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

**紫荆花（ 1.0.0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 | 紫荆花 |
| 版本 | 1.0.0 |
| 包名 | com.zhonglian.zlgame |
| 域名线索 | 9条 |
| URL线索 | 9条 |
| APP图标 |  |
| 分析日期 | 2025年2月6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 | zjh.apk |
| 文件大小 | 223.52MB |
| MD5值 | c2254b6bd1e7a3f4ba74537cff122609 |
| SHA1值 | 626a3f3f8090ca08648bd8eefdf99f83ef7591ff |
| SHA256值 | 17fe94cdb716daea528cf5bb4f8f1de704c36bb34deb2369eaa55e98b5cb6191 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 紫荆花 |
| 包名 | com.zhonglian.zlgame |
| 主活动Activity | com.zhonglian.zlgame.wxapi.WXEntryActivity |
| 安卓版本名称 | 1.0.0 |
| 安卓版本 | 100 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| rqd.uu.qq.com | IP: 60.28.219.32 所属国家: China 地区: Tianjin 城市: Tianjin  |
| android.bugly.qq.com | IP: 124.95.225.169 所属国家: China 地区: Liaoning 城市: Shenyang  |
| example.com | IP: 96.7.128.198 所属国家: United States of America 地区: California 城市: El Segundo  |
| itsdata.map.baidu.com | IP: 111.206.209.180 所属国家: China 地区: Beijing 城市: Beijing  |
| ofloc.map.baidu.com | IP: 111.206.209.193 所属国家: China 地区: Beijing 城市: Beijing  |
| api.map.baidu.com | IP: 111.206.208.72 所属国家: China 地区: Beijing 城市: Beijing  |
| daup.map.baidu.com | IP: 110.242.69.98 所属国家: China 地区: Hebei 城市: Baoding  |
| loc.map.baidu.com | IP: 111.206.209.174 所属国家: China 地区: Beijing 城市: Beijing  |
| bbs.lbsyun.baidu.com | 没有服务器地理信息.  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://loc.map.baidu.com/cfgs/loc/commcfgs  | com/baidu/location/b/a.java  |
| https://ofloc.map.baidu.com/locnu  | com/baidu/location/b/q.java  |
| https://loc.map.baidu.com/cc.php  | com/baidu/location/b/e.java  |
| https://itsdata.map.baidu.com/long-conn-gps/sdk.php  | com/baidu/location/b/e.java  |
| http://loc.map.baidu.com/sdk.php  | com/baidu/location/e/g.java  |
| http://loc.map.baidu.com/user\_err.php  | com/baidu/location/e/g.java  |
| http://loc.map.baidu.com/oqur.php  | com/baidu/location/e/g.java  |
| https://loc.map.baidu.com/tcu.php  | com/baidu/location/e/g.java  |
| http://loc.map.baidu.com/rtbu.php  | com/baidu/location/e/g.java  |
| http://loc.map.baidu.com/iofd.php  | com/baidu/location/e/g.java  |
| http://loc.map.baidu.com/wloc  | com/baidu/location/e/g.java  |
| https://loc.map.baidu.com/sdk\_ep.php  | com/baidu/location/e/g.java  |
| https://loc.map.baidu.com/sdk.php  | com/baidu/location/e/g.java  |
| https://daup.map.baidu.com/cltr/rcvr  | com/baidu/location/e/g.java  |
| https://api.map.baidu.com/sdkcs/verify  | com/baidu/lbsapi/auth/LBSAuthManager.java  |
| http://bbs.lbsyun.baidu.com/forum.php?mod=viewthread&tid=106461\n=============================================\n  | com/baidu/mapsdkplatform/comapi/util/PermissionCheck.java  |
| https://api.map.baidu.com/lbs\_sdkcc/report  | com/baidu/mapsdkplatform/comapi/c/a/b.java  |
| http://android.bugly.qq.com/rqd/async  | com/tencent/bugly/crashreport/common/strategy/StrategyBean.java  |
| http://rqd.uu.qq.com/rqd/sync  | com/tencent/bugly/crashreport/common/strategy/StrategyBean.java  |
| http://example.com/  | cz/msebera/android/httpclient/impl/client/cache/CacheKeyGenerator.java  |

