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

**沙发管家（ 4.9.29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 | 沙发管家 |
| 版本 | 4.9.29 |
| 包名 | com.shafa.market |
| 域名线索 | 39条 |
| URL线索 | 67条 |
| APP图标 |  |
| 分析日期 | 2025年8月22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 | webwww\_sfgj\_4.9.29.apk |
| 文件大小 | 10.92MB |
| MD5值 | df3b22efab344018c835241d67e75336 |
| SHA1值 | 1592a359daf0acb90db1cd43f84c7b5965a06103 |
| SHA256值 | 57f138346eac443e02c16456f8b64f37668fab6fef9a1958de9bc111667ba0dc |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 沙发管家 |
| 包名 | com.shafa.market |
| 主活动Activity | com.shafa.market.ShafaHomeAct |
| 安卓版本名称 | 4.9.29 |
| 安卓版本 | 315 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| app.shafa.com | IP: 218.98.54.79  所属国家: China  地区: Jiangsu  城市: Changzhou |
| zero.shafa.com | IP: 101.71.168.166  所属国家: China  地区: Zhejiang  城市: Taizhou |
| www.ddz | 没有服务器地理信息. |
| errlog.umeng.com | IP: 223.109.148.143  所属国家: China  地区: Beijing  城市: Beijing |
| pslog.umeng.com | IP: 59.82.31.154  所属国家: China  地区: Beijing  城市: Beijing |
| report.shafaguanjia.com | 没有服务器地理信息. |
| api.shafaguanjia.com | IP: 218.98.54.75  所属国家: China  地区: Jiangsu  城市: Changzhou |
| ulogs.umengcloud.com | IP: 223.109.148.178  所属国家: China  地区: Beijing  城市: Beijing |
| android.bugly.qq.com | IP: 109.244.244.35  所属国家: China  地区: Beijing  城市: Beijing |
| px-intl.ucweb.com | IP: 157.185.188.1  所属国家: United States of America  地区: California  城市: Monrovia |
| account.shafa.com | IP: 218.98.54.75  所属国家: China  地区: Jiangsu  城市: Changzhou |
| app.sfgj.org | IP: 218.98.54.75  所属国家: China  地区: Jiangsu  城市: Changzhou |
| stats.shafaguanjia.com | IP: 218.98.54.75  所属国家: China  地区: Jiangsu  城市: Changzhou |
| alogus.umeng.com | IP: 223.109.148.178  所属国家: China  地区: Beijing  城市: Beijing |
| www.shafa.com.jiang | 没有服务器地理信息. |
| service.shafa.com | IP: 218.98.54.79  所属国家: China  地区: Jiangsu  城市: Changzhou |
| api.kanbaobei.com | IP: 218.98.54.75  所属国家: China  地区: Jiangsu  城市: Changzhou |
| ulogs.umeng.com | IP: 223.109.148.177  所属国家: China  地区: Beijing  城市: Beijing |
| pingmid.qq.com | IP: 121.51.23.33  所属国家: China  地区: Guangdong  城市: Shenzhen |
| astat.bugly.qcloud.com | IP: 150.109.27.253  所属国家: Singapore  地区: Singapore  城市: Singapore |
| tvkoudai.com | IP: 192.64.119.255  所属国家: United States of America  地区: Georgia  城市: Atlanta |
| h.trace.qq.com | IP: 109.244.244.241  所属国家: China  地区: Beijing  城市: Beijing |
| aaid.umeng.com | IP: 218.91.197.68  所属国家: China  地区: Jiangsu  城市: Nantong |
| developer.umeng.com | IP: 59.82.29.248  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| plbslog.umeng.com | IP: 36.156.202.78  所属国家: China  地区: Beijing  城市: Beijing |
| schemas.android.com | 没有服务器地理信息. |
| www.shafa.com | IP: 218.98.54.79  所属国家: China  地区: Jiangsu  城市: Changzhou |
| errlogos.umeng.com | IP: 47.246.110.96  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| github.com | IP: 20.205.243.166  所属国家: United States of America  地区: Washington  城市: Redmond |
| ouplog.umeng.com | IP: 47.246.110.93  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| app.shafaguanjia.com | IP: 218.98.54.79  所属国家: China  地区: Jiangsu  城市: Changzhou |
| astat.bugly.cros.wr.pvp.net | IP: 170.106.135.32  所属国家: United States of America  地区: California  城市: San Francisco |
| apps.sfcdn.org | IP: 42.176.34.16  所属国家: China  地区: Liaoning  城市: Fuxin |
| rqd.uu.qq.com | IP: 109.244.173.225  所属国家: China  地区: Beijing  城市: Beijing |
| pay.shafa.com | IP: 218.91.237.6  所属国家: China  地区: Jiangsu  城市: Nantong |
| ip.cn | IP: 104.21.58.125  所属国家: United States of America  地区: California  城市: San Francisco |
| service.shafaguanjia.com | IP: 218.98.54.75  所属国家: China  地区: Jiangsu  城市: Changzhou |
| alogsus.umeng.com | IP: 223.109.148.178  所属国家: China  地区: Beijing  城市: Beijing |
