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

**树拍易购（ 2.5.1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 | 树拍易购 |
| 版本 | 2.5.1 |
| 包名 | com.spyg.yigou.mall |
| 域名线索 | 21条 |
| URL线索 | 5条 |
| APP图标 |  |
| 分析日期 | 2025年7月3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 | com.spyg.yigou.mall\_2.5.1.apk |
| 文件大小 | 92.42MB |
| MD5值 | b7682006395e1b9a1fe0aecc9c2019ad |
| SHA1值 | d3308d35cede8eea525bd823324dae884ec3beb8 |
| SHA256值 | 8f1d914ac60c1617b342200f44dc0472e3d6135a4211e9f4d0cf9b606c54bba0 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 树拍易购 |
| 包名 | com.spyg.yigou.mall |
| 主活动Activity | com.ghsc.yigou.live.ui.LaunchActivity |
| 安卓版本名称 | 2.5.1 |
| 安卓版本 | 251 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| www.ietf.org | IP: 104.16.45.99 所属国家: United States of America 地区: California 城市: San Francisco  |
| data-drcn.push.dbankcloud.com | IP: 118.194.33.160 所属国家: China 地区: Shanghai 城市: Shanghai  |
| metrics5.data.hicloud.com | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| slsrole.alicdn.com | IP: 218.11.15.230 所属国家: China 地区: Hebei 城市: Shijiazhuang  |
| grs.dbankcloud.asia | IP: 49.4.35.251 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| grs.platform.dbankcloud.ru | 没有服务器地理信息.  |
| metrics2.data.hicloud.com | IP: 80.158.38.48 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| www.webrtc.org | IP: 142.250.73.110 所属国家: United States of America 地区: California 城市: Mountain View  |
| data-dra.push.dbankcloud.com | IP: 119.8.163.189 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| grs.dbankcloud.eu | 没有服务器地理信息.  |
| metrics5.dt.dbankcloud.ru | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| www.alibaba.com | IP: 203.119.204.250 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| grs.dbankcloud.com | IP: 60.28.200.159 所属国家: China 地区: Tianjin 城市: Tianjin  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| metrics1-drcn.dt.dbankcloud.cn | IP: 111.202.16.252 所属国家: China 地区: Beijing 城市: Beijing  |
| data-drru.push.dbankcloud.com | IP: 159.138.202.31 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| cloud-config-service.rtc.aliyuncs.com | IP: 47.93.95.208 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| metrics-dra.dt.hicloud.com | IP: 94.74.88.100 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| px.ucweb.com | IP: 116.132.217.241 所属国家: China 地区: Hebei 城市: Shijiazhuang  |
