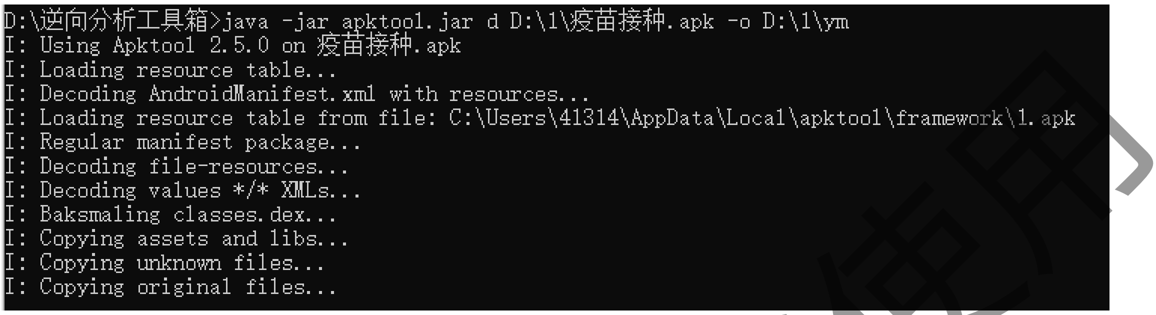
工具：Apktool、apksign

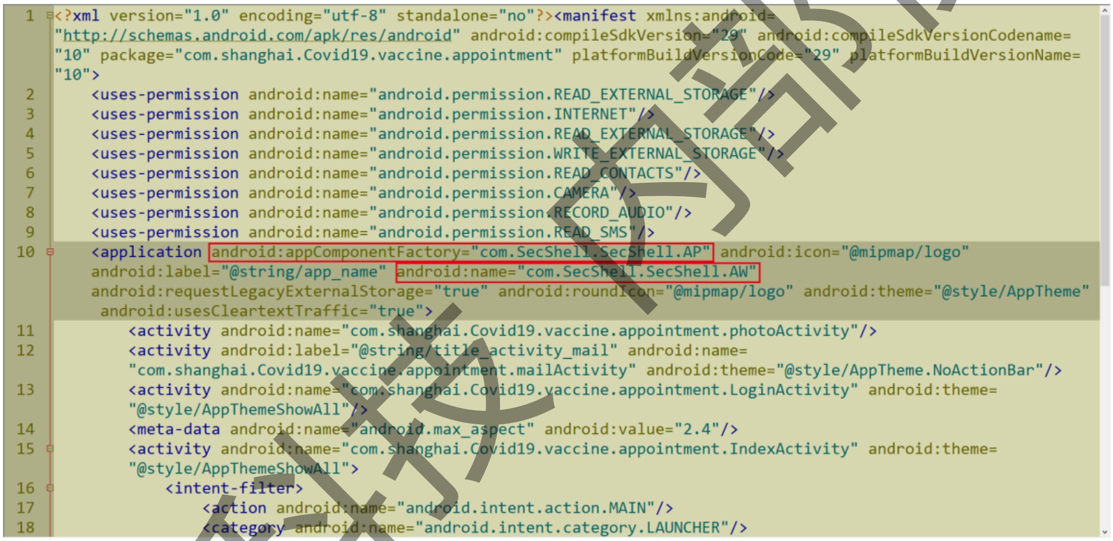
1. APK 脱壳得到 dex 文件
2. 通过 Apktool 对 APK 解包

