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

**秀色约会私密间（ 0.2.79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 | 秀色约会私密间 |
| 版本 | 0.2.79 |
| 包名 | com.QF8Oc3nYOv7X.org |
| 域名线索 | 32条 |
| URL线索 | 56条 |
| APP图标 |  |
| 分析日期 | 2025年7月4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 | 26232714fkqx.apk |
| 文件大小 | 36.54MB |
| MD5值 | af18bab3beaa14185f09a15b9cdc4cac |
| SHA1值 | f6412c58ca2823b12e538ef9735b82713e9bbc1d |
| SHA256值 | c82b2fcca6394b345fb41d991f9c3270599d7529a9c5a20bc134f2eef1272784 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 秀色约会私密间 |
| 包名 | com.QF8Oc3nYOv7X.org |
| 主活动Activity | com.uzmap.pkg.LauncherUI |
| 安卓版本名称 | 0.2.79 |
| 安卓版本 | 279 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| tsapi.amap.com | IP: 106.11.43.116  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| abroad.apilocate.amap.com | IP: 59.82.34.246  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| restsdk.amap.com | IP: 106.11.43.113  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| www.ccil.org | IP: 142.251.43.19  所属国家: United States of America  地区: California  城市: Mountain View |
| apilocate.amap.com | IP: 59.82.60.15  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| www.winimage.com | IP: 198.50.170.91  所属国家: Canada  地区: Quebec  城市: Beauharnois |
| s.apicloud.com | 没有服务器地理信息. |
| nls-wave.aliyuncs.com | IP: 106.15.18.6  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| lbs.amap.com | IP: 59.82.60.56  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| a.app3c.cn | IP: 47.93.90.46  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| dualstack.apilocate.amap.com | IP: 106.11.40.50  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| dualstack-a.apilocate.amap.com | IP: 106.11.40.50  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| adiu.amap.com | IP: 59.82.60.56  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| r.app3c.cn | IP: 47.93.90.46  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| m5.amap.com | IP: 106.11.35.98  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| yuntuapi.amap.com | 没有服务器地理信息. |
| wb.amap.com | IP: 59.82.60.45  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| lame.sf.net | IP: 204.68.111.100  所属国家: United States of America  地区: California  城市: San Diego |
| wprd0d.is.autonavi.com | 没有服务器地理信息. |
| dualstack-arestapi.amap.com | IP: 39.98.22.142  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| maps.testing.amap.com | IP: 140.205.69.9  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| apiinit.amap.com | IP: 203.119.175.194  所属国家: China  地区: Beijing  城市: Beijing |
| schemas.android.com | 没有服务器地理信息. |
| as.apicloud.com | 没有服务器地理信息. |
| wap.amap.com | IP: 150.138.203.248  所属国家: China  地区: Shandong  城市: Jinan |
| cgicol.amap.com | IP: 59.82.31.99  所属国家: China  地区: Beijing  城市: Beijing |
| nls-log-gather.aliyuncs.com | IP: 203.119.207.129  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| schemas.alibaba-inc.com | 没有服务器地理信息. |
