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

**九方智投（ 4.25.1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 | 九方智投 |
| 版本 | 4.25.1 |
| 包名 | com.rjhy.uranus |
| 域名线索 | 30条 |
| URL线索 | 8条 |
| APP图标 |  |
| 分析日期 | 2025年6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 | jiufangzhito...4.apk |
| 文件大小 | 206.9MB |
| MD5值 | f707dd20a889df809767d3405779697d |
| SHA1值 | b5ab6ddf08bb2ea76fa66cdc0a1116a066771e57 |
| SHA256值 | 745e2e18d688e1c78e077853e2b9678160e8bdf8e0466607cdc7578882a2aace |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 九方智投 |
| 包名 | com.rjhy.uranus |
| 主活动Activity | com.rjhy.newstar.module.splash.SplashActivity |
| 安卓版本名称 | 4.25.1 |
| 安卓版本 | 42510000 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| metrics1-drcn.dt.dbankcloud.cn | IP: 111.202.16.252 所属国家: China 地区: Beijing 城市: Beijing  |
| data-dre.push.dbankcloud.com | IP: 80.158.49.244 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| data-drcn.push.dbankcloud.com | IP: 121.36.117.8 所属国家: China 地区: Beijing 城市: Beijing  |
| metrics5.dt.dbankcloud.ru | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| news.newone.com.cn | IP: 58.251.26.126 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| data-dra.push.dbankcloud.com | IP: 119.8.163.189 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| 162.14.6.247 | IP: 162.14.6.247 所属国家: China 地区: Beijing 城市: Beijing  |
| journeyapps.com | IP: 3.169.183.86 所属国家: United States of America 地区: Washington 城市: Seattle  |
| 119.29.29.98 | IP: 119.29.29.98 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| h5.9fh5.cn | IP: 116.142.235.231 所属国家: China 地区: Beijing 城市: Beijing  |
| grs.dbankcloud.com | IP: 60.28.200.159 所属国家: China 地区: Tianjin 城市: Tianjin  |
| grs.platform.dbankcloud.ru | 没有服务器地理信息.  |
| stage-h5.techgp.cn | IP: 47.117.171.254 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| h5-9fzt.secon.cn | IP: 106.14.133.100 所属国家: China 地区: Shanghai 城市: Shanghai  |
| ip.taobao.com | IP: 59.82.121.179 所属国家: China 地区: Beijing 城市: Beijing  |
| www.95516.com | IP: 123.126.74.16 所属国家: China 地区: Beijing 城市: Beijing  |
| yhtm.i618.com.cn | IP: 221.204.232.51 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| metrics5.data.hicloud.com | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| metrics-dra.dt.hicloud.com | IP: 94.74.88.100 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| data-drru.push.dbankcloud.com | IP: 159.138.202.31 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| grs.dbankcloud.asia | IP: 49.4.40.185 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| www.newone.com.cn | IP: 27.39.91.238 所属国家: China 地区: Guangdong 城市: Meizhou  |
| test-jsapp.jinyi999.cn | IP: 106.14.1.16 所属国家: China 地区: Shanghai 城市: Shanghai  |
| api.map.baidu.com | IP: 111.206.208.72 所属国家: China 地区: Beijing 城市: Beijing  |
| grs.dbankcloud.eu | 没有服务器地理信息.  |
| ping.huatuo.qq.com | IP: 220.194.111.195 所属国家: China 地区: Tianjin 城市: Tianjin  |
| metrics2.data.hicloud.com | IP: 80.158.38.48 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| www.mob.com | IP: 180.188.26.28 所属国家: China 地区: Zhejiang 城市: Taizhou  |
| grs.dbankcloud.cn | IP: 49.4.40.185 所属国家: China 地区: Guangdong 城市: Guangzhou  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://yhtm.i618.com.cn:8060/indexnew  | 摸瓜V1引擎  |
| http://yhtm.i618.com.cn:8060/upload  | 摸瓜V1引擎  |
| https://journeyapps.com/  | 摸瓜V1引擎  |
| https://github.com/journeyapps/zxing-android-embedded  | 摸瓜V1引擎  |