### **4.3 邮箱线索**

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 18345352118  | com/baidu/mapsdkplatform/comapi/util/b.java  |

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: C=yy, ST=tt, L=rr, O=ee, OU=ww, CN=qq 签名算法: rsassa\_pkcs1v15 有效期自: 2024-04-09 09:55:16+00:00 有效期至: 2049-04-03 09:55:16+00:00 发行人: C=yy, ST=tt, L=rr, O=ee, OU=ww, CN=qq 序列号: 0x3f86e7de 哈希算法: sha256 md5值: e30c04dd9151a43fcc10430f2310c598 sha1值: ced23322d5b7753e3ea6c12ad7cc134c0883392c sha256值: 9fd82de771e0711d8a39327caeb057d74df00e6f6e14d91eb9a86be373583781 sha512值: 78f8499b00e1815b1b38db0debda6ce82262c902cd81fb9bea1d48326af717e868328d63912145aab93760c02e76c5217bd3c56eef2fbbe8680779dd0ebed10b 公钥算法: rsa 密钥长度: 2048 指纹: 0b15db2995363a1e832a75a573b4fdba4389007a05b76b62c0d3d15d9afb1cb1**

## **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.LOCAL\_MAC\_ADDRESS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_PRIVILEGED\_PHONE\_STATE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.READ\_LOGS | 危险 | 读取敏感日志数据 | 允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息 |
| 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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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\_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.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.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.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.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.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.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\_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.WRITE\_SMS | 危险 | 编辑短信或彩信 | 允许应用程序写入存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会删除您的消息 |
| android.permission.RECEIVE\_SMS | 危险 | 接收短信 | 允许应用程序接收和处理 SMS 消息。恶意应用程序可能会监视您的消息或将其删除而不向您显示 |
| android.permission.BLUETOOTH | 正常 | 创建蓝牙连接 | 允许应用程序连接到配对的蓝牙设备 |
| android.permission.BLUETOOTH\_ADMIN | 正常 | 蓝牙管理 | 允许应用程序发现和配对蓝牙设备。  |
| 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.DOWNLOAD\_WITHOUT\_NOTIFICATION | 未知 | Unknown permission | Unknown permission from android reference |
| net.edaibu.easywalking.permission.JPUSH\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.USE\_CREDENTIALS | 危险 | 使用帐户的身份验证凭据 | 允许应用程序请求身份验证令牌 |
| android.permission.MANAGE\_ACCOUNTS | 危险 | 管理帐户列表 | 允许应用程序执行添加和删除帐户以及删除其密码等操作 |
| android.permission.AUTHENTICATE\_ACCOUNTS | 危险 | 充当帐户验证器 | 允许应用程序使用帐户管理器的帐户验证器功能,包括创建帐户以及获取和设置其密码 |
| com.android.launcher.permission.READ\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BAIDU\_LOCATION\_SERVICE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ACCES\_MOCK\_LOCATION | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ACCESS\_GPS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BROADCAST\_STICKY | 正常 | 发送粘性广播 | 允许应用程序发送粘性广播,在广播结束后保留。恶意应用程序会导致手机使用过多内存,从而使手机运行缓慢或不稳定 |
| 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.CAMERA | 危险 | 拍照和录像 | 允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像 |
| 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.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.CHANGE\_NETWORK\_STATE | 正常 | 更改网络连接 | 允许应用程序更改网络连接状态。 |
| 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.RECEIVE\_BOOT\_COMPLETED | 正常 | 开机时自动启动 | 允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度 |
| android.permission.BROADCAST\_PACKAGE\_ADDED | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BROADCAST\_PACKAGE\_CHANGED | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BROADCAST\_PACKAGE\_INSTALL | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BROADCAST\_PACKAGE\_REPLACED | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| 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 |

## **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。**