| d.app3c.cn | IP: 47.93.90.46  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| mst01.is.autonavi.com | IP: 106.11.15.2  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| p.app3c.cn | IP: 47.93.154.30  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| mpsapi.amap.com | IP: 203.119.169.143  所属国家: China  地区: Beijing  城市: Beijing |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://www.ccil.org/~cowan/tagsoup/properties/schema | com/deepe/c/h/l.java |
| http://mpsapi.amap.com/ | com/autonavi/base/ae/gmap/GLMapEngine.java |
| http://m5.amap.com/ | com/autonavi/base/ae/gmap/GLMapEngine.java |
| http://restsdk.amap.com/rest/lbs/dem/dataservice?z=%d&x=%d&y=%d&type=2 | com/autonavi/base/ae/gmap/TerrainOverlayProvider.java |
| http://mst01.is.autonavi.com/appmaptile?z=%d&x=%d&y=%d&lang=zh\_cn&size=1&scale=1&style=6 | com/autonavi/base/ae/gmap/TerrainOverlayProvider.java |
| http://m5.amap.com/ | com/autonavi/base/amap/mapcore/maploader/AMapLoader.java |
| http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/查看错误码说明 | com/autonavi/amap/mapcore/Inner\_3dMap\_location.java |
| http://dualstack-arestapi.amap.com/v3/geocode/regeo | com/autonavi/aps/amapapi/trans/c.java |
| http://restsdk.amap.com/v3/geocode/regeo | com/autonavi/aps/amapapi/trans/c.java |
| http://abroad.apilocate.amap.com/mobile/binary | com/autonavi/aps/amapapi/trans/a.java |
| http://apilocate.amap.com/mobile/binary | com/autonavi/aps/amapapi/utils/b.java |
| http://dualstack-a.apilocate.amap.com/mobile/binary | com/autonavi/aps/amapapi/utils/b.java |
| http://abroad.apilocate.amap.com/mobile/binary | com/autonavi/aps/amapapi/utils/b.java |
| http://abroad.apilocate.amap.com/mobile/binary | com/autonavi/aps/amapapi/utils/g.java |
| http://schemas.android.com/apk/res/android | com/apicloud/third/gif/GifTextureView.java |
| http://schemas.android.com/apk/res/android | com/apicloud/third/gif/GifTextView.java |
| http://schemas.android.com/apk/res/android | com/apicloud/third/gif/GifViewUtils.java |
| http://apiinit.amap.com/v3/log/init | com/amap/api/col/p0003nsl/ld.java |
| https://restsdk.amap.com/sdk/compliance/params | com/amap/api/col/p0003nsl/mm.java |
| http://restsdk.amap.com/sdk/compliance/params | com/amap/api/col/p0003nsl/mm.java |
| https://adiu.amap.com/ws/device/adius | com/amap/api/col/p0003nsl/ni.java |
| http://restsdk.amap.com/v4/grasproad/driving? | com/amap/api/col/p0003nsl/kw.java |
| https://restsdk.amap.com/v3/iasdkauth | com/amap/api/col/p0003nsl/lc.java |
| https://dualstack-arestapi.amap.com/v3/iasdkauth | com/amap/api/col/p0003nsl/lc.java |
| http://mpsapi.amap.com/ws/mps/lyrdata/ugc/ | com/amap/api/col/p0003nsl/k.java |
| http://restsdk.amap.com/v4 | com/amap/api/col/p0003nsl/co.java |
| http://wprd0%d.is.autonavi.com/appmaptile? | com/amap/api/col/p0003nsl/db.java |
| http://restsdk.amap.com/v4/gridmap? | com/amap/api/col/p0003nsl/db.java |
| http://restsdk.amap.com/v3/batch?key= | com/amap/api/col/p0003nsl/fn.java |
| http://wb.amap.com/?r=%f,%f,%s,%f,%f,%s,%d,%d,%d,%s,%s,%s&sourceapplication=openapi/0 | com/amap/api/col/p0003nsl/kq.java |