| px.ucweb.com | IP: 106.8.139.148  所属国家: China  地区: Hebei  城市: Zhangjiakou |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://schemas.android.com/apk/res/android | com/tvkoudai/tv/ui/Attributes.java |
| http://tvkoudai.com/api/profiles | com/tvkoudai/tv/util/DeviceManager.java |
| http://tvkoudai.com/download? | com/tvkoudai/tv/qrcode/QRCodeManager.java |
| https://errlog.umeng.com/api/crashsdk/logcollect | com/efs/sdk/base/core/f/c.java |
| https://errlogos.umeng.com/api/crashsdk/logcollect | com/efs/sdk/base/core/controller/ControllerCenter.java |
| https://errlog.umeng.com/api/crashsdk/logcollect | com/efs/sdk/base/core/controller/ControllerCenter.java |
| https://pslog.umeng.com | com/umeng/commonsdk/vchannel/a.java |
| https://pslog.umeng.com/ | com/umeng/commonsdk/vchannel/a.java |
| https://ulogs.umeng.com | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://alogus.umeng.com | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://alogsus.umeng.com | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://ulogs.umengcloud.com | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://developer.umeng.com/docs/66632/detail/ | com/umeng/commonsdk/debug/UMLogUtils.java |
| https://developer.umeng.com/docs/119267/detail/182050 | com/umeng/commonsdk/debug/UMLogCommon.java |
| https://plbslog.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://ulogs.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://ouplog.umeng.com | com/umeng/commonsdk/stateless/a.java |
| http://developer.umeng.com/docs/66650/cate/66650 | com/umeng/analytics/pro/j.java |
| https://aaid.umeng.com/api/updateZdata | com/umeng/umzid/ZIDManager.java |
| https://aaid.umeng.com/api/postZdata | com/umeng/umzid/ZIDManager.java |
| https://pay.shafa.com/api/order-status | com/xmxgame/pay/d/b.java |
| https://pay.shafa.com/api/request-pay | com/xmxgame/pay/d/b.java |
| https://pay.shafa.com/api/order-status? | com/xmxgame/pay/d/b.java |
| http://ip.cn | com/shafa/net/NetTool.java |
| http://service.shafa.com/ip | com/shafa/net/NetTool.java |
| http://apps.sfcdn.org | com/shafa/update/slient/download/FileDownLoad.java |
| http://app.sfgj.org/api/splash | com/shafa/splash/util/Config.java |
| http://app.shafaguanjia.com/api/backup/available\_list | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/backup/add | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/backup/del | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/backup/list | com/shafa/market/http/HttpConfig.java |
| http://service.shafaguanjia.com/dns | com/shafa/market/http/HttpConfig.java |
| http://service.shafaguanjia.com/geo | com/shafa/market/http/HttpConfig.java |
| http://stats.shafaguanjia.com/healthcheck | com/shafa/market/http/HttpConfig.java |
| http://www.shafa.com/jiang | com/shafa/market/http/HttpConfig.java |
| http://account.shafa.com/api/points/up | com/shafa/market/http/HttpConfig.java |
| http://account.shafa.com/api/points/check-in | com/shafa/market/http/HttpConfig.java |
| http://account.shafa.com/api/rewards/wins | com/shafa/market/http/HttpConfig.java |
| http://account.shafa.com/api/rewards/list | com/shafa/market/http/HttpConfig.java |
| http://account.shafa.com/api/rewards/lottery | com/shafa/market/http/HttpConfig.java |
| http://account.shafa.com/api/points/info | com/shafa/market/http/HttpConfig.java |
| http://stats.shafaguanjia.com/zhuangji/onekey | com/shafa/market/http/HttpConfig.java |
| http://stats.shafaguanjia.com/zhuangji/installed | com/shafa/market/http/HttpConfig.java |
| http://stats.shafaguanjia.com/i/lan\_upload\_pv | com/shafa/market/http/HttpConfig.java |
| http://stats.shafaguanjia.com/i/url | com/shafa/market/http/HttpConfig.java |
| http://service.shafaguanjia.com/patch | com/shafa/market/http/HttpConfig.java |
| http://service.shafaguanjia.com/gdns | com/shafa/market/http/HttpConfig.java |
