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

**硕阳爱家（ 1.2.33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 | 硕阳爱家 |
| 版本 | 1.2.33 |
| 包名 | com.shuoyang.aijia |
| 域名线索 | 26条 |
| URL线索 | 8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 | aijia.apk |
| 文件大小 | 55.52MB |
| MD5值 | 8efc9e3700bfb6c41c072c6201ac8832 |
| SHA1值 | b36340e8f2ad46d5c715dcbe4953d7c1a2158219 |
| SHA256值 | 60965348a5c2e379ee93b6338486e391ef156a34924eb12968f8ff7f7b07850b |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 硕阳爱家 |
| 包名 | com.shuoyang.aijia |
| 主活动Activity | io.dcloud.PandoraEntry |
| 安卓版本名称 | 1.2.33 |
| 安卓版本 | 1230 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| quilljs.com | IP: 172.66.40.163 所属国家: United States of America 地区: California 城市: San Francisco  |
| obj.pipi.cn | IP: 27.221.71.235 所属国家: China 地区: Shandong 城市: Jinan  |
| underscorejs.org | IP: 172.67.134.18 所属国家: United States of America 地区: California 城市: San Francisco  |
| npms.io | IP: 172.67.152.251 所属国家: United States of America 地区: California 城市: San Francisco  |
| lodash.com | IP: 13.228.199.255 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| feross.org | IP: 50.116.11.184 所属国家: United States of America 地区: California 城市: Fremont  |
| service.dcloud.net.cn | IP: 111.229.199.57 所属国家: China 地区: Beijing 城市: Beijing  |
| aijia.dexininc.com | IP: 8.134.149.162 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| api.bspapp.com | IP: 39.96.249.142 所属国家: China 地区: Beijing 城市: Beijing  |
| static.fxzb.vip | IP: 146.56.240.106 所属国家: China 地区: Beijing 城市: Beijing  |
| openjsf.org | IP: 76.76.21.21 所属国家: United States of America 地区: California 城市: Walnut  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| oss.fxzb.vip | IP: 112.80.252.187 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| gw.alicdn.com | IP: 221.194.162.248 所属国家: China 地区: Hebei 城市: Langfang  |
| ask.dcloud.net.cn | IP: 221.204.43.242 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| imgapixs.pysmei.com | 没有服务器地理信息.  |
| www.google.com | IP: 31.13.94.49 所属国家: Argentina 地区: Ciudad Autonoma de Buenos Aires 城市: Buenos Aires  |
| img10.360buyimg.com | IP: 101.75.249.219 所属国家: China 地区: Hebei 城市: Chengde  |
| files.hnxishu.cn | IP: 121.29.38.221 所属国家: China 地区: Hebei 城市: Shijiazhuang  |
| img1.baidu.com | IP: 101.72.203.35 所属国家: China 地区: Hebei 城市: Langfang  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| api.next.bspapp.com | IP: 203.107.60.33 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| vuejs.org | IP: 54.67.4.46 所属国家: United States of America 地区: California 城市: San Jose  |
| apis.map.qq.com | IP: 116.130.223.114 所属国家: China 地区: Beijing 城市: Beijing  |
| uniapp.dcloud.net.cn | IP: 116.136.170.251 所属国家: China 地区: Nei Mongol 城市: Hohhot  |
| mths.be | IP: 83.137.145.144 所属国家: Netherlands 地区: Groningen 城市: Groningen  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://ask.dcloud.net.cn/article/36199  | Mogua Engine V1  |