| http://wb.amap.com/?q=%f,%f,%s&sourceapplication=openapi/0 | com/amap/api/col/p0003nsl/kq.java |
| http://wb.amap.com/?n=%f,%f,%f,%f,%d&sourceapplication=openapi/0 | com/amap/api/col/p0003nsl/kq.java |
| http://wb.amap.com/?p=%s,%f,%f,%s,%s&sourceapplication=openapi/0 | com/amap/api/col/p0003nsl/kq.java |
| http://apilocate.amap.com/mobile/binary | com/amap/api/col/p0003nsl/rc.java |
| http://dualstack.apilocate.amap.com/mobile/binary | com/amap/api/col/p0003nsl/rc.java |
| http://restsdk.amap.com/v4 | com/amap/api/col/p0003nsl/r.java |
| http://restsdk.amap.com | com/amap/api/col/p0003nsl/lm.java |
| http://restsdk.amap.com/v4/gridmap? | com/amap/api/col/p0003nsl/dc.java |
| http://restsdk.amap.com/v3 | com/amap/api/col/p0003nsl/is.java |
| https://restsdk.amap.com/v3 | com/amap/api/col/p0003nsl/is.java |
| http://restsdk.amap.com/v4 | com/amap/api/col/p0003nsl/is.java |
| https://restsdk.amap.com/v4 | com/amap/api/col/p0003nsl/is.java |
| http://yuntuapi.amap.com | com/amap/api/col/p0003nsl/is.java |
| https://yuntuapi.amap.com | com/amap/api/col/p0003nsl/is.java |
| http://restsdk.amap.com/rest/me/cpoint | com/amap/api/col/p0003nsl/is.java |
| https://restsdk.amap.com/rest/me/cpoint | com/amap/api/col/p0003nsl/is.java |
| http://m5.amap.com/ws/mapapi/shortaddress/transform | com/amap/api/col/p0003nsl/is.java |
| https://m5.amap.com/ws/mapapi/shortaddress/transform | com/amap/api/col/p0003nsl/is.java |
| http://restsdk.amap.com/v3/assistant/inputtips? | com/amap/api/col/p0003nsl/fm.java |
| http://cgicol.amap.com/collection/collectData?src=baseCol&ver=v74& | com/amap/api/col/p0003nsl/pd.java |
| http://restsdk.amap.com/v3/place/text? | com/amap/api/col/p0003nsl/a.java |
| http://restsdk.amap.com/v3/place/around? | com/amap/api/col/p0003nsl/a.java |
| http://restsdk.amap.com/v3/config/district? | com/amap/api/col/p0003nsl/a.java |
| http://restsdk.amap.com | com/amap/api/col/p0003nsl/hd.java |
| http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/查看错误码说明 | com/amap/api/location/AMapLocation.java |
| http://restsdk.amap.com/v4/stats/alitts | com/amap/api/navi/core/network/h.java |
| http://wap.amap.com/ | com/amap/api/maps/AMapUtils.java |
| https://a.app3c.cn | compile/Properties.java |
| https://d.app3c.cn | compile/Properties.java |
| https://s.apicloud.com | compile/Properties.java |
| https://p.app3c.cn | compile/Properties.java |
| https://r.app3c.cn | compile/Properties.java |
| https://as.apicloud.com | compile/Properties.java |
| http://m5.amap.com/ws/shield/elevated/downloadData | lib/arm64-v8a/libAMapSDK\_NAVI\_v8\_1\_0.so |
| http://m5.amap.com/ws/shield/rdr/log/upload | lib/arm64-v8a/libAMapSDK\_NAVI\_v8\_1\_0.so |
| http://m5.amap.com/ws/shield/mainsideroad/downloadData | lib/arm64-v8a/libAMapSDK\_NAVI\_v8\_1\_0.so |
| http://maps.testing.amap.com/ws/shield/motor-route/etatrafficupdate | lib/arm64-v8a/libAMapSDK\_NAVI\_v8\_1\_0.so |
| http://maps.testing.amap.com/ws/shield/motor-route/cross | lib/arm64-v8a/libAMapSDK\_NAVI\_v8\_1\_0.so |