| http://stats.shafaguanjia.com/i/lan\_upload | com/shafa/market/http/HttpConfig.java |
| http://account.shafa.com/api/node/new | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/market/app | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/market/list\_v2 | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/market/app\_ids | com/shafa/market/http/HttpConfig.java |
| http://stats.shafaguanjia.com/common/counter | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/market/events | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/update/add | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/update/remove | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/update/sync | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/user/add\_app | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/user/apps | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/user/remove\_app | com/shafa/market/http/HttpConfig.java |
| http://stats.shafaguanjia.com/i/app | com/shafa/market/http/HttpConfig.java |
| http://stats.shafaguanjia.com/i/app\_download | com/shafa/market/http/HttpConfig.java |
| http://stats.shafaguanjia.com/i/app\_download\_installed | com/shafa/market/http/HttpConfig.java |
| http://stats.shafaguanjia.com/i/app\_update | com/shafa/market/http/HttpConfig.java |
| https://account.shafa.com | com/shafa/market/http/HttpConfig.java |
| http://account.shafa.com | com/shafa/market/http/HttpConfig.java |
| http://zero.shafa.com | com/shafa/market/http/HttpConfig.java |
| http://api.kanbaobei.com/v1/videoshelf/get\_hot\_keywords | com/shafa/market/http/HttpConfig.java |
| http://zero.shafa.com/api/channel/setting/ | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/update/check | com/shafa/market/http/HttpConfig.java |
| http://service.shafaguanjia.com | com/shafa/market/http/HttpConfig.java |
| http://stats.shafaguanjia.com | com/shafa/market/http/HttpConfig.java |
| http://service.shafaguanjia.com/tools/adblock | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/market/rank | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/market/apps | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/market/versions | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/search | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/search/stroke | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/related | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/cleanup/rules | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/market/channels | com/shafa/market/http/HttpConfig.java |
| http://account.shafa.com/api/points/app | com/shafa/market/http/HttpConfig.java |
| http://stats.shafaguanjia.com/i/device | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/market/create\_app\_review | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/market/get\_daily\_raffle\_ticket | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/device/info | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/market/discover | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/market/event | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/market/event\_query | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/market/featured\_list | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/cleanup/configuration | com/shafa/market/http/HttpConfig.java |
| http://api.kanbaobei.com/video\_shelf/v1/top? | com/shafa/market/http/HttpConfig.java |
| http://api.kanbaobei.com/v1/videoshelf/episodes?source=com\_shafa\_market | com/shafa/market/http/HttpConfig.java |
| http://api.kanbaobei.com/v1/videoshelf/search | com/shafa/market/http/HttpConfig.java |
| http://api.kanbaobei.com/v1/videoshelf/videolist?source=com\_shafa\_market | com/shafa/market/http/HttpConfig.java |