| https://github.com/uuidjs/uuid  | Mogua Engine V2  |
| https://apis.map.qq.com/jsapi?qt=translate&type=1&points=$  | Mogua Engine V2  |
| https://apis.map.qq.com/uri/v1/routeplan?type=drive&to=  | Mogua Engine V2  |
| https://www.google.com/maps/?daddr=  | Mogua Engine V2  |
| https://www.google.com/maps/  | Mogua Engine V2  |
| https://quilljs.com/  | Mogua Engine V2  |
| https://quilljs.com  | Mogua Engine V2  |
| https://aijia.dexininc.com  | Mogua Engine V2  |
| https://lodash.com/>  | Mogua Engine V2  |
| https://openjsf.org/>  | Mogua Engine V2  |
| https://lodash.com/license>  | Mogua Engine V2  |
| http://underscorejs.org/LICENSE>  | Mogua Engine V2  |
| https://npms.io/search?q=ponyfill.  | Mogua Engine V2  |
| https://aijia.dexininc.com/shop/api/upgrade  | Mogua Engine V2  |
| https://img1.baidu.com/it/u=1601695551,235775011&fm=26&fmt=auto  | Mogua Engine V2  |
| https://user  | Mogua Engine V2  |
| https://files.hnxishu.cn/down/aijia.apk  | Mogua Engine V2  |
| http://www.w3.org/2000/svg  | Mogua Engine V2  |
| https://obj.pipi.cn/festatic/fe-trade/public/img/today-no-show.3f026db3.png  | Mogua Engine V2  |
| http://gw.alicdn.com/imgextra/i3/O1CN01vEXvKl1f5R6Q2XsHx\_!!6000000003955-55-tps-48-48.svg  | Mogua Engine V2  |
| https://api.next.bspapp.com  | Mogua Engine V2  |
| https://api.bspapp.com  | Mogua Engine V2  |
| https://$  | Mogua Engine V2  |
| https://uniapp.dcloud.net.cn/uniCloud/secure-network.html  | Mogua Engine V2  |
| https://uniapp.dcloud.net.cn/uniCloud/faq?id=promise  | Mogua Engine V2  |
| https://files.hnxishu.cn/static/assets/white\_row.png  | Mogua Engine V2  |
| http://feross.org>  | Mogua Engine V2  |
| https://mths.be/utf8js  | Mogua Engine V2  |
| https://oss.fxzb.vip/202111/480be48e0077c7aa95f785eb8d6437f8.png  | Mogua Engine V2  |
| https://oss.fxzb.vip/202111/3a7bfbbefe49a9c50830ea0a460bff5f.png  | Mogua Engine V2  |
| https://oss.fxzb.vip/202111/3fa28b71eff2dd0fc57cb8d4be4c000e.png  | Mogua Engine V2  |
| https://static.fxzb.vip/chupiao.svg  | Mogua Engine V2  |
| https://img10.360buyimg.com/mcmktadmin/jfs/t1/157638/20/28009/92327/62330893Ecbe79d5b/ecb37cb1d74e519c.png  | Mogua Engine V2  |
| https://img10.360buyimg.com/mcmktadmin/jfs/t1/189703/14/21161/23214/612e0049E095e8685/be5f31dd732221bd.png  | Mogua Engine V2  |
| https://img10.360buyimg.com/mcmktadmin/jfs/t1/190823/12/19327/5325/611e881fE06c9e89d/0d9b4544202fe2ba.png  | Mogua Engine V2  |
| https://imgapixs.pysmei.com/bookfiles/bookimages/  | Mogua Engine V2  |
| https://vuejs.org/error-reference/  | Mogua Engine V2  |
| http://www.w3.org/2000/svg  | Mogua Engine V2  |
| http://www.w3.org/1998/Math/MathML  | Mogua Engine V2  |
| http://www.w3.org/1999/xlink  | Mogua Engine V2  |
| https://service.dcloud.net.cn/uniapp/feedback.html  | Mogua Engine V2  |
| http://www.w3.org/2000/svg  | Mogua Engine V2  |