| data-dre.push.dbankcloud.com | IP: 80.158.49.244 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| grs.dbankcloud.cn | IP: 49.4.35.251 所属国家: China 地区: Guangdong 城市: Guangzhou  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://github.com/vinc3m1  | 摸瓜V1引擎  |
| https://github.com/vinc3m1/RoundedImageView  | 摸瓜V1引擎  |
| https://github.com/vinc3m1/RoundedImageView.git  | 摸瓜V1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  |
| https://px.ucweb.com/upload  | lib/arm64-v8a/libAliVCIM.so  |
| https://cloud-config-service.rtc.aliyuncs.com/configservice/v1/getAioLoggerConfig  | lib/arm64-v8a/libAliVCIM.so  |
| https://slsrole.alicdn.com  | lib/arm64-v8a/libAliVCIM.so  |
| http://www.ietf.org/id/draft-holmer-rmcat-transport-wide-cc-extensions-01  | lib/arm64-v8a/libAliVCIM.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/abs-send-time  | lib/arm64-v8a/libAliVCIM.so  |
| http://www.alibaba.com/experiments/rtp-hdrext/picture\_id  | lib/arm64-v8a/libAliVCIM.so  |
| http://www.alibaba.com/experiments/rtp-hdrext/audio\_ranking\_level\_id  | lib/arm64-v8a/libAliVCIM.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| ftp@example.com  | lib/arm64-v8a/libAliVCIM.so  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 13117485397  | 摸瓜V2引擎  |
| 13025983332  | 摸瓜V2引擎  |
| 13028568181  | 摸瓜V2引擎  |
| 13043634778  | 摸瓜V2引擎  |
| 13045878678  | 摸瓜V2引擎  |
| 13054880680  | 摸瓜V2引擎  |
| 13081039366  | 摸瓜V2引擎  |
| 13113212965  | 摸瓜V2引擎  |
| 13138380505  | 摸瓜V2引擎  |
| 13147025988  | 摸瓜V2引擎  |
| 13149261444  | 摸瓜V2引擎  |
| 13182616700  | 摸瓜V2引擎  |
| 13182670840  | 摸瓜V2引擎  |
| 13242851818  | 摸瓜V2引擎  |
| 13243835358  | 摸瓜V2引擎  |
| 13263769555  | 摸瓜V2引擎  |
| 13366708682  | 摸瓜V2引擎  |
| 13378981666  | 摸瓜V2引擎  |
| 13402753742  | 摸瓜V2引擎  |
| 13407840910  | 摸瓜V2引擎  |
| 13414628999  | 摸瓜V2引擎  |
| 13417437358  | 摸瓜V2引擎  |
| 13418585882  | 摸瓜V2引擎  |
| 13418603123  | 摸瓜V2引擎  |
| 13424276248  | 摸瓜V2引擎  |
| 13437729078  | 摸瓜V2引擎  |
| 13467892989  | 摸瓜V2引擎  |
| 13477282334  | 摸瓜V2引擎  |
| 13480173922  | 摸瓜V2引擎  |
| 13480570688  | 摸瓜V2引擎  |
| 13480845065  | 摸瓜V2引擎  |
| 13510233578  | 摸瓜V2引擎  |
| 13510539859  | 摸瓜V2引擎  |
| 13510976323  | 摸瓜V2引擎  |
| 13511794849  | 摸瓜V2引擎  |
| 13530237028  | 摸瓜V2引擎  |
| 13531640999  | 摸瓜V2引擎  |
| 13537077355  | 摸瓜V2引擎  |
| 13542900088  | 摸瓜V2引擎  |
| 13554734833  | 摸瓜V2引擎  |
| 13556082977  | 摸瓜V2引擎  |