| http://www.mob.com/policy/en>http://www.mob.com/policy/en</a>.  | 摸瓜V1引擎  |
| http://www.mob.com/about/policy>http://www.mob.com/about/policy</a>  | 摸瓜V1引擎  |
| https://www.95516.com/portal/open/init.do?entry=open  | 摸瓜V1引擎  |
| https://www.mob.com  | 摸瓜V1引擎  |
| http://www.mob.com/about/policy/en>http://www.mob.com/about/policy/en</a>.If  | 摸瓜V1引擎  |
| http://www.mob.com/policy/zh>http://www.mob.com/policy/zh</a>  | 摸瓜V1引擎  |
| https://test-jsapp.jinyi999.cn/rjhy/hxg-app-h5  | 摸瓜V2引擎  |
| https://test-jsapp.jinyi999.cn/jsapp/rjhy/video-living-h5  | 摸瓜V2引擎  |
| https://test-jsapp.jinyi999.cn/rjhy/jfzg-mall-h5  | 摸瓜V2引擎  |
| https://stage-h5.techgp.cn/rjhy/hxg-app-h5  | 摸瓜V2引擎  |
| https://stage-h5.techgp.cn/rjhy/video-living-h5  | 摸瓜V2引擎  |
| https://stage-h5.techgp.cn/rjhy/jfzg-mall-h5  | 摸瓜V2引擎  |
| https://h5.9fh5.cn/rjhy/hxg-app-h5  | 摸瓜V2引擎  |
| https://h5-9fzt.secon.cn/video-living-h5  | 摸瓜V2引擎  |
| https://h5.9fh5.cn/rjhy/jfzg-mall-h5  | 摸瓜V2引擎  |
| https://data-drcn.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-dra.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-dre.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-drru.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://metrics1-drcn.dt.dbankcloud.cn:443  | 摸瓜V2引擎  |
| https://metrics-dra.dt.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics2.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics5.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics5.dt.dbankcloud.ru:6447  | 摸瓜V2引擎  |
| https://grs.dbankcloud.com  | 摸瓜V2引擎  |
| https://grs.dbankcloud.cn  | 摸瓜V2引擎  |
| https://grs.dbankcloud.asia  | 摸瓜V2引擎  |
| https://grs.platform.dbankcloud.ru  | 摸瓜V2引擎  |
| https://grs.dbankcloud.eu  | 摸瓜V2引擎  |
| http://162.14.6.247/v4/ConfigGetSvc/GetOpenSSOIPList  | lib/arm64-v8a/libImSDK.so  |
| https://ping.huatuo.qq.com/api.im.qcloud.com  | lib/arm64-v8a/libImSDK.so  |
| http://119.29.29.98/d?id=3743  | lib/arm64-v8a/libImSDK.so  |
| http://news.newone.com.cn/newone/service/zhuoyue/index.htm  | lib/arm64-v8a/libTdxAndroid.so  |
| http://www.newone.com.cn/newone/expert/nodelist\_showa\_zyb.jsp?khh=  | lib/arm64-v8a/libTdxAndroid.so  |
| http://www.newone.com.cn/ws/html?arg=2personal/95565/index  | lib/arm64-v8a/libTdxAndroid.so  |
| http://www.newone.com.cn/sms  | lib/arm64-v8a/libTdxAndroid.so  |
| http://www.newone.com.cn/mytzgw?khh=  | lib/arm64-v8a/libTdxAndroid.so  |
| http://news.newone.com.cn/newone/zhuanyeban/gpad/gpad.html  | lib/arm64-v8a/libTdxAndroid.so  |
| http://api.map.baidu.com  | lib/arm64-v8a/libTdxAndroidCore.so  |
| http://ip.taobao.com  | lib/arm64-v8a/libTdxAndroidCore.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| 椭圆形@3x.png  | 摸瓜V2引擎  |
| 收藏002@3x.png 收藏黄@3x.png  | 摸瓜V2引擎  |
| 点赞002@3x.png 点赞红@3x.png  | 摸瓜V2引擎  |
| 矩形@3x.png  | 摸瓜V2引擎  |
| 手@3x.png 查看奖品@3x.png 按钮底@3x.png  | 摸瓜V2引擎  |
| 手@3x.png 查看结果@3x.png 按钮底@3x.png  | 摸瓜V2引擎  |
| 页面跳转加载@3x.png  | 摸瓜V2引擎  |
| img5@3x.png img2@3x.png img4@3x.png img3@3x.png img1@3x.png  | 摸瓜V2引擎  |
| 行情2备份-底板@3x.png  | 摸瓜V2引擎  |
| 首页2备份-底板@3x.png  | 摸瓜V2引擎  |
| 行情2备份-底板@3x.png  | 摸瓜V2引擎  |
| 视频3备份-底板@3x.png  | 摸瓜V2引擎  |
| vip2备份-底板@3x.png  | 摸瓜V2引擎  |
| 自选2备份-底板@3x.png  | 摸瓜V2引擎  |
| 手@3x.png 立即参与@3x.png 按钮底@3x.png  | 摸瓜V2引擎  |
| 页面跳转加载@3x.png  | 摸瓜V2引擎  |
| 4id@qh.کu  | 摸瓜V2引擎  |
| 刷新@3x.png 刷新di@3x.png  | 摸瓜V2引擎  |
| 手@3x.png 下次再说@3x.png 按钮底@3x.png  | 摸瓜V2引擎  |