| http://api.kanbaobei.com/video\_shelf/v1/videolist/show | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/market/game\_kinds | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/market/game\_promotions | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/market/recommendations\_by\_type | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/market/zhuangji\_list | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/market/keyword\_list | com/shafa/market/http/HttpConfig.java |
| http://service.shafaguanjia.com/live\_sources/check | com/shafa/market/http/HttpConfig.java |
| http://service.shafaguanjia.com/live\_sources/formats | com/shafa/market/http/HttpConfig.java |
| http://service.shafaguanjia.com/live\_sources/list | com/shafa/market/http/HttpConfig.java |
| http://service.shafaguanjia.com/live\_sources/shared\_list\_v2 | com/shafa/market/http/HttpConfig.java |
| http://service.shafaguanjia.com/live\_sources/shared\_list\_by\_id | com/shafa/market/http/HttpConfig.java |
| http://service.shafaguanjia.com/live\_sources/my\_list\_preview | com/shafa/market/http/HttpConfig.java |
| http://service.shafaguanjia.com/live\_sources/shared\_list\_preview\_by\_id | com/shafa/market/http/HttpConfig.java |
| http://service.shafaguanjia.com/live\_sources/token | com/shafa/market/http/HttpConfig.java |
| http://service.shafaguanjia.com/live\_sources/upload | com/shafa/market/http/HttpConfig.java |
| https://account.shafa.com/api/points/resources | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/activity/resources | com/shafa/market/http/HttpConfig.java |
| http://account.shafa.com/api/points/activity-apps | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/activity/rules | com/shafa/market/http/HttpConfig.java |
| http://account.shafa.com/api/rewards/recent | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/market/mini\_launcher | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/market/promotions\_by\_key | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/market/raffle | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/market/get\_raffle\_ticket | com/shafa/market/http/HttpConfig.java |
| http://service.shafaguanjia.com/gg/get\_by\_id | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/market/get\_app\_reviews | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/market/get\_app\_review\_config | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/market/rookie\_list | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/market/search\_promotions\_list | com/shafa/market/http/HttpConfig.java |
| http://zero.shafa.com/api/version/0 | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/market/kinds | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/market/splash | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/market/tags\_by\_group | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/market/update\_app\_review | com/shafa/market/http/HttpConfig.java |
| http://zero.shafa.com/app/law/protocol | com/shafa/market/http/HttpConfig.java |
| http://zero.shafa.com/app/law/privacy | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/market/rank\_v2 | com/shafa/market/http/HttpConfig.java |
| http://app.shafaguanjia.com/api/WebController/report | com/shafa/market/http/HttpConfig.java |
| http://app.shafa.com | com/shafa/market/http/HttpHeaderManager.java |
| http://app.shafaguanjia.com/api/market/kinds\_TV\_SHORTCUT | com/shafa/market/http/cache/TvTrackerCache.java |
| http://service.shafaguanjia.com/live\_sources/shared\_list\_preview\_by\_id/ | com/shafa/market/http/volley/RequestManager.java |
| http://service.shafaguanjia.com/live\_sources/shared\_list\_by\_id/ | com/shafa/market/http/volley/RequestManager.java |
| http://app.shafaguanjia.com/api/market/promotions\_by\_key | com/shafa/market/http/volley/RequestManager.java |