| 13560947659  | 摸瓜V2引擎  |
| 13570848997  | 摸瓜V2引擎  |
| 13574601114  | 摸瓜V2引擎  |
| 13589334659  | 摸瓜V2引擎  |
| 13590406567  | 摸瓜V2引擎  |
| 13599736507  | 摸瓜V2引擎  |
| 13599919798  | 摸瓜V2引擎  |
| 13615496167  | 摸瓜V2引擎  |
| 13617741714  | 摸瓜V2引擎  |
| 13625076216  | 摸瓜V2引擎  |
| 13634242480  | 摸瓜V2引擎  |
| 13650057021  | 摸瓜V2引擎  |
| 13656021119  | 摸瓜V2引擎  |
| 13657004997  | 摸瓜V2引擎  |
| 13667991284  | 摸瓜V2引擎  |
| 13669826154  | 摸瓜V2引擎  |
| 13669850977  | 摸瓜V2引擎  |
| 13675704700  | 摸瓜V2引擎  |
| 13675835435  | 摸瓜V2引擎  |
| 13675948706  | 摸瓜V2引擎  |
| 13682633578  | 摸瓜V2引擎  |
| 13682666759  | 摸瓜V2引擎  |
| 13683225666  | 摸瓜V2引擎  |
| 13685953855  | 摸瓜V2引擎  |
| 13687283103  | 摸瓜V2引擎  |
| 13691557109  | 摸瓜V2引擎  |
| 13691951717  | 摸瓜V2引擎  |
| 13692142141  | 摸瓜V2引擎  |
| 13697180887  | 摸瓜V2引擎  |
| 13699869797  | 摸瓜V2引擎  |
| 13713869378  | 摸瓜V2引擎  |
| 13713895835  | 摸瓜V2引擎  |
| 13714420245  | 摸瓜V2引擎  |
| 13714636533  | 摸瓜V2引擎  |
| 13723721226  | 摸瓜V2引擎  |
| 13750567158  | 摸瓜V2引擎  |
| 13751060758  | 摸瓜V2引擎  |
| 13755814471  | 摸瓜V2引擎  |
| 13760345378  | 摸瓜V2引擎  |
| 13774251588  | 摸瓜V2引擎  |
| 13788801623  | 摸瓜V2引擎  |
| 13789321188  | 摸瓜V2引擎  |
| 13789900224  | 摸瓜V2引擎  |
| 13790551234  | 摸瓜V2引擎  |
| 13798398589  | 摸瓜V2引擎  |
| 13799863997  | 摸瓜V2引擎  |
| 13805076056  | 摸瓜V2引擎  |
| 13809281578  | 摸瓜V2引擎  |
| 13864042859  | 摸瓜V2引擎  |
| 13911723846  | 摸瓜V2引擎  |
| 13916989656  | 摸瓜V2引擎  |
| 13925754686  | 摸瓜V2引擎  |
| 13950891887  | 摸瓜V2引擎  |
| 13954458026  | 摸瓜V2引擎  |
| 13984418900  | 摸瓜V2引擎  |
| 15001298335  | 摸瓜V2引擎  |
| 15073870677  | 摸瓜V2引擎  |
| 15800568668  | 摸瓜V2引擎  |
| 15801627230  | 摸瓜V2引擎  |
| 15811837155  | 摸瓜V2引擎  |
| 15814496556  | 摸瓜V2引擎  |
| 15815006383  | 摸瓜V2引擎  |
| 15815443535  | 摸瓜V2引擎  |
| 15875222466  | 摸瓜V2引擎  |
| 15880601077  | 摸瓜V2引擎  |
| 15889587272  | 摸瓜V2引擎  |
| 15905146004  | 摸瓜V2引擎  |
| 15911679607  | 摸瓜V2引擎  |
| 15951105879  | 摸瓜V2引擎  |
| 15962679272  | 摸瓜V2引擎  |
| 15977277174  | 摸瓜V2引擎  |
| 15999702789  | 摸瓜V2引擎  |
| 18701380196  | 摸瓜V2引擎  |
| 13366636936  | 摸瓜V2引擎  |
| 18718689362  | 摸瓜V2引擎  |
| 15873871833  | 摸瓜V2引擎  |
| 13552315502  | 摸瓜V2引擎  |
| 13717712609  | 摸瓜V2引擎  |
| 18289325866  | 摸瓜V2引擎  |
| 13751893776  | 摸瓜V2引擎  |
| 13422432246  | 摸瓜V2引擎  |
| 18608648530  | 摸瓜V2引擎  |
| 15000898079  | 摸瓜V2引擎  |
| 15817424205  | 摸瓜V2引擎  |
| 15681999090  | 摸瓜V2引擎  |
| 13896666258  | 摸瓜V2引擎  |
| 13681698482  | 摸瓜V2引擎  |
| 15570711605  | 摸瓜V2引擎  |