| 天财加载@3x.png  | 摸瓜V2引擎  |
| 路径@3x.png 矩形@3x.png  | 摸瓜V2引擎  |
| 收藏002@3x.png  | 摸瓜V2引擎  |
| bai点赞002@3x.png  | 摸瓜V2引擎  |
| 手势1@3x.png 向上@3x.png  | 摸瓜V2引擎  |
| 椭圆形蓝@3x.png 2@3x.png 椭圆形紫@3x.png 3@3x.png 椭圆形备份@3x.png 椭圆形@3x.png img@3x.png  | 摸瓜V2引擎  |
| 矩形22@3x.png  | 摸瓜V2引擎  |
| 获取支付结果中@3x.png  | 摸瓜V2引擎  |
| i@k.4n  | 摸瓜V2引擎  |
| yם@x.iv8  | 摸瓜V2引擎  |
| d@f.ny  | 摸瓜V2引擎  |
| 3@3x.png  | 摸瓜V2引擎  |
| 3@3x.png  | 摸瓜V2引擎  |
| 3@3x.png  | 摸瓜V2引擎  |
| 3@3x.png  | 摸瓜V2引擎  |
| 2@3x.png  | 摸瓜V2引擎  |
| 反馈2@3x.png  | 摸瓜V2引擎  |
| 拨打电话了解更多@3x.png 三角形@3x.png  | 摸瓜V2引擎  |
| 矩形@3x.png  | 摸瓜V2引擎  |
| 001@3x.png 002@3x.png  | 摸瓜V2引擎  |
| 矩形@3x.png  | 摸瓜V2引擎  |
| 蒙版@3x.png  | 摸瓜V2引擎  |
| 文字3@3x.png 文字4@3x.png  | 摸瓜V2引擎  |
| 提示@3x.png  | 摸瓜V2引擎  |
| 联系专属助理了解更多@3x.png 三角形@3x.png  | 摸瓜V2引擎  |
| 风车@3x.png 椭圆@1x.png 椭圆形@3x.png 底色@3x.png  | 摸瓜V2引擎  |
| mobile-login@1.06  | lib/arm64-v8a/libTdxAndroid.so  |
| bill456@yahoo.com 5456509@qq.com dami@tcalc1.0\_export alice123@yahoo.com ftp@example.com  | lib/arm64-v8a/libTdxAndroidCore.so  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 18431372549  | 摸瓜V2引擎  |

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: True 找到 1 个唯一证书 主题: O=uranus, OU=uranus 签名算法: rsassa\_pkcs1v15 有效期自: 2019-11-13 06:43:22+00:00 有效期至: 2044-11-06 06:43:22+00:00 发行人: O=uranus, OU=uranus 序列号: 0x738dfefa 哈希算法: sha256 md5值: b84f3cbbccea0a896697035a8ee50a14 sha1值: 0f607e328e084e2f0df0d490226e6cc9e2f60c33 sha256值: 8bca08dde70b067ceb159e1bd1203ebe3270698ad9420e7959abaea9b2bca2bb sha512值: f0ae2a3b1997028839b0c5473b5bd42cf9144138e5d5cdfc1a8d52c4e67a33a62296e2301a074f42295553391c92fdc1b45c8d6c0a107c485e7cb2612191f534 公钥算法: rsa 密钥长度: 2048 指纹: cf93ea368bd3b58f837693d9a5595dc433ec48945fd1e128b19c207b7a36f1c6**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "CRVIDEOSDK\_QUE\_NOUSER" : "没有用户在排队"  |
| "Please\_enter\_a\_username" : "Please enter a username"  |
| "Two\_input\_password" : "Inconsistent password, please enter again!"  |
| "authorization\_agree" : "OK"  |
| "authorization\_cancel" : "Cancel"  |
| "authorization\_title" : "Privacy Authorization"  |
| "base\_tv\_author\_service" : "服务期内自动播放直播/视频"  |
| "base\_tv\_author\_seven" : "七天内自动播放直播/视频"  |
| "beauty\_setting\_pannel\_key\_AI\_key" : "AI抠背"  |
| "cancel\_auth" : "取消自动授权"  |
| "check\_result\_get\_token\_fail" : "Get token from server failed%1$s%2$s"  |
| "check\_result\_get\_token\_success" : "Get token from server success"  |
| "default\_user\_name" : "游客"  |
| "err\_auth\_dented" : "认证被否决"  |
| "fin\_applet\_admin\_auth\_err\_title" : "没有审核权限"  |
| "fin\_applet\_authorization\_setting" : "小程序授权管理"  |
| "fin\_applet\_default\_userinfo\_auth\_notice" : "您授权后，小程序开发者（包括小程序代开发服务商的开发者及小程序中使用插件的开发者）将%1$s，为您提供相关服务。开发者收集、存储、处理或使用用户隐私及数据，应当遵守网络安全法与个人信息保护规范等相关法律法规。若您认为开发者未遵守上述规定或存在其他侵害用户隐私或数据的情况，可进行%2$s。"  |
| "fin\_applet\_third\_userinfo\_auth" : "第三方用户信息授权说明"  |
| "fin\_applet\_third\_userinfo\_auth\_notice" : "您授权后，小程序开发者（包括小程序代开发服务商的开发者及小程序中使用插件的开发者）将%1$s，为您提供相关服务。开发者严格按照%2$s处理您的个人信息，如您发现开发者不当处理您的个人信息，可进行%3$s。"  |
| "forget\_pwd" : "忘记密码"  |
| "illegal\_user\_name" : "Illegal user name"  |
| "input\_password" : "请输入有效的密码"  |
| "input\_username" : "请输入您的用户名"  |
| "library\_zxingandroidembedded\_author" : "JourneyApps"  |
| "library\_zxingandroidembedded\_authorWebsite" : "https://journeyapps.com/"  |
| "login\_forget\_password" : "忘记密码？"  |
| "mobcommon\_authorize\_dialog\_accept" : "Accept"  |