| http://app.shafaguanjia.com/api/market/app | com/shafa/market/http/volley/RequestManager.java |
| http://schemas.android.com/apk/res/android | com/shafa/market/ui/button/BlueBackButton.java |
| http://schemas.android.com/apk/res/android | com/shafa/market/ui/button/PopupAppButton.java |
| http://schemas.android.com/apk/res/android | com/shafa/market/ui/common/UnconspicuousButton.java |
| http://schemas.android.com/apk/res/android | com/shafa/market/ui/common/BackButton.java |
| http://service.shafa.com/speedtest/file | com/shafa/market/ui/testspeed/TestSpeedView.java |
| www.ddz | com/shafa/market/ui/homekey/SortUtils.java |
| http://app.shafaguanjia.com/api/market/bgms | com/shafa/market/filemanager/imagescan/BackgroundMusic.java |
| http://app.shafaguanjia.com/api/backup/available\_list? | com/shafa/market/back/BackUpManager.java |
| http://app.shafaguanjia.com/api/backup/add? | com/shafa/market/back/BackUpManager.java |
| http://app.shafaguanjia.com/api/backup/del? | com/shafa/market/back/BackUpManager.java |
| http://account.shafa.com/qr | com/shafa/market/application/ShafaConfig.java |
| www.shafa.com | com/shafa/market/application/APPGlobal.java |
| http://app.shafaguanjia.com/api/market/apps | com/shafa/market/util/LocalAppManager.java |
| http://report.shafaguanjia.com/install\_failed | com/shafa/market/util/install/InstallFailedReporter.java |
| http://app.shafaguanjia.com/api/market/apps | com/shafa/market/util/baseappinfo/ServiceLocalBaseAppManager.java |
| http://app.shafaguanjia.com/api/update/remove | com/shafa/market/util/service/ServiceAppChangeManager.java |
| http://app.shafaguanjia.com/api/update/add | com/shafa/market/util/service/ServiceAppChangeManager.java |
| http://api.shafaguanjia.com/v2 | com/shafa/market/account/AccountManager.java |
| http://account.shafa.com/ | com/shafa/market/account/AccountManager.java |
| http://app.shafaguanjia.com/ | com/shafa/market/account/AccountManager.java |
| http://account.shafa.com/api/user\_info | com/shafa/market/account/AccountManager.java |
| http://account.shafa.com/api/update\_getui | com/shafa/market/account/AccountManager.java |
| http://schemas.android.com/apk/res/android | com/shafa/market/widget/WhiteRoundButton.java |
| http://schemas.android.com/apk/res/android | com/shafa/market/widget/BackButton.java |
| http://schemas.android.com/apk/res/android | com/shafa/market/view/SpacedRatingBar.java |
| http://api.shafaguanjia.com/v2? | com/shafa/market/modules/detail/tabs/review/Api.java |
| http://api.shafaguanjia.com/v2? | com/shafa/market/modules/detail/tabs/tip/Api.java |
| http://app.shafaguanjia.com | com/shafa/market/modules/detail/api/Api.java |
| http://app.shafaguanjia.com/api/market/app? | com/shafa/market/modules/detail/api/Api.java |
| http://account.shafa.com/api/points/app? | com/shafa/market/modules/detail/api/Api.java |
| http://app.shafaguanjia.com/api/market/promotions\_by\_key | com/shafa/market/modules/ipr/Requester.java |
| http://account.shafa.com | com/shafa/market/modules/exchange/api/Api.java |
| http://account.shafa.com/api/exchange\_rewards/list | com/shafa/market/modules/exchange/api/Api.java |
| http://account.shafa.com/api/exchange\_rewards/exchange | com/shafa/market/modules/exchange/api/Api.java |
| http://account.shafa.com/api/exchange\_rewards/history? | com/shafa/market/modules/exchange/api/Api.java |
| http://service.shafa.com/speedtest/file | com/shafa/market/netspeedtest/TestSpeedAct.java |
| http://api.shafaguanjia.com/v2 | com/shafa/market/api/v2/Api.java |
| http://app.shafaguanjia.com/api/market/front\_page | com/shafa/market/fragment/IIndexRequest.java |
| http://pingmid.qq.com:80/ | com/tencent/mid/util/Util.java |
| http://rqd.uu.qq.com/rqd/sync | com/tencent/bugly/crashreport/common/strategy/StrategyBean.java |