| 15899977266  | 摸瓜V2引擎  |
| 15018925756  | 摸瓜V2引擎  |
| 18758158778  | 摸瓜V2引擎  |
| 15811836450  | 摸瓜V2引擎  |
| 13417318189  | 摸瓜V2引擎  |
| 15257119224  | 摸瓜V2引擎  |
| 15586267028  | 摸瓜V2引擎  |
| 13886113114  | 摸瓜V2引擎  |
| 15327775395  | 摸瓜V2引擎  |
| 13694210008  | 摸瓜V2引擎  |
| 13716140748  | 摸瓜V2引擎  |
| 15201736612  | 摸瓜V2引擎  |
| 15170046198  | 摸瓜V2引擎  |
| 18969732658  | 摸瓜V2引擎  |
| 15107115580  | 摸瓜V2引擎  |
| 15088901960  | 摸瓜V2引擎  |
| 13212300164  | 摸瓜V2引擎  |
| 18602748061  | 摸瓜V2引擎  |
| 13727358394  | 摸瓜V2引擎  |
| 13544378151  | 摸瓜V2引擎  |
| 13711679614  | 摸瓜V2引擎  |
| 13535267074  | 摸瓜V2引擎  |
| 18627273443  | 摸瓜V2引擎  |
| 13762562271  | 摸瓜V2引擎  |
| 18716562415  | 摸瓜V2引擎  |
| 13983231935  | 摸瓜V2引擎  |
| 13424447948  | 摸瓜V2引擎  |
| 13728719333  | 摸瓜V2引擎  |
| 18868716522  | 摸瓜V2引擎  |
| 13808186252  | 摸瓜V2引擎  |
| 15608183376  | 摸瓜V2引擎  |
| 18780265461  | 摸瓜V2引擎  |
| 18657301902  | 摸瓜V2引擎  |
| 15328036056  | 摸瓜V2引擎  |
| 13717618648  | 摸瓜V2引擎  |
| 13466558750  | 摸瓜V2引擎  |
| 15928356665  | 摸瓜V2引擎  |
| 15803810075  | 摸瓜V2引擎  |
| 18603034070  | 摸瓜V2引擎  |
| 15058349527  | 摸瓜V2引擎  |
| 13551110238  | 摸瓜V2引擎  |
| 18681816011  | 摸瓜V2引擎  |
| 18699998939  | 摸瓜V2引擎  |
| 18743057575  | 摸瓜V2引擎  |
| 15198200049  | 摸瓜V2引擎  |
| 15156207009  | 摸瓜V2引擎  |
| 15673966072  | 摸瓜V2引擎  |
| 18658019002  | 摸瓜V2引擎  |
| 15995460194  | 摸瓜V2引擎  |
| 15821352296  | 摸瓜V2引擎  |
| 13524796179  | 摸瓜V2引擎  |
| 13235522999  | 摸瓜V2引擎  |
| 15166039217  | 摸瓜V2引擎  |
| 13162979460  | 摸瓜V2引擎  |
| 15801200046  | 摸瓜V2引擎  |
| 18688753385  | 摸瓜V2引擎  |
| 18627173918  | 摸瓜V2引擎  |
| 15982833246  | 摸瓜V2引擎  |
| 13100738115  | 摸瓜V2引擎  |
| 15999194485  | 摸瓜V2引擎  |
| 13718344635  | 摸瓜V2引擎  |
| 15860741389  | 摸瓜V2引擎  |
| 13520677618  | 摸瓜V2引擎  |
| 15010955036  | 摸瓜V2引擎  |
| 18681863881  | 摸瓜V2引擎  |
| 18603755606  | 摸瓜V2引擎  |
| 13011374222  | 摸瓜V2引擎  |
| 13589955178  | 摸瓜V2引擎  |
| 15611666996  | 摸瓜V2引擎  |
| 13510211905  | 摸瓜V2引擎  |
| 13826419279  | 摸瓜V2引擎  |
| 15944111112  | 摸瓜V2引擎  |
| 13817341272  | 摸瓜V2引擎  |
| 15260481229  | 摸瓜V2引擎  |
| 15969515233  | 摸瓜V2引擎  |
| 15903692234  | 摸瓜V2引擎  |
| 13651186558  | 摸瓜V2引擎  |
| 13676941998  | 摸瓜V2引擎  |
| 15960959321  | 摸瓜V2引擎  |
| 13657023137  | 摸瓜V2引擎  |
| 15060858221  | 摸瓜V2引擎  |
| 15220245437  | 摸瓜V2引擎  |
| 15960959585  | 摸瓜V2引擎  |
| 15060777704  | 摸瓜V2引擎  |
| 15871494077  | 摸瓜V2引擎  |
| 15278374434  | 摸瓜V2引擎  |
| 15268753155  | 摸瓜V2引擎  |
| 18676681297  | 摸瓜V2引擎  |