| "mobcommon\_authorize\_dialog\_content" : "In order to provide you with Mobservice, please check our service policy. For details, please click <a href=http://www.mob.com/policy/en>http://www.mob.com/policy/en</a>. If you agree with our service policy, please click accept, if you do not agree with our service policy, please click reject"  |
| "mobcommon\_authorize\_dialog\_reject" : "Reject"  |
| "mobcommon\_authorize\_dialog\_title" : "Terms of Use"  |
| "mobdemo\_authorize\_dialog\_content" : "为了给您提供Mobservice相关产品服务，请您详细查看我们的隐私政策，详见<a href=http://www.mob.com/about/policy>http://www.mob.com/about/policy</a>。如您同意我们的隐私政策，请点击“接受”，如您不同意我们的隐私政策，请点击“拒绝”。"  |
| "mobdemo\_authorize\_dialog\_title" : "服务授权"  |
| "password" : "Password"  |
| "pos\_pwd\_display\_yiqianbao" : "请输入壹钱包支付密码:"  |
| "ppplugin\_dialog\_purse\_not\_get\_pwdinfo\_yiqianbao" : "壹钱包密码键盘无密文信息返回"  |
| "ppplugin\_forgetpwd\_prompt" : "忘记密码"  |
| "ppplugin\_input\_cardinfo\_cardpwd\_prompt" : "确认密码"  |
| "ppplugin\_inputpaypwd\_pos\_prompt" : "请输入6位全民付移动支付密码"  |
| "ppplugin\_inputpaypwd\_prompt" : "请输入6位支付密码"  |
| "ppplugin\_inputpwddialog\_accbalance\_prompt" : "账户余额"  |
| "ppplugin\_inputpwddialog\_coupon\_prompt" : "优惠券"  |
| "ppplugin\_microfreepwd\_amount\_prompt" : "免密金额"  |
| "ppplugin\_microfreepwd\_pay\_prompt" : "小额免密支付"  |
| "ppplugin\_microfreepwd\_prompt" : "小额免密"  |
| "ppplugin\_microfreepwd\_switchoff" : "关闭"  |
| "ppplugin\_microfreepwd\_switchon" : "已开启"  |
| "ppplugin\_microfreepwd\_use\_prompt" : "超过免密额度时，需要验证支付密码，并且系统会移除可疑交易。"  |
| "ppplugin\_modifypaypwd\_ok" : "支付密码修改成功"  |
| "ppplugin\_modifypwd\_prompt" : "修改支付密码"  |
| "ppplugin\_resetpaypwd\_ok" : "支付密码重置成功"  |
| "ppplugin\_session\_timeout\_prompt" : "由于您长时间未操作，请重新登录"  |
| "ppplugin\_set\_pwd\_prompt" : "设置密码"  |
| "session" : "Conversation"  |
| "session\_data" : "场次数据"  |
| "session\_timeout" : "会话超时,请重新登录"  |
| "set\_custom\_appkey" : "Set custom App key"  |
| "ssdk\_cmcc\_auth" : "手机认证服务由中国移动提供"  |
| "ssdk\_cmcc\_login\_one\_key" : "本机号码一键登录"  |
| "ssdk\_instapaper\_pwd" : "密码"  |
| "ssdk\_weibo\_oauth\_regiseter" : "应用授权"  |
| "tips\_amount\_free\_pwd" : "已为您开启200元额度小额免密，可在右上角设置"  |
| "tips\_input\_password" : "为了您的账号安全请输入支付密码"  |
| "user\_name" : "User name"  |
| "fin\_applet\_admin\_auth\_err\_title" : "No examine access"  |
| "fin\_applet\_authorization\_setting" : "Authorization setting"  |
| "fin\_applet\_default\_userinfo\_auth\_notice" : "Upon your authorization, the mini-app developers (including mini-app developers on behalf of development services and developers of embedded plugins in mini-app) will %1$s to provide services for you. The developer shall process your personal information in strict accordance with network security law and personal information protection norms and other relevant laws and regulations when collecting, storing, processing or using user privacy and data. In the event of the developer's improper use of your personal information, please %2$s to us."  |
| "fin\_applet\_third\_userinfo\_auth" : "Third-party user information authorization description"  |
| "fin\_applet\_third\_userinfo\_auth\_notice" : "Upon your authorization, the mini-app developers (including mini-app developers on behalf of development services and developers of embedded plugins in mini-app) will %1$s to provide services for you. The developer shall process your personal information in strict accordance with %2$s. In the event of the developer's improper use of your personal information, please %3$s to us."  |
