission=
35 "android.permission.BIND_NOTIFICATION_LISTENER_SERVICE" android:priority="1000">
36 <intent-filter android:priority="1000">
37 <action android:name="android.service.notification.NotificationListenerService"/>
38 </intent-filter>
39 </service>
40 </application>
41 </manifest>

```

5. 用 apktool 回编译 APK

命令: java -jar apktool.jar b --use-aapt2 /xxx/xxx -o /xxx/xxx.apk

```

D:\逆向分析工具箱>java -jar apktool.jar b --use-aapt2 D:\1\ym -o ym.apk
I: Using Apktool 2.5.0
I: Checking whether sources has changed...
I: Smaling smali folder into classes.dex...
I: Checking whether resources has changed...
I: Building resources...
I: Copying libs... (/lib)
I: Copying libs... (/kotlin)
I: Building apk file...
I: Copying unknown files/dir...
I: Built apk...

```

6. 把脱壳出来的 dex 文件改成 classes.dex, 替换 apk 压缩包中的 dex 文件

7. 最后重新签名完成修复