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

**同城约（ 1.0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 | 同城约 |
| 版本 | 1.0 |
| 包名 | com.eg.android.csipayGphone.igum |
| 域名线索 | 10条 |
| URL线索 | 14条 |
| APP图标 |  |
| 分析日期 | 2025年7月18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 | 同城约.apk |
| 文件大小 | 10.09MB |
| MD5值 | 2c05bf97cca8716dd666faea15bdd6c6 |
| SHA1值 | 9c8b9f0f2de7a515da1f6012c6212198fd615b71 |
| SHA256值 | 0240df3e1dd5376d6daa24590065bde500b1f28e9ebc93afb9a88a9a23269cc4 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 同城约 |
| 包名 | com.eg.android.csipayGphone.igum |
| 主活动Activity | com.eg.android.csipayGphone.igum.LoginActivity |
| 安卓版本名称 | 1.0 |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| adiu.amap.com | IP: 110.253.189.147 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| apilocate.amap.com | IP: 106.11.43.81 所属国家: China 地区: Beijing 城市: Beijing  |
| schemas.android.com | 没有服务器地理信息.  |
| restsdk.amap.com | IP: 203.119.169.174 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| www.tonghua.center | IP: 103.140.238.70 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| cgicol.amap.com | IP: 110.253.188.148 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| lbs.amap.com | IP: 110.253.188.148 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| dualstack-a.apilocate.amap.com | IP: 59.82.31.183 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| abroad.apilocate.amap.com | IP: 59.82.44.11 所属国家: China 地区: Shanghai 城市: Shanghai  |
| dualstack-arestapi.amap.com | IP: 203.119.169.174 所属国家: China 地区: Zhejiang 城市: Hangzhou  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://www.tonghua.center/  | com/eg/android/csipayGphone/igum/Api.java  |
| https://adiu.amap.com/ws/device/adius  | com/loc/be.java  |
| http://cgicol.amap.com/collection/collectData?src=baseCol&ver=v74&  | com/loc/cu.java  |
| http://apilocate.amap.com/mobile/binary  | com/loc/fi.java  |
| http://dualstack-a.apilocate.amap.com/mobile/binary  | com/loc/fi.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | com/loc/fi.java  |
| https://restsdk.amap.com/sdk/compliance/params  | com/loc/ao.java  |
| http://restsdk.amap.com/sdk/compliance/params  | com/loc/ao.java  |
| http://restsdk.amap.com  | com/loc/u.java  |
| http://restsdk.amap.com/v3/place/text?  | com/loc/a.java  |
| http://restsdk.amap.com/v3/place/around?  | com/loc/a.java  |
| http://restsdk.amap.com/v3/config/district?  | com/loc/a.java  |
| https://restsdk.amap.com/v3/iasdkauth  | com/loc/l.java  |
| https://dualstack-arestapi.amap.com/v3/iasdkauth  | com/loc/l.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | com/loc/fn.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | com/loc/fb.java  |
| http://dualstack-arestapi.amap.com/v3/geocode/regeo  | com/loc/fd.java  |
| http://restsdk.amap.com/v3/geocode/regeo  | com/loc/fd.java  |
| http://schemas.android.com/apk/res/android  | com/hjq/permissions/AndroidManifestParser.java  |
| http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/  | com/amap/api/location/AMapLocation.java  |

### **4.3 邮箱线索**

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 15222222222  | com/loc/l.java  |

## **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=chengdu, ST=chengdu, L=chengdu, O=mu1752253208693, OU=go1752253208693, CN=dvyv 签名算法: rsassa\_pkcs1v15 有效期自: 2025-07-11 17:00:08+00:00 有效期至: 2075-06-29 17:00:08+00:00 发行人: C=chengdu, ST=chengdu, L=chengdu, O=mu1752253208693, OU=go1752253208693, CN=dvyv 序列号: 0x22d8bad1 哈希算法: sha1 md5值: cdfc6a78cb6a99947ed159a252bcad80 sha1值: 781901d77bdfad7c691fcac4cb4e496b1a5c10b1 sha256值: 2b8b5d496a9abf4997e2f43881703b894610e068b5e342e215fa3b2ce399b0c0 sha512值: c563dc222a120411d26d9361d2c51c0d0e01c1c690b1677bcf1866e0a3d4986e5843e0c4e259fd6ec29c5a6022cecc086c1d622c14afd7cced21bcea4920fe2d 公钥算法: rsa 密钥长度: 1024 指纹: bd12c8f8e9925f79d7448404f8dbb30d5b52603f9e824d648c9701b85a09ac3a**

## **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.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.MANAGE\_EXTERNAL\_STORAGE | 危险 | 允许应用程序广泛访问范围存储中的外部存储 | 允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用 |
| android.permission.WRITE\_EXTERNAL\_STORAGE  | 未知 | Unknown permission | Unknown permission from android reference |
| 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\_MEDIA\_IMAGES | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_VIDEO | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_AUDIO | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.ACCESS\_WIFI\_STATE | 正常 | 查看Wi-Fi状态 | 允许应用程序查看有关 Wi-Fi 状态的信息 |
| android.permission.REQUEST\_INSTALL\_PACKAGES | 危险 | 允许应用程序请求安装包。 | 恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。 |
| 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.CALL\_PHONE | 危险 | 直接拨打电话号码 | 允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码 |
| android.permission.ACCESS\_COARSE\_LOCATION | 危险 | 粗定位 | 访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置 |
| 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.CHANGE\_WIFI\_STATE | 正常 | 更改Wi-Fi状态 | 允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改 |
| android.permission.WRITE\_EXTERNAL\_STORAGE | 危险 | 读取/修改/删除外部存储内容 | 允许应用程序写入外部存储 |
| android.permission.ACCESS\_LOCATION\_EXTRA\_COMMANDS | 正常 | 访问额外的位置提供程序命令 | 访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.ACCESS\_BACKGROUND\_LOCATION | 危险 | 后台访问位置 | 允许应用程序在后台访问位置 |
| com.eg.android.csipayGphone.igum.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |

## **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。**