| "mobcommon\_authorize\_dialog\_accept" : "Accept"  |
| "mobcommon\_authorize\_dialog\_content" : "In order to provide you with Mobservice, please check our service policy. For details, please click <a href=http://www.mob.com/policy/en>http://www.mob.com/policy/en</a>. If you agree with our service policy, please click accept, if you do not agree with our service policy, please click reject"  |
| "mobcommon\_authorize\_dialog\_reject" : "Reject"  |
| "mobcommon\_authorize\_dialog\_title" : "Terms of Use"  |
| "mobdemo\_authorize\_dialog\_content" : "In order to provide you with Mobservice related products and services, please check our privacy policy in detail, see details<a href=http://www.mob.com/about/policy/en>http://www.mob.com/about/policy/en</a>.If you agree with our privacy policy, please click accept. If you disagree with our privacy policy, please click reject."  |
| "mobdemo\_authorize\_dialog\_title" : "service authority"  |
| "ssdk\_cmcc\_auth" : "Provided by China Mobile"  |
| "ssdk\_cmcc\_login\_one\_key" : "PhoneNum Login"  |
| "ssdk\_instapaper\_pwd" : "Password"  |
| "ssdk\_weibo\_oauth\_regiseter" : "Authorization"  |
| "authorization\_agree" : "同意"  |
| "authorization\_cancel" : "取消"  |
| "authorization\_title" : "隐私授权"  |
| "mobcommon\_authorize\_dialog\_accept" : "同意"  |
| "mobcommon\_authorize\_dialog\_content" : "为了给您提供Mobservice相关产品服务，请您详细查看我们的隐私政策，详见<a href=http://www.mob.com/policy/zh>http://www.mob.com/policy/zh</a>。如您同意我们的隐私政策，请点击“接受”，如您不同意我们的隐私政策，请点击“拒绝”。"  |
| "mobcommon\_authorize\_dialog\_reject" : "拒绝"  |
| "mobcommon\_authorize\_dialog\_title" : "服务授权"  |
| "Please\_enter\_a\_username" : "请输入用户名"  |
| "Two\_input\_password" : "两次输入的密码不一致，请重新输入!"  |
| "check\_result\_get\_token\_fail" : "Token获取失败%1$s%2$s"  |
| "check\_result\_get\_token\_success" : "Token获取成功"  |
| "illegal\_user\_name" : "用户名不合法"  |
| "password" : "密码"  |
| "session" : "会话"  |
| "set\_custom\_appkey" : "自定义App key"  |
| "user\_name" : "用户名"  |

## **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.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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.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.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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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.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.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.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.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 |
| com.android.launcher.permission.READ\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.READ\_CALENDAR | 危险 | 读取日历事件 | 允许应用程序读取您手机上存储的所有日历事件。恶意应用程序可以借此将您的日历事件发送给其他人 |
| android.permission.WRITE\_CALENDAR | 危险 | 添加或修改日历事件并向客人发送电子邮件 | 允许应用程序添加或更改日历上的事件,这可能会向客人发送电子邮件。恶意应用程序可以使用它来删除或修改您的日历活动或向客人发送电子邮件 |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| com.vivo.notification.permission.BADGE\_ICON | 未知 | Unknown permission | Unknown permission from android reference |
| 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。 |
| com.rjhy.uranus.permission.xenv.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.rjhy.uranus.gdt.qq.SEND\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| com.rjhy.uranus.gdt.qq.RECEIVE\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| freemme.permission.msa | 未知 | Unknown permission | Unknown permission from android reference |