| http://maps.testing.amap.com/ws/shield/navigation/motor\_traffic\_report | lib/arm64-v8a/libAMapSDK\_NAVI\_v8\_1\_0.so |
| http://maps.testing.amap.com/ws/shield/navigation/motor\_off\_route\_report | lib/arm64-v8a/libAMapSDK\_NAVI\_v8\_1\_0.so |
| http://maps.testing.amap.com/ws/shield/open\_di/jiache\_deepinfo/ | lib/arm64-v8a/libAMapSDK\_NAVI\_v8\_1\_0.so |
| http://m5.amap.com | lib/arm64-v8a/libAMapSDK\_NAVI\_v8\_1\_0.so |
| http://restsdk.amap.com/rest/lbs | lib/arm64-v8a/libAMapSDK\_NAVI\_v8\_1\_0.so |
| http://restsdk.amap.com/v4 | lib/arm64-v8a/libAMapSDK\_NAVI\_v8\_1\_0.so |
| http://tsapi.amap.com/v1 | lib/arm64-v8a/libAMapSDK\_NAVI\_v8\_1\_0.so |
| http://restsdk.amap.com/v3 | lib/arm64-v8a/libAMapSDK\_NAVI\_v8\_1\_0.so |
| http://restsdk.amap.com/opennavi | lib/arm64-v8a/libAMapSDK\_NAVI\_v8\_1\_0.so |
| http://mpsapi.amap.com/ws/mps/vmap | lib/arm64-v8a/libAMapSDK\_NAVI\_v8\_1\_0.so |
| http://mpsapi.amap.com/ws/mps/rtt | lib/arm64-v8a/libAMapSDK\_NAVI\_v8\_1\_0.so |
| http://mpsapi.amap.com/ws/mps/smap | lib/arm64-v8a/libAMapSDK\_NAVI\_v8\_1\_0.so |
| http://m5.amap.com/ws/transfer/auth/map/indoor\_maps | lib/arm64-v8a/libAMapSDK\_NAVI\_v8\_1\_0.so |
| http://mpsapi.amap.com/ws/mps/lyrdata/ugc/ | lib/arm64-v8a/libAMapSDK\_NAVI\_v8\_1\_0.so |
| http://mpsapi.amap.com/ | lib/arm64-v8a/libAMapSDK\_NAVI\_v8\_1\_0.so |
| https://nls-wave.aliyuncs.com/api/gather | lib/arm64-v8a/libneonui\_shared.so |
| https://nls-log-gather.aliyuncs.com/api/gather | lib/arm64-v8a/libneonui\_shared.so |
| http://www.winimage.com/zLibDll | lib/arm64-v8a/libneonui\_shared.so |
| http://schemas.alibaba-inc.com/tts | lib/arm64-v8a/libneonui\_shared.so |
| http://lame.sf.net | lib/arm64-v8a/libneonui\_shared.so |
| http://m5.amap.com/ws/shield/elevated/downloadData | lib/armeabi/libAMapSDK\_NAVI\_v8\_1\_0.so |
| http://m5.amap.com/ws/shield/rdr/log/upload | lib/armeabi/libAMapSDK\_NAVI\_v8\_1\_0.so |
| http://m5.amap.com/ws/shield/mainsideroad/downloadData | lib/armeabi/libAMapSDK\_NAVI\_v8\_1\_0.so |
| http://maps.testing.amap.com/ws/shield/motor-route/etatrafficupdate | lib/armeabi/libAMapSDK\_NAVI\_v8\_1\_0.so |
| http://maps.testing.amap.com/ws/shield/motor-route/cross | lib/armeabi/libAMapSDK\_NAVI\_v8\_1\_0.so |
| http://maps.testing.amap.com/ws/shield/navigation/motor\_traffic\_report | lib/armeabi/libAMapSDK\_NAVI\_v8\_1\_0.so |
| http://maps.testing.amap.com/ws/shield/navigation/motor\_off\_route\_report | lib/armeabi/libAMapSDK\_NAVI\_v8\_1\_0.so |
| http://maps.testing.amap.com/ws/shield/open\_di/jiache\_deepinfo/ | lib/armeabi/libAMapSDK\_NAVI\_v8\_1\_0.so |
| http://m5.amap.com | lib/armeabi/libAMapSDK\_NAVI\_v8\_1\_0.so |
| http://restsdk.amap.com/rest/lbs | lib/armeabi/libAMapSDK\_NAVI\_v8\_1\_0.so |
| http://restsdk.amap.com/v4 | lib/armeabi/libAMapSDK\_NAVI\_v8\_1\_0.so |
| http://tsapi.amap.com/v1 | lib/armeabi/libAMapSDK\_NAVI\_v8\_1\_0.so |
| http://restsdk.amap.com/v3 | lib/armeabi/libAMapSDK\_NAVI\_v8\_1\_0.so |
| http://restsdk.amap.com/opennavi | lib/armeabi/libAMapSDK\_NAVI\_v8\_1\_0.so |