| 15292216266  | 摸瓜V2引擎  |
| 15179408523  | 摸瓜V2引擎  |
| 13650212165  | 摸瓜V2引擎  |
| 13172169888  | 摸瓜V2引擎  |
| 13850507433  | 摸瓜V2引擎  |
| 13728832595  | 摸瓜V2引擎  |
| 18750254740  | 摸瓜V2引擎  |
| 13510969558  | 摸瓜V2引擎  |
| 15576616552  | 摸瓜V2引擎  |
| 13677399886  | 摸瓜V2引擎  |
| 13710054171  | 摸瓜V2引擎  |
| 13128788787  | 摸瓜V2引擎  |
| 13651063008  | 摸瓜V2引擎  |
| 13761999047  | 摸瓜V2引擎  |
| 13155803009  | 摸瓜V2引擎  |
| 13575469173  | 摸瓜V2引擎  |
| 13383457770  | 摸瓜V2引擎  |
| 13716743141  | 摸瓜V2引擎  |
| 13556276767  | 摸瓜V2引擎  |
| 13671904111  | 摸瓜V2引擎  |
| 15259245585  | 摸瓜V2引擎  |
| 15160047932  | 摸瓜V2引擎  |
| 13162325010  | 摸瓜V2引擎  |
| 13697464845  | 摸瓜V2引擎  |
| 15083625566  | 摸瓜V2引擎  |
| 13559479544  | 摸瓜V2引擎  |
| 13159266984  | 摸瓜V2引擎  |
| 15150156457  | 摸瓜V2引擎  |
| 13707568123  | 摸瓜V2引擎  |
| 15257829058  | 摸瓜V2引擎  |
| 13410128940  | 摸瓜V2引擎  |
| 13699890874  | 摸瓜V2引擎  |
| 18751123147  | 摸瓜V2引擎  |
| 18718577257  | 摸瓜V2引擎  |
| 15910486275  | 摸瓜V2引擎  |
| 13482287776  | 摸瓜V2引擎  |
| 13117383239  | 摸瓜V2引擎  |
| 15999939939  | 摸瓜V2引擎  |
| 13751212246  | 摸瓜V2引擎  |
| 13691600682  | 摸瓜V2引擎  |
| 18750615367  | 摸瓜V2引擎  |
| 18786811035  | 摸瓜V2引擎  |
| 18627123396  | 摸瓜V2引擎  |
| 18750255874  | 摸瓜V2引擎  |
| 15990499877  | 摸瓜V2引擎  |
| 13816120484  | 摸瓜V2引擎  |
| 13145991588  | 摸瓜V2引擎  |
| 18755333217  | 摸瓜V2引擎  |
| 15177089366  | 摸瓜V2引擎  |
| 13459633077  | 摸瓜V2引擎  |
| 15160757578  | 摸瓜V2引擎  |
| 15019232247  | 摸瓜V2引擎  |
| 13681752655  | 摸瓜V2引擎  |
| 13761512831  | 摸瓜V2引擎  |
| 15821056189  | 摸瓜V2引擎  |
| 15008902920  | 摸瓜V2引擎  |
| 13683597691  | 摸瓜V2引擎  |
| 15021398621  | 摸瓜V2引擎  |
| 18807466399  | 摸瓜V2引擎  |
| 13960933625  | 摸瓜V2引擎  |
| 15160048094  | 摸瓜V2引擎  |
| 15108450199  | 摸瓜V2引擎  |
| 13860420171  | 摸瓜V2引擎  |
| 18801695839  | 摸瓜V2引擎  |
| 13246616285  | 摸瓜V2引擎  |
| 13538882789  | 摸瓜V2引擎  |
| 13818798170  | 摸瓜V2引擎  |
| 15811166234  | 摸瓜V2引擎  |
| 13667906844  | 摸瓜V2引擎  |
| 13459516157  | 摸瓜V2引擎  |
| 13790635807  | 摸瓜V2引擎  |
| 15125659339  | 摸瓜V2引擎  |
| 18608735968  | 摸瓜V2引擎  |
| 13995698078  | 摸瓜V2引擎  |
| 13145838885  | 摸瓜V2引擎  |
| 13767519896  | 摸瓜V2引擎  |
| 13695044579  | 摸瓜V2引擎  |
| 13266668834  | 摸瓜V2引擎  |
| 18611059369  | 摸瓜V2引擎  |
| 15866784614  | 摸瓜V2引擎  |
| 13688857422  | 摸瓜V2引擎  |
| 15527795902  | 摸瓜V2引擎  |
| 15527795901  | 摸瓜V2引擎  |
| 15253168708  | 摸瓜V2引擎  |
| 15865318642  | 摸瓜V2引擎  |
| 16042886949  | 摸瓜V2引擎  |
| 15816125959  | 摸瓜V2引擎  |
| 15909465885  | 摸瓜V2引擎  |
