Evaluation Warning: The document was created with Spire.Doc for Python.

**往后余生（ 15.22.23版本）
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | 往后余生 |
| 版本 | 15.22.23 |
| 包名 | pt.q5VsU29b.lUi8z13u |
| 域名线索 | 2条 |
| URL线索 | 6条 |
| APP图标 |  |
| 分析日期 | 2025年7月31日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | 往后余生.apk |
| 文件大小 | 24.57MB |
| MD5值 | 173c2cd8743eb4aae510e2fd6e3bc2c4 |
| SHA1值 | b512dd7a8e63dcbbeac80e968ea8a601b2eb8337 |
| SHA256值 | eea0feab6f6ee10f0116b6f7c2c2e8159fb7e21056f89e2df2dffd0473c97a70 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 往后余生 |
| 包名 | pt.q5VsU29b.lUi8z13u |
| 主活动Activity | .main |
| 安卓版本名称 | 15.22.23 |
| 安卓版本 | 2223 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| schemas.android.com | 没有服务器地理信息.  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://github.com/kongzue/DialogX/wiki  | com/kongzue/dialogx/DialogX.java  |
| https://github.com/kongzue/DialogX  | com/kongzue/dialogx/interfaces/BaseDialog.java  |
| https://github.com/kongzue/DialogX  | com/kongzue/dialogx/impl/ActivityLifecycleImpl.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/GifViewUtils.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/GifTextureView.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/GifTextView.java  |

### **4.3 邮箱线索**

### **4.4 手机号线索**

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: True 找到 1 个唯一证书 主题: C=o2bm0ZWKVkIGmHWf, ST=BulpfWsSM8e93p8R, L=RQZB9qninK5Vof84, O=T7Cl21752589081144, OU=dqj1752589081144, CN=Re0r1752589081144 签名算法: rsassa\_pkcs1v15 有效期自: 2025-07-15 14:18:01+00:00 有效期至: 2075-07-15 14:18:01+00:00 发行人: C=o2bm0ZWKVkIGmHWf, ST=BulpfWsSM8e93p8R, L=RQZB9qninK5Vof84, O=T7Cl21752589081144, OU=dqj1752589081144, CN=Re0r1752589081144 序列号: 0xcaa22e81191f8aa3 哈希算法: sha256 md5值: bc64dcb66bafbc4b7f71bf799431bd7d sha1值: 36b3b50abe00aca08c862eecd5420e005fffa7dc sha256值: 4ea857e2ad10864d48c2f0b986b0df12bcfce5e398a7d4c12f2a3ffc9c540995 sha512值: f92e23445ab82eda37d08df3def30deafdaf1a4e65e3c9d75e096d383f6878be5f9f680923123d3064e0e8faa555e5bbbcef90e7f55f6b17613612f19eb80c44 公钥算法: rsa 密钥长度: 2048 指纹: 770f888a9774415c90cf3133e9b58c8bce3efa6494a1b8a9c695e900a81c52e9**

## **6. 硬编码敏感信息**

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看  |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看  |  |  |

## **9. 此APP的危险动作**

| 向手机申请的权限 | 是否危险 | 类型  | 详细情况 |
| --- | --- | --- | --- |
| android.permission.READ\_PHONE\_STATE | 危险 | 读取电话状态和身份 | 允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等 |
| android.permission.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| android.permission.ACCESS\_NETWORK\_STATE | 正常 | 查看网络状态 | 允许应用程序查看所有网络的状态 |
| android.permission.ACCESS\_FINE\_LOCATION | 危险 | 精细定位（GPS） | 访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量 |
| android.permission.READ\_EXTERNAL\_STORAGE | 危险 | 读取外部存储器内容 | 允许应用程序从外部存储读取 |
| android.permission.READ\_CALL\_LOG | 危险 |  | 允许应用程序读取用户的通话日志 |
| android.permission.READ\_CONTACTS | 危险 | 读取联系人数据 | 允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人 |
| android.permission.READ\_SMS | 危险 | 阅读短信或彩信 | 允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息 |
| android.permission.QUERY\_ALL\_PACKAGES | 正常 |  | 允许查询设备上的任何普通应用程序,无论清单声明如何 |
| android.permission.SYSTEM\_ALERT\_WINDOW | 危险 | 显示系统级警报 | 允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕 |
| android.permission.ACCESS\_NOTIFICATION\_POLICY | 正常 |  | 希望访问通知策略的应用程序的标记权限。 |

## **10. 应用内通信**

**报告由**  [**摸瓜APK反编译平台**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**