| freemme.permission.msa.SECURITY\_ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| oplus.permission.settings.LAUNCH\_FOR\_EXPORT | 未知 | Unknown permission | Unknown permission from android reference |
| com.vivo.identifier.permission.OAID\_STATE\_DIALOG | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.RECORD\_VIDEO | 未知 | Unknown permission | Unknown permission from android reference |
| android.hardware.camera | 未知 | Unknown permission | Unknown permission from android reference |
| android.hardware.camera.autofocus | 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.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.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 |
| org.simalliance.openmobileapi.SMARTCARD | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.USE\_FINGERPRINT | 正常 | allow use of指纹 | 该常量在 API 级别 28 中已被弃用。应用程序应改为请求 USE\_BIOMETRIC |
| 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\_MEDIA\_AUDIO | 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 |
| com.android.launcher.permission.INSTALL\_SHORTCUT | 未知 | Unknown permission | Unknown permission from android reference |
| com.android.launcher.permission.UNINSTALL\_SHORTCUT | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.NFC | 正常 | 控制近场通信 | 允许应用程序与近场通信 (NFC) 标签,卡和读卡器进行通信 |
| com.rjhy.uranus.permission.FIN\_APPLET\_RECEIVER | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FOREGROUND\_SERVICE\_MEDIA\_PROJECTION | 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.READ\_PRIVILEGED\_PHONE\_STATE | 未知 | Unknown permission | Unknown permission from android reference |
| com.coloros.mcs.permission.RECIEVE\_MCS\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.heytap.mcs.permission.RECIEVE\_MCS\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.SCHEDULE\_EXACT\_ALARM | 正常 |  | 允许应用程序使用精确的警报调度 API 来执行对时间敏感的后台工作 |
| getui.permission.GetuiService.com.rjhy.uranus | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| com.rjhy.uranus.permission.MIPUSH\_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.hihonor.push.permission.READ\_PUSH\_NOTIFICATION\_INFO | 未知 | Unknown permission | Unknown permission from android reference |
| com.rjhy.uranus.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| com.rjhy.uranus.permission.PUSH\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.rjhy.newstar.module.splash.SplashActivity | **Schemes**: hxgapp://,  |
| com.rjhy.newstar.module.main.MainActivity | **Schemes**: sa9498327e://, **Hosts:** heatmap,  |
| com.rjhy.newstar.module.externaljump.IntentParseActivity | **Schemes**: jfztqlbapp://, xi49xjscr://, http://, https://, **Hosts:** @string/jf\_app\_link\_test, @string/jf\_app\_link\_uat, @string/jf\_app\_link\_release, **Path Patterns:** /.\*,  |
| com.rjhy.uranus.AlipayMiniProgramCallbackActivity | **Schemes**: jfzt\_ql\_app\_pay://,  |
| com.sensorsdata.analytics.android.sdk.dialog.SchemeActivity | **Schemes**: sa596d308e://, sa03177384://,  |
| com.finogeeks.lib.applet.modules.urlrouter.UrlRouterActivity | **Schemes**: @string/fin\_applet\_router\_url\_scheme://,  |
| cn.sharesdk.loopshare.LoopShareActivity | **Schemes**: ssdk25089b50864f7://, **Hosts:** cn.sharesdk.loop,  |

**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。**