| http://android.bugly.qq.com/rqd/async | com/tencent/bugly/crashreport/common/strategy/StrategyBean.java |
| http://astat.bugly.qcloud.com/rqd/async | com/tencent/bugly/crashreport/common/strategy/a.java |
| https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async | com/tencent/bugly/crashreport/common/strategy/a.java |
| http://astat.bugly.cros.wr.pvp.net/:8180/rqd/async | com/tencent/bugly/crashreport/common/strategy/a.java |
| https://h.trace.qq.com/kv?attaid=0f500064192&token=4725229671&carrier= | com/tencent/msdk/dns/d/a.java |
| http://%s/d?%s | com/tencent/msdk/dns/core/n/b/c.java |
| http://%s/d?%s&alg=aes | com/tencent/msdk/dns/core/n/a/c.java |
| http://apps.sfcdn.org | com/tv/download/FileDownLoad.java |
| http://tvkoudai.com/api/report | com/tv/background/IPReporter.java |
| http://tvkoudai.com/api/get\_app | com/tv/background/server/DownloadResponse.java |
| https://github.com/mcxiaoke/packer-ng-plugin | com/mcxiaoke/packer/helper/PackerNg.java |
| https://errlogos.umeng.com/upload | com/uc/crashsdk/e.java |
| https://errlog.umeng.com/upload | com/uc/crashsdk/e.java |
| https://px-intl.ucweb.com | com/uc/crashsdk/a/h.java |
| https://px.ucweb.com | com/uc/crashsdk/a/h.java |
| https://errlog.umeng.com/api/crashsdk/logcollect | com/uc/crashsdk/a/h.java |
| https://errlogos.umeng.com/api/crashsdk/logcollect | com/uc/crashsdk/a/h.java |
| https://errlog.umeng.com | com/uc/crashsdk/a/d.java |
| https://errlogos.umeng.com | com/uc/crashsdk/a/d.java |
| www.shafa.com/jiang | Android String Resource |
| www.shafa.com.jiang | Android String Resource |
| www.shafa.com | Android String Resource |
| https://errlog.umeng.com/api/crashsdk/logcollect | lib/armeabi-v7a/libcrashsdk.so |
| https://errlogos.umeng.com/api/crashsdk/logcollect | lib/armeabi-v7a/libcrashsdk.so |
| https://errlog.umeng.com | lib/armeabi-v7a/libcrashsdk.so |
| https://errlogos.umeng.com | lib/armeabi-v7a/libcrashsdk.so |
| https://errlog.umeng.com/api/crashsdk/logcollect | lib/x86/libcrashsdk.so |
| https://errlogos.umeng.com/api/crashsdk/logcollect | lib/x86/libcrashsdk.so |
| https://errlog.umeng.com | lib/x86/libcrashsdk.so |
| https://errlogos.umeng.com | lib/x86/libcrashsdk.so |
| https://errlog.umeng.com/api/crashsdk/logcollect | lib/arm64-v8a/libcrashsdk.so |
| https://errlogos.umeng.com/api/crashsdk/logcollect | lib/arm64-v8a/libcrashsdk.so |
| https://errlog.umeng.com | lib/arm64-v8a/libcrashsdk.so |
| https://errlogos.umeng.com | lib/arm64-v8a/libcrashsdk.so |
| https://errlog.umeng.com/api/crashsdk/logcollect | lib/armeabi/libcrashsdk.so |
| https://errlogos.umeng.com/api/crashsdk/logcollect | lib/armeabi/libcrashsdk.so |
| https://errlog.umeng.com | lib/armeabi/libcrashsdk.so |
| https://errlogos.umeng.com | lib/armeabi/libcrashsdk.so |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| admin@shafa.com  service@shafa.com | Android String Resource |

### **4.4 手机号线索**

## **5. 签名证书**

**APK is signed v1 signature: True v2 signature: False v3 signature: False Found 1 unique certificates Subject: C=CN, ST=Shanghai, L=Zhabei, O=www.shafa.com, OU=www.shafa.com Signature Algorithm: rsassa\_pkcs1v15 Valid From: 2013-07-11 10:41:24+00:00 Valid To: 2038-07-05 10:41:24+00:00 Issuer: C=CN, ST=Shanghai, L=Zhabei, O=www.shafa.com, OU=www.shafa.com Serial Number: 0x51de8bd4 Hash Algorithm: sha1 md5: be5a929f79fcb4a977a1896a45714a11 sha1: 442164055502d25fd133079f6b3db5cd55afb434 sha256: e310c10d458b4a9f6e8e4275e71a7ffbd0b8082ac8970acfb6713d6d742ff612 sha512: ea08699674f959bab249f5aacc782c679b0472dc68b09e108d003157c6ece3a78529cf3c617bf54cb8df5cbb5741b55448bfde57fa204eb4830dd2eaf26feaf6**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "app\_name\_user" : "沙发应用市场" |
| "key\_position" : "key\_position" |
| "keyboard\_key\_enter" : "完成" |
| "keyboard\_key\_next" : "下一步" |
| "setting\_home\_key" : "按主页键时调出我的常用应用" |