### **4.3 邮箱线索**

### **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=86, ST=浙江省, L=杭州市, O=浙江硕阳控股有限公司, OU=浙江硕阳控股有限公司, CN=sign.keystore 签名算法: rsassa\_pkcs1v15 有效期自: 2023-04-23 02:32:26+00:00 有效期至: 2033-04-20 02:32:26+00:00 发行人: C=86, ST=浙江省, L=杭州市, O=浙江硕阳控股有限公司, OU=浙江硕阳控股有限公司, CN=sign.keystore 序列号: 0x8399834 哈希算法: sha256 md5值: 5b0f742703b8f46ba28b5c2181d38e3b sha1值: bac85b415aca5f1785f1d76053603f57dead8f53 sha256值: 3d554f0b3b7c05bd33c60c65ccc8a9722e25586cade48d5a711f73d3d95018a1 sha512值: 41b78844293bc112517b14adfa58c88074b46a13a37437d4c0c77dfb1a834f1b2c621a2522405e7cbee664f451a554776a2d4e0feb45b6950c0a99cc72d4f612 公钥算法: rsa 密钥长度: 1024 指纹: 512c383e8a5185e2a040fb64bae996a884369cce3ab34aff25fc282eb8618bb7**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "dcloud\_common\_user\_refuse\_api" : "the user denies access to the API"  |
| "dcloud\_io\_without\_authorization" : "not authorized"  |
| "dcloud\_oauth\_authentication\_failed" : "failed to obtain authorization to log in to the authentication service"  |
| "dcloud\_oauth\_empower\_failed" : "the Authentication Service operation to obtain authorized logon failed"  |
| "dcloud\_oauth\_logout\_tips" : "not logged in or logged out"  |
| "dcloud\_oauth\_oauth\_not\_empower" : "oAuth authorization has not been obtained"  |
| "dcloud\_oauth\_token\_failed" : "failed to get token"  |
| "dcloud\_permissions\_reauthorization" : "reauthorize"  |
| "dcloud\_tips\_certificate" : "certificate"  |
| "dcloud\_common\_user\_refuse\_api" : "用户拒绝该API访问"  |
| "dcloud\_io\_without\_authorization" : "没有获得授权"  |
| "dcloud\_oauth\_authentication\_failed" : "获取授权登录认证服务操作失败"  |
| "dcloud\_oauth\_empower\_failed" : "获取授权登录认证服务操作失败"  |
| "dcloud\_oauth\_logout\_tips" : "未登录或登录已注销"  |
| "dcloud\_oauth\_oauth\_not\_empower" : "尚未获取oauth授权"  |
| "dcloud\_oauth\_token\_failed" : "获取token失败"  |
| "dcloud\_permissions\_reauthorization" : "重新授权"  |
| "dcloud\_tips\_certificate" : "证书"  |

## **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.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\_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.INSTALL\_PACKAGES | 系统需要 | 直接安装应用程序 | 允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序 |
| 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.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\_MOCK\_LOCATION | 危险 | 用于测试的模拟位置源 | 创建模拟位置源进行测试。恶意应用程序可以使用它来覆盖由真实位置源（如 GPS 或网络提供商）返回的位置和/或状态 |
| 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.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\_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.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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| android.permission.GET\_ACCOUNTS | 危险 | 列出帐户 | 允许访问账户服务中的账户列表 |
| 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.INTERNAL\_SYSTEM\_WINDOW | 合法 | 显示未经授权的窗口 | 允许创建供内部系统用户界面使用的窗口。不供普通应用程序使用 |
| 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.LOCATION\_HARDWARE | 正常 |  | 允许应用程序使用硬件中的位置功能,例如地理围栏 api |
| android.permission.MODIFY\_AUDIO\_SETTINGS | 正常 | 更改您的音频设置 | 允许应用程序修改全局音频设置,例如音量和路由 |
| 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.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.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.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.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.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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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.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.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\_USER\_PRESENT | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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 |
| com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| 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\_VISUAL\_USER\_SELECTED | 未知 | Unknown permission | Unknown permission from android reference |
| 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。 |
| com.vivo.notification.permission.BADGE\_ICON | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| io.dcloud.PandoraEntry | **Schemes**: shopro://,  |

**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。**