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

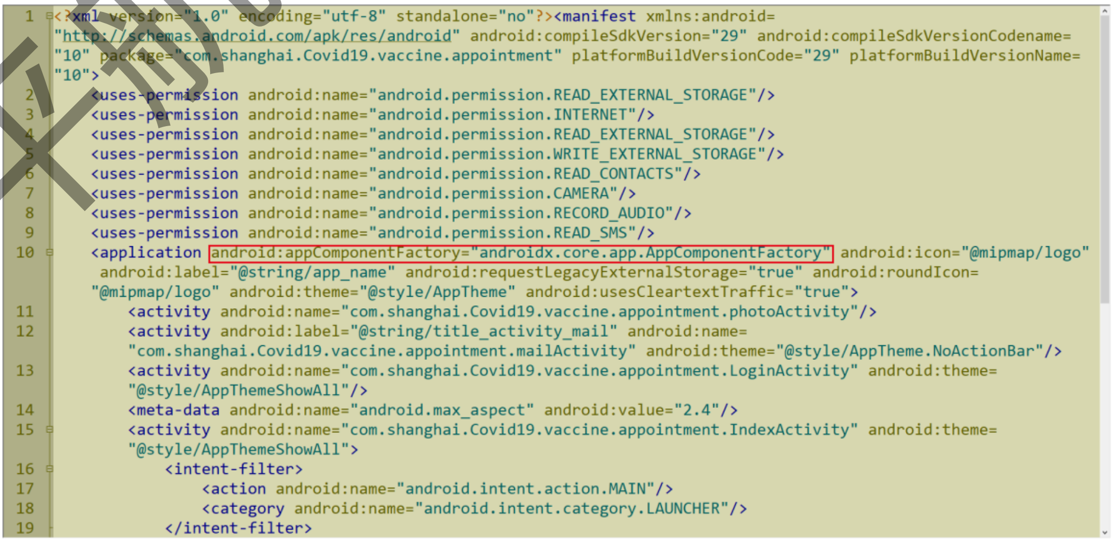


```
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/android" android:compileSdkVersion="29" android:compileSdkVersionCodename="10" package="com.shanghai.Covid19.vaccine.appointment" platformBuildVersionCode="29" platformBuildVersionName="10">
    <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.READ_CONTACTS"/>
    <uses-permission android:name="android.permission.CAMERA"/>
    <uses-permission android:name="android.permission.RECORD_AUDIO"/>
    <uses-permission android:name="android.permission.READ_SMS"/>
    <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">
        <activity android:name="com.shanghai.Covid19.vaccine.appointment.photoActivity"/>
        <activity android:label="@string/title_activity_mail" android:name="com.shanghai.Covid19.vaccine.appointment.mailActivity" android:theme="@style/AppTheme.NoActionBar"/>
        <activity android:name="com.shanghai.Covid19.vaccine.appointment.LoginActivity" android:theme="@style/AppThemeShowAll"/>
        <meta-data android:name="android.max_aspect" android:value="2.4"/>
        <activity android:name="com.shanghai.Covid19.vaccine.appointment.IndexActivity" android:theme="@style/AppThemeShowAll">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
```