| "setting\_super\_user" : "需要先对设备进行ROOT" |
| "shafa\_setting\_homekey\_shortcut\_close" : "关闭" |
| "shafa\_setting\_homekey\_shortcut\_open" : "开启" |
| "shafa\_setting\_homekey\_shortcut\_open\_tips" : "开启(主页键调出常用功能)" |
| "shafa\_setting\_homekey\_title" : "桌面小管家" |
| "shafa\_setting\_super\_authority" : "超级权限" |
| "shafa\_setting\_super\_authority\_close" : "关闭" |
| "shafa\_setting\_super\_authority\_open" : "开启" |
| "switch\_user" : "切换用户" |
| "username" : "用户名" |
| "wifi\_dlg\_conn\_show\_pwd" : "显示密码" |
| "app\_name\_user" : "Shafa Market" |
| "keyboard\_key\_enter" : "Done" |
| "keyboard\_key\_next" : "Next" |
| "setting\_home\_key" : "Press the Homekey to bring up my common apps" |
| "setting\_super\_user" : "Need to get root privileges first" |
| "shafa\_setting\_homekey\_shortcut\_close" : "Close" |
| "shafa\_setting\_homekey\_shortcut\_open" : "Open" |
| "shafa\_setting\_homekey\_shortcut\_open\_tips" : "Open(Homekey get common feature)" |
| "shafa\_setting\_homekey\_title" : "Desktop housekeeper" |
| "shafa\_setting\_super\_authority" : "Super authority" |
| "shafa\_setting\_super\_authority\_close" : "Close" |
| "shafa\_setting\_super\_authority\_open" : "Open" |
| "switch\_user" : "Switch User" |
| "username" : "Username" |
| "wifi\_dlg\_conn\_show\_pwd" : "Show password" |
| "app\_name\_user" : "沙發應用市場" |
| "keyboard\_key\_enter" : "完成" |
| "keyboard\_key\_next" : "下一步" |
| "setting\_home\_key" : "按主頁鍵時調出我的常用應用" |
| "setting\_super\_user" : "需要先對設備進行ROOT" |
| "shafa\_setting\_homekey\_shortcut\_close" : "關閉" |
| "shafa\_setting\_homekey\_shortcut\_open" : "開啟" |
| "shafa\_setting\_homekey\_shortcut\_open\_tips" : "開啟(主頁鍵調出常用功能)" |
| "shafa\_setting\_homekey\_title" : "桌面小管家" |
| "shafa\_setting\_super\_authority" : "超級權限" |
| "shafa\_setting\_super\_authority\_close" : "關閉" |
| "shafa\_setting\_super\_authority\_open" : "開啟" |
| "switch\_user" : "切換用戶" |
| "username" : "用戶名" |
| "wifi\_dlg\_conn\_show\_pwd" : "顯示密碼" |

## **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.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\_DOWNLOAD\_MANAGER | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.DOWNLOAD\_WITHOUT\_NOTIFICATION | 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.GET\_PACKAGE\_SIZE | 正常 | 测量应用程序存储空间 | 允许应用程序找出任何包使用的空间 |
| 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.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\_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.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.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.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.RECEIVE\_USER\_PRESENT | 未知 | Unknown permission | Unknown permission from android reference |
| 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.CLEAR\_APP\_CACHE | 系统需要 | 删除所有应用程序缓存数据 | 允许应用程序通过删除应用程序缓存目录中的文件来释放手机存储空间。访问通常非常受限于系统进程。 |
| 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.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.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 |
| 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.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.DELETE\_PACKAGES | 系统需要 | 删除应用程序 | 允许应用程序删除 Android 包。恶意应用程序可以使用它来删除重要的应用程序 |
| 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.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.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 |
| com.baidu.permission.SHARE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.shafa.market.ShafaRouterHandlerActivity | **Schemes**: shafa://,  **Hosts:** shafa.com, |
| com.shafa.market.filemanager.imagescan.ImageWatcherAct | **Schemes**: file://,  **Mime Types:** image/bmp, image/jpeg, image/gif, image/png, image/webp, image/x-ms-bmp, image/vnd.wap.wbmp, |

**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。**