| 13681150469  | 摸瓜V2引擎  |
| 15545601110  | 摸瓜V2引擎  |
| 13391910755  | 摸瓜V2引擎  |
| 15160071317  | 摸瓜V2引擎  |
| 13675712818  | 摸瓜V2引擎  |
| 13552232910  | 摸瓜V2引擎  |
| 15101517758  | 摸瓜V2引擎  |
| 13223380751  | 摸瓜V2引擎  |
| 13265726544  | 摸瓜V2引擎  |
| 15189732080  | 摸瓜V2引擎  |
| 13533367239  | 摸瓜V2引擎  |
| 18720038211  | 摸瓜V2引擎  |
| 15227789200  | 摸瓜V2引擎  |
| 15059162411  | 摸瓜V2引擎  |
| 13178356956  | 摸瓜V2引擎  |
| 13552197909  | 摸瓜V2引擎  |
| 13020191613  | 摸瓜V2引擎  |
| 13725932528  | 摸瓜V2引擎  |
| 15120944941  | 摸瓜V2引擎  |
| 13718370891  | 摸瓜V2引擎  |
| 15860839605  | 摸瓜V2引擎  |
| 15800289855  | 摸瓜V2引擎  |
| 15985977003  | 摸瓜V2引擎  |
| 15068772274  | 摸瓜V2引擎  |
| 15888277683  | 摸瓜V2引擎  |
| 13135320112  | 摸瓜V2引擎  |
| 13468155807  | 摸瓜V2引擎  |
| 18659992255  | 摸瓜V2引擎  |
| 13631354179  | 摸瓜V2引擎  |
| 13714188466  | 摸瓜V2引擎  |
| 15975192462  | 摸瓜V2引擎  |
| 13208921209  | 摸瓜V2引擎  |
| 13645922829  | 摸瓜V2引擎  |
| 13302690386  | 摸瓜V2引擎  |
| 13467880101  | 摸瓜V2引擎  |
| 15859243634  | 摸瓜V2引擎  |
| 18913107009  | 摸瓜V2引擎  |
| 15205150189  | 摸瓜V2引擎  |
| 15807902658  | 摸瓜V2引擎  |
| 13517904441  | 摸瓜V2引擎  |
| 13770707873  | 摸瓜V2引擎  |
| 18789820038  | 摸瓜V2引擎  |
| 15860781673  | 摸瓜V2引擎  |
| 13053980517  | 摸瓜V2引擎  |
| 15169547788  | 摸瓜V2引擎  |
| 15801187688  | 摸瓜V2引擎  |
| 13688941186  | 摸瓜V2引擎  |
| 15215130930  | 摸瓜V2引擎  |
| 13122660010  | 摸瓜V2引擎  |
| 15901425089  | 摸瓜V2引擎  |
| 15062278011  | 摸瓜V2引擎  |
| 13530093260  | 摸瓜V2引擎  |
| 13797575744  | 摸瓜V2引擎  |
| 13621126591  | 摸瓜V2引擎  |
| 15259243997  | 摸瓜V2引擎  |
| 13121939703  | 摸瓜V2引擎  |
| 15362415378  | 摸瓜V2引擎  |
| 13973251117  | 摸瓜V2引擎  |
| 13707518698  | 摸瓜V2引擎  |
| 13668077011  | 摸瓜V2引擎  |
| 13560834241  | 摸瓜V2引擎  |
| 13532736776  | 摸瓜V2引擎  |
| 13791823760  | 摸瓜V2引擎  |
| 15079028993  | 摸瓜V2引擎  |
| 15828210768  | 摸瓜V2引擎  |
| 13632701190  | 摸瓜V2引擎  |
| 13310122326  | 摸瓜V2引擎  |
| 13827203280  | 摸瓜V2引擎  |
| 13790242560  | 摸瓜V2引擎  |
| 13413819899  | 摸瓜V2引擎  |
| 15887078668  | 摸瓜V2引擎  |
| 13655000884  | 摸瓜V2引擎  |
| 18759210823  | 摸瓜V2引擎  |
| 13696870702  | 摸瓜V2引擎  |
| 15327106013  | 摸瓜V2引擎  |
| 13713884827  | 摸瓜V2引擎  |
| 13651276266  | 摸瓜V2引擎  |
| 15101595957  | 摸瓜V2引擎  |
| 18603577634  | 摸瓜V2引擎  |
| 18766373789  | 摸瓜V2引擎  |
| 13519892902  | 摸瓜V2引擎  |
| 18720037058  | 摸瓜V2引擎  |
| 18626178707  | 摸瓜V2引擎  |
| 13973848836  | 摸瓜V2引擎  |
| 13352626289  | 摸瓜V2引擎  |
| 13125135185  | 摸瓜V2引擎  |
| 15081161115  | 摸瓜V2引擎  |