application 中

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

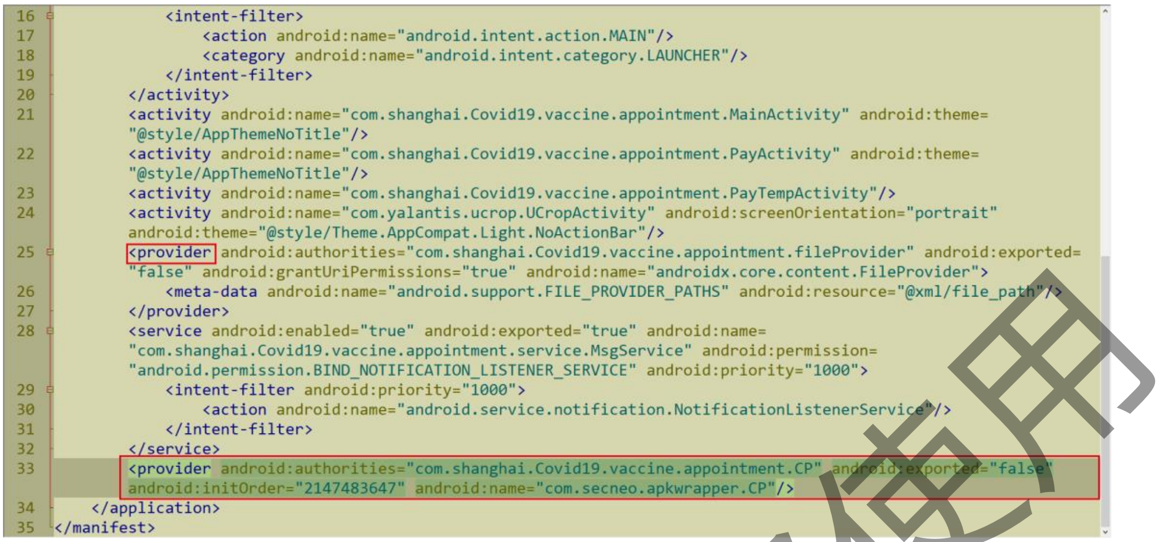
android:name 直接整个删掉



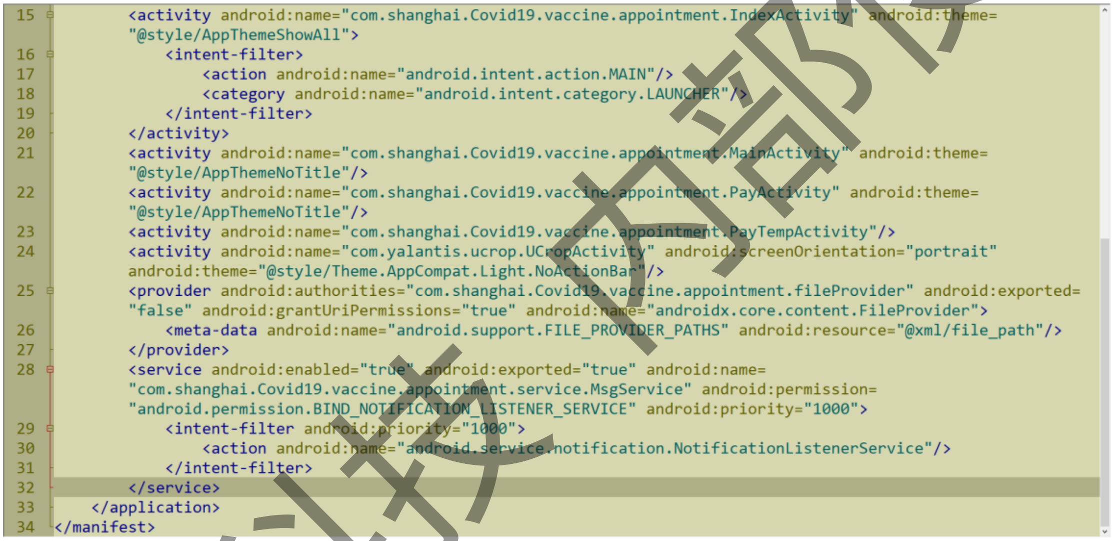
```
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/android" android:compileSdkVersion="29" android:compileSdkVersionCodename="10" package="com.shanghai.Covid19.vaccine.appointment" platformBuildVersionCode="29" platformBuildVersionName="10">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

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

平航科技内部使用



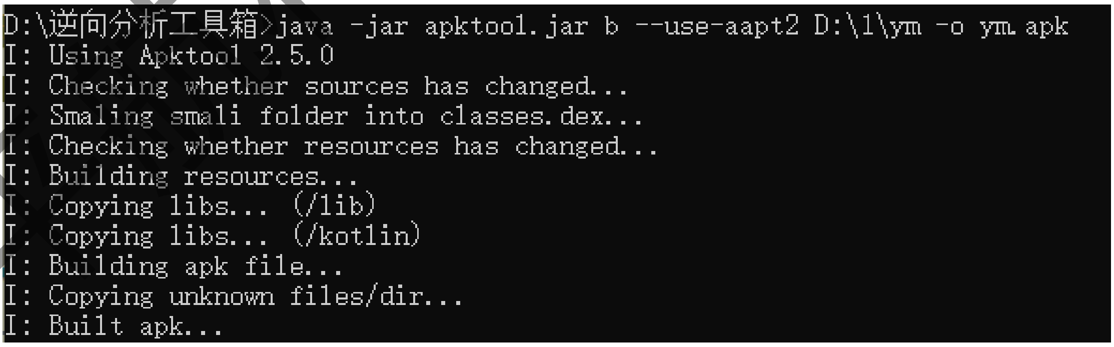
```
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
        </activity>
        <activity android:name="com.shanghai.Covid19.vaccine.appointment.MainActivity" android:theme=
        "@style/AppThemeNoTitle"/>
        <activity android:name="com.shanghai.Covid19.vaccine.appointment.PayActivity" android:theme=
        "@style/AppThemeNoTitle"/>
        <activity android:name="com.shanghai.Covid19.vaccine.appointment.PayTempActivity"/>
        <activity android:name="com.yalantis.ucrop.UCropActivity" android:screenOrientation="portrait"
        android:theme="@style/Theme.AppCompat.Light.NoActionBar"/>
        <provider android:authorities="com.shanghai.Covid19.vaccine.appointment.fileProvider" android:exported=
        "false" android:grantUriPermissions="true" android:name="androidx.core.content.FileProvider">
            <meta-data android:name="android.support.FILE_PROVIDER_PATHS" android:resource="@xml/file_path"/>
        </provider>
        <service android:enabled="true" android:exported="true" android:name=
        "com.shanghai.Covid19.vaccine.appointment.service.MsgService" android:permission=
        "android.permission.BIND_NOTIFICATION_LISTENER_SERVICE" android:priority="1000">
            <intent-filter android:priority="1000">
                <action android:name="android.service.notification.NotificationListenerService"/>
            </intent-filter>
        </service>
        <provider android:authorities="com.shanghai.Covid19.vaccine.appointment.CP" android:exported="false"
        android:initOrder="2147483647" android:name="com.secneo.apkwrapper.CP"/>
    </application>
</manifest>
```



