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

**王牌影院（ 1.2.2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 | 王牌影院 |
| 版本 | 1.2.2 |
| 包名 | com.wc.wangpai |
| 域名线索 | 3条 |
| URL线索 | 1条 |
| APP图标 |  |
| 分析日期 | 2025年2月8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 | wpyy1.2.2.apk |
| 文件大小 | 32.59MB |
| MD5值 | 929ca1ccc498dd09be3ea695c0afac25 |
| SHA1值 | 8f7f763da4d0729e3a532f617422b0767666e787 |
| SHA256值 | c142483dda6eb6fd6a7c4583aab00a389c074376b5cd83da0d308c46fb4933b1 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 王牌影院 |
| 包名 | com.wc.wangpai |
| 主活动Activity | com.wc.wangpai.SplashActivity |
| 安卓版本名称 | 1.2.2 |
| 安卓版本 | 13 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| p6-ad-sign.byteimg.com | IP: 42.81.247.46 所属国家: China 地区: Tianjin 城市: Tianjin  |
| gz.adsl.cn | IP: 42.81.212.169 所属国家: China 地区: Tianjin 城市: Tianjin  |
| p9-ad-sign.byteimg.com | IP: 42.81.63.22 所属国家: China 地区: Tianjin 城市: Tianjin  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://gz.adsl.cn/gluttony/page/?adsluid=wsh8k9rts3qljvi\\u0026union\_site=\_\_UNION\_SITE\_\_\\u0026adid=1741696558327869\\u0026creativeid=1741704398922798\\u0026creativetype=15\\u0026clickid=EK7IgcCigowDGJ744KG0jNkEIJyaoJrpjbYGMAw4jLECQiIyMDIyMDgyMjE4MjUyNTAxMDEzMzAzNTE1MDEzMDg4QTZESMG4ApABAA\  | Mogua Engine V2  |
| http://p6-ad-sign.byteimg.com/web.business.image/a072248c4f0a926079831fa91c40459f  | Mogua Engine V2  |
| http://p9-ad-sign.byteimg.com/web.business.image/a072248c4f0a926079831fa91c40459f  | Mogua Engine V2  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| 邮件至tuiguangvip2021\_3@163.com 邮箱tuiguangvip2021\_3@163.com  | Mogua Engine V1  |

### **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: False 找到 1 个唯一证书 主题: C=a1, ST=a1, L=a1, O=a1, OU=a1a, CN=a1a2 签名算法: rsassa\_pkcs1v15 有效期自: 2022-03-24 01:28:22+00:00 有效期至: 2047-03-18 01:28:22+00:00 发行人: C=a1, ST=a1, L=a1, O=a1, OU=a1a, CN=a1a2 序列号: 0x296c1801 哈希算法: sha256 md5值: fc357301ce571a49be85ba20b85761ab sha1值: d1cad2ac0d2e72b5a75fe9b5b99373ed7e9d5d41 sha256值: e372611030d65f5e27fe51e97333f5d5447688d31c25f8dff0e5eacdec7361db sha512值: a45e9df5044d73510300f3b24866be19836a8d5a22515e58ad3d4b9666f94a8a47828becf475449a48601845b9ebd05b7618af4aae462292cf25bc8369557b19 公钥算法: rsa 密钥长度: 2048 指纹: a841a2282c835508a98c63ac9144b7780dbeec3b7028542e156c5750c1daf0a5**

## **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\_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.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 |
| com.wc.wangpai.openadsdk.permission.TT\_PANGOLIN | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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.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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.SYSTEM\_OVERLAY\_WINDOW | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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.REORDER\_TASKS | 正常 | 重新排序正在运行的应用程序 | 允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前 |
| 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.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.REPLACE\_EXISTING\_PACKAGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.CHANGE\_WIFI\_MULTICAST\_STATE | 正常 | 允许Wi-Fi多播接收  | 允许应用程序接收不是直接发送到您设备的数据包。这在发现附近提供的服务时很有用。它比非多播模式使用更多的功率 |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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.ACTIVITY\_RECOGNITION | 危险 | 允许应用程序识别身体活动 | 允许应用程序识别身体活动 |
| com.asus.msa.SupplementaryDID.ACCESS | 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。**