| 13071284711  | 摸瓜V2引擎  |
| 13913471015  | 摸瓜V2引擎  |
| 15011916195  | 摸瓜V2引擎  |
| 15271079593  | 摸瓜V2引擎  |
| 13652411655  | 摸瓜V2引擎  |
| 13917340054  | 摸瓜V2引擎  |
| 13237560159  | 摸瓜V2引擎  |
| 13521113240  | 摸瓜V2引擎  |
| 13824358180  | 摸瓜V2引擎  |
| 15677256897  | 摸瓜V2引擎  |
| 13874383940  | 摸瓜V2引擎  |
| 15520714182  | 摸瓜V2引擎  |
| 13219332228  | 摸瓜V2引擎  |
| 18858735747  | 摸瓜V2引擎  |
| 18910958280  | 摸瓜V2引擎  |
| 13312924991  | 摸瓜V2引擎  |
| 13476023749  | 摸瓜V2引擎  |
| 15262493531  | 摸瓜V2引擎  |
| 18955865559  | 摸瓜V2引擎  |
| 18721756801  | 摸瓜V2引擎  |
| 13196786975  | 摸瓜V2引擎  |
| 13950108349  | 摸瓜V2引擎  |
| 15932849797  | 摸瓜V2引擎  |
| 13453205113  | 摸瓜V2引擎  |
| 13418784295  | 摸瓜V2引擎  |
| 13107059955  | 摸瓜V2引擎  |
| 13913841440  | 摸瓜V2引擎  |
| 13755557188  | 摸瓜V2引擎  |
| 15573837711  | 摸瓜V2引擎  |
| 18688963126  | 摸瓜V2引擎  |
| 13530487772  | 摸瓜V2引擎  |
| 13664195011  | 摸瓜V2引擎  |
| 15073147216  | 摸瓜V2引擎  |
| 13208258358  | 摸瓜V2引擎  |
| 15118812644  | 摸瓜V2引擎  |
| 15973793985  | 摸瓜V2引擎  |
| 13605049658  | 摸瓜V2引擎  |
| 15225909162  | 摸瓜V2引擎  |
| 15261389171  | 摸瓜V2引擎  |
| 18688430388  | 摸瓜V2引擎  |
| 13637479737  | 摸瓜V2引擎  |
| 13762824073  | 摸瓜V2引擎  |
| 18259230869  | 摸瓜V2引擎  |
| 13537690947  | 摸瓜V2引擎  |
| 13418938912  | 摸瓜V2引擎  |
| 18759963979  | 摸瓜V2引擎  |
| 13175074757  | 摸瓜V2引擎  |
| 15259252038  | 摸瓜V2引擎  |
| 15960259230  | 摸瓜V2引擎  |
| 13599905473  | 摸瓜V2引擎  |
| 13917433611  | 摸瓜V2引擎  |
| 13510176318  | 摸瓜V2引擎  |
| 15918888573  | 摸瓜V2引擎  |
| 15029404025  | 摸瓜V2引擎  |
| 18750751753  | 摸瓜V2引擎  |
| 13889444328  | 摸瓜V2引擎  |
| 13781238894  | 摸瓜V2引擎  |
| 13113051472  | 摸瓜V2引擎  |
| 13423205670  | 摸瓜V2引擎  |
| 13725516608  | 摸瓜V2引擎  |
| 13875448369  | 摸瓜V2引擎  |
| 15112886328  | 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: CN=xiaolin, OU=xiaolin, O=x, L=x, ST=x, C=086 签名算法: rsassa\_pkcs1v15 有效期自: 2024-08-02 03:12:37+00:00 有效期至: 2049-07-27 03:12:37+00:00 发行人: CN=xiaolin, OU=xiaolin, O=x, L=x, ST=x, C=086 序列号: 0x1 哈希算法: sha256 md5值: 8e0439a03063a55263520cb2fcb42ace sha1值: 1252d824bc38c3a15d74462a265f2e2dca01113c sha256值: d5a452253dfd231ffd840e7dd810bcb000f004eea65e8a47dbc87b1c65b40e2d sha512值: 01391cd6d294d9c1765f8a69f09985d7fc9d89e8b8d3b8c9c526a3bc091d223572e5b2ebc8fedc0c378dd51085a8805be2ca161278adffafbdd955744e3c8ea5 公钥算法: rsa 密钥长度: 2048 指纹: b07afd570bf419039632e204c5ba2a6b52016feffdb62040b81ee3be63c474bb**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "app\_name\_user" : "树拍易购"  |