```
        <activity android:name="com.shanghai.Covid19.vaccine.appointment.IndexActivity" android:theme=
        "@style/AppThemeShowAll">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
        </activity>
        <activity android:name="com.shanghai.Covid19.vaccine.appointment.MainActivity" android:theme=
        "@style/AppThemeNoTitle"/>
        <activity android:name="com.shanghai.Covid19.vaccine.appointment.PayActivity" android:theme=
        "@style/AppThemeNoTitle"/>
        <activity android:name="com.shanghai.Covid19.vaccine.appointment.PayTempActivity"/>
        <activity android:name="com.yalantis.ucrop.UCropActivity" android:screenOrientation="portrait"
        android:theme="@style/Theme.AppCompat.Light.NoActionBar"/>
        <provider android:authorities="com.shanghai.Covid19.vaccine.appointment.fileProvider" android:exported=
        "false" android:grantUriPermissions="true" android:name="androidx.core.content.FileProvider">
            <meta-data android:name="android.support.FILE_PROVIDER_PATHS" android:resource="@xml/file_path"/>
        </provider>
        <service android:enabled="true" android:exported="true" android:name=
        "com.shanghai.Covid19.vaccine.appointment.service.MsgService" android:permission=
        "android.permission.BIND_NOTIFICATION_LISTENER_SERVICE" android:priority="1000">
            <intent-filter android:priority="1000">
                <action android:name="android.service.notification.NotificationListenerService"/>
            </intent-filter>
        </service>
    </application>
</manifest>
```

5. 用 apktool 回编译 APK

命令：java -jar apktool.jar b –use-aapt2 /xxx/xxxx -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

科技内部使用