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

**白娘子（ 1.0.0.0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 | 白娘子 |
| 版本 | 1.0.0.0 |
| 包名 | com.bnzcq.sysdk |
| 域名线索 | 21条 |
| URL线索 | 22条 |
| APP图标 |  |
| 分析日期 | 2025年6月30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 | bainiangzi1.1\_2265.com.apk |
| 文件大小 | 298.08MB |
| MD5值 | e60810bc02c57c69ec552bad22a9b511 |
| SHA1值 | b27aaf5681f1abd27ddc108050ae5ce5d4791913 |
| SHA256值 | 9aa57c4b39b359c3c6591b25ff71203554177064a667d03e6c43c263a1eaaddc |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 白娘子 |
| 包名 | com.bnzcq.sysdk |
| 主活动Activity | com.cilugame.h1.UnityPlayerActivity |
| 安卓版本名称 | 1.0.0.0 |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| weixin.qq.com | IP: 182.50.12.167 所属国家: China 地区: Beijing 城市: Beijing  |
| d.alipay.com | IP: 123.125.216.242 所属国家: China 地区: Beijing 城市: Beijing  |
| dev.sdk.cilugame.com | IP: 183.6.21.133 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| dev.185sy.com | IP: 81.68.185.27 所属国家: China 地区: Beijing 城市: Beijing  |
| apilocate.amap.com | IP: 106.11.43.81 所属国家: China 地区: Beijing 城市: Beijing  |
| www.sy527.com | IP: 154.92.62.28 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| restapi.amap.com | IP: 106.11.43.113 所属国家: China 地区: Beijing 城市: Beijing  |
| p.185sy.com | IP: 118.89.186.125 所属国家: China 地区: Beijing 城市: Beijing  |
| www.qq.com | IP: 221.198.70.47 所属国家: China 地区: Tianjin 城市: Tianjin  |
| 182.254.116.117 | IP: 182.254.116.117 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| www.baidu.com | IP: 110.242.68.3 所属国家: China 地区: Hebei 城市: Baoding  |
| api.uca.cloud.unity3d.com | IP: 43.156.88.56 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| pingma.qq.com | IP: 116.147.19.64 所属国家: China 地区: Beijing 城市: Beijing  |
| cgicol.amap.com | IP: 123.125.216.212 所属国家: China 地区: Beijing 城市: Beijing  |
| apilocatesrc.amap.com | IP: 106.11.43.81 所属国家: China 地区: Beijing 城市: Beijing  |
| config.uca.cloud.unity3d.com | IP: 34.111.113.40 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| log.reyun.com | IP: 52.80.199.120 所属国家: China 地区: Beijing 城市: Beijing  |
| abroad.apilocate.amap.com | IP: 59.82.44.11 所属国家: China 地区: Shanghai 城市: Shanghai  |
| api.185sy.com | IP: 81.68.185.27 所属国家: China 地区: Beijing 城市: Beijing  |
| stats.unity3d.com | 没有服务器地理信息.  |
| lbs.amap.com | IP: 59.82.31.203 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://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/  | com/amap/api/location/AMapLocation.java  |
| https://dev.sdk.cilugame.com/v1/sdkc/pay/orderid.json  | com/cilugame/h1/CLSDKPlugin.java  |
| http://restapi.amap.com/v3/place/around?  | com/loc/a.java  |
| http://restapi.amap.com/v3/place/text?  | com/loc/a.java  |
| http://restapi.amap.com/v3/config/district?  | com/loc/a.java  |
| http://apilocate.amap.com/mobile/binary  | com/loc/cs.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | com/loc/cs.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | com/loc/cl.java  |
| http://apilocatesrc.amap.com/mobile/binary  | com/loc/cl.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | com/loc/cx.java  |
| http://cgicol.amap.com/collection/writedata?ver=v1.0\_ali&  | com/loc/ce.java  |
| https://restapi.amap.com/v3/iasdkauth  | com/loc/l.java  |
| http://restapi.amap.com/v3/iasdkauth  | com/loc/l.java  |
| http://restapi.amap.com  | com/loc/q.java  |
| http://restapi.amap.com/v3/geocode/regeo  | com/loc/bu.java  |
| http://log.reyun.com/  | com/reyun/common/ReYunConst.java  |
| http://log.reyun.com/receive/rest/heartbeat  | com/reyun/sdk/ReYunGame.java  |
| http://log.reyun.com/receive/pkginfo  | com/reyun/utils/HttpNetworkUtil.java  |
| http://log.reyun.com/receive/tkio/  | com/reyun/utils/HttpNetworkUtil.java  |
| http://log.reyun.com/receive/rest/  | com/reyun/utils/HttpNetworkUtil.java  |
| http://log.reyun.com/receive/track/  | com/reyun/utils/HttpNetworkUtil.java  |
| http://dev.185sy.com  | com/ssy185/sdk/SDKManager.java  |
| http://www.sy527.com  | com/sy/sdk/model/HttpUrls.java  |
| http://api.185sy.com/  | com/sy/sdk/model/HttpUrls.java  |
| http://p.185sy.com/index.php?g=api&m=FreeSub&a=get\_c  | com/sy/sdk/model/HttpUrls.java  |
| http://api.185sy.com/index.php?g=api&m=index&a=map  | com/sy/sdk/model/HttpUrls.java  |
| http://api.185sy.com/index.php?g=api&m=user&a=upload\_log  | com/sy/sdk/resloader/ReadConfig.java  |
| https://d.alipay.com  | com/sy/sdk/ui/dialog/PayDialog.java  |
| https://weixin.qq.com  | com/sy/sdk/ui/dialog/PayDialog.java  |
| http://182.254.116.117/d?dn=99e2d153e4d0527186ebed5ac5608367&id=6&ttl=1  | com/tencent/android/tpush/service/b/b.java  |
| http://www.baidu.com  | com/tencent/android/tpush/service/channel/i.java  |
| http://www.qq.com  | com/tencent/android/tpush/service/channel/i.java  |
| http://pingma.qq.com:80/mstat/report  | com/tencent/android/tpush/stat/c.java  |
| http://rp  | com/xsj/crasheye/util/Utils.java  |
| https://stats.unity3d.com/HWStatsUpdate.cgi  | lib/armeabi-v7a/libunity.so  |
| https://stats.unity3d.com/HWStats.cgi  | lib/armeabi-v7a/libunity.so  |
| https://config.uca.cloud.unity3d.com  | lib/armeabi-v7a/libunity.so  |
| https://api.uca.cloud.unity3d.com/v1/events  | lib/armeabi-v7a/libunity.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| ctwap@mycdma.cn  | com/tencent/mid/a/a.java  |