| http://mpsapi.amap.com/ws/mps/vmap | lib/armeabi/libAMapSDK\_NAVI\_v8\_1\_0.so |
| http://mpsapi.amap.com/ws/mps/rtt | lib/armeabi/libAMapSDK\_NAVI\_v8\_1\_0.so |
| http://mpsapi.amap.com/ws/mps/smap | lib/armeabi/libAMapSDK\_NAVI\_v8\_1\_0.so |
| http://m5.amap.com/ws/transfer/auth/map/indoor\_maps | lib/armeabi/libAMapSDK\_NAVI\_v8\_1\_0.so |
| http://mpsapi.amap.com/ws/mps/lyrdata/ugc/ | lib/armeabi/libAMapSDK\_NAVI\_v8\_1\_0.so |
| http://mpsapi.amap.com/ | lib/armeabi/libAMapSDK\_NAVI\_v8\_1\_0.so |
| https://nls-wave.aliyuncs.com/api/gather | lib/armeabi/libneonui\_shared.so |
| https://nls-log-gather.aliyuncs.com/api/gather | lib/armeabi/libneonui\_shared.so |
| http://schemas.alibaba-inc.com/tts | lib/armeabi/libneonui\_shared.so |
| http://lame.sf.net | lib/armeabi/libneonui\_shared.so |
| http://www.winimage.com/zLibDll | lib/armeabi/libneonui\_shared.so |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| developer@apicloud.com | com/uzmap/pkg/uzcore/b/d.java |

### **4.4 手机号线索**

## **5. 签名证书**

**APK is signed v1 signature: True v2 signature: True v3 signature: False Found 1 unique certificates Subject: C=(zh), ST=(Beijing), L=(Beijing), O=(abc808@w.com), OU=(QF8Oc3nYOv7X), CN=(QF8Oc3nYOv7X) Signature Algorithm: rsassa\_pkcs1v15 Valid From: 2022-06-26 15:15:41+00:00 Valid To: 2122-06-02 15:15:41+00:00 Issuer: C=(zh), ST=(Beijing), L=(Beijing), O=(abc808@w.com), OU=(QF8Oc3nYOv7X), CN=(QF8Oc3nYOv7X) Serial Number: 0x17dbabcd Hash Algorithm: sha256 md5: 3546437296a85e09877aa74a9758f850 sha1: 444a67c2e6daf39f2dfc6541cbc42e3c3ec67374 sha256: 8154998036931a111f39e7bcf6df74661a12ed690c6ecec775f2d993838f1b2a sha512: aa17653d62e9bcffea8c4c260340fbd2a6d2757d86e5df8dda7f250b86ca5a508a9a5068bbe2d5cb8751a154fb1df046d147b9d23355e569331be08b7d52193f PublicKey Algorithm: rsa Bit Size: 1024 Fingerprint: 778904a5e9b55faaefff8becd7dff3d0e2107889f9702d2d8fd35b2e9239e161**

## **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 |
| com.huawei.android.launcher.permission.CHANGE\_BADGE | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章。 |
| 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\_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.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\_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.WAKE\_LOCK | 正常 | 防止手机睡眠 | 允许应用程序防止手机进入睡眠状态 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.SEND\_SMS | 危险 | 发送短信 | 允许应用程序发送 SMS 消息。恶意应用程序可能会在未经您确认的情况下发送消息,从而使您付出代价 |
| 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.WRITE\_CONTACTS | 危险 | 写入联系人数据 | 允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可以使用它来删除或修改您的联系人数据 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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.MOUNT\_UNMOUNT\_FILESYSTEMS | 危险 | 装载和卸载文件系统 | 允许应用程序为可移动存储安装和卸载文件系统 |
| 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\_SETTINGS | 危险 | 修改全局系统设置 | 允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。 |
| 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 |

## **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。**