### **4.4 手机号线索**

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: False v3 签名: False 找到 1 个唯一证书 主题: C=china, ST=sichuan, L=chengdu, O=jiangxihuyu, OU=rc, CN=lz 签名算法: rsassa\_pkcs1v15 有效期自: 2017-10-17 02:34:43+00:00 有效期至: 2027-10-15 02:34:43+00:00 发行人: C=china, ST=sichuan, L=chengdu, O=jiangxihuyu, OU=rc, CN=lz 序列号: 0x2c69f187 哈希算法: sha256 md5值: 1985aba51314baca016662533522ed3c sha1值: 2261b8176af6219d418c8f03dbb381cd00da67df sha256值: 2f13e3076a26ef0ae2d21fe98c4a1b61ea281054a06be23d53c6e7ab077843b4 sha512值: aa8e01066899be3deb97fb7bd6e34e0aed504a8df23c92b0a8b4b70ab7ce28abd67fbadd8e6eaabd718ced47c78752fbf8cdbd57b504c04ba83b2c66a2712bf1**

## **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.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.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.BATTERY\_STATS | 合法 | 修改电池统计信息 | 允许修改收集的电池统计信息。不供普通应用程序使用 |
| android.permission.WRITE\_MEDIA\_STORAGE | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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\_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.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.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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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.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.GET\_TASKS | 危险 | 检索正在运行的应用程序 | 允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息 |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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\_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.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.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.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\_USER\_PRESENT | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.RESTART\_PACKAGES | 正常 | 杀死后台进程 | 允许应用程序杀死其他应用程序的后台进程,即使内存不低 |
| 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.KILL\_BACKGROUND\_PROCESSES | 正常 | 杀死后台进程 | 允许应用程序杀死其他应用程序的后台进程,即使内存不低 |
| 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.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.CHANGE\_CONFIGURATION | 系统需要 | 更改您的 UI 设置 | 允许应用程序更改当前配置,例如语言环境或整体字体大小 |

## **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。**