| "chat\_team\_need\_authentication" : "需要身份验证"  |
| "library\_roundedimageview\_author" : "Vince Mi"  |
| "library\_roundedimageview\_authorWebsite" : "https://github.com/vinc3m1"  |
| "loading\_go\_auth" : "Go to Alipay for authorization"  |
| "team\_session\_pin" : "聊天置顶"  |
| "url\_auth" : "Url Auth Setting"  |
| "loading\_go\_auth" : "前往支付寶授權"  |
| "loading\_go\_auth" : "去支付寶授權"  |
| "loading\_go\_auth" : "去支付宝授权"  |
| "chat\_team\_need\_authentication" : "Needs Identify"  |
| "team\_session\_pin" : "Sticky on Top"  |

## **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\_CLIPBOARD\_IN\_BACKGROUND | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_CLIPBOARD\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.MANAGE\_EXTERNAL\_STORAGE | 危险 | 允许应用程序广泛访问范围存储中的外部存储 | 允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用 |
| android.permission.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| com.spyg.yigou.mall.permission.JPUSH\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.USE\_FULL\_SCREEN\_INTENT | 正常 |  | 针对想要使用通知全屏意图的 Build.VERSION\_CODES.Q 的应用程序是必需的 |
| 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.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\_AUDIO | 未知 | Unknown permission | Unknown permission from android reference |
| 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.READ\_PRIVILEGED\_PHONE\_STATE | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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.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.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.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\_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.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.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\_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.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.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\_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.ACCESS\_MEDIA\_LOCATION | 危险 | 访问的任何地理位置 | 允许应用程序访问的任何地理位置持久保存在用户的共享集合 |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.ACCESS\_BACKGROUND\_LOCATION | 危险 | 后台访问位置 | 允许应用程序在后台访问位置 |
| android.permission.ACCESS\_NOTIFICATION\_POLICY | 正常 |  | 希望访问通知策略的应用程序的标记权限。 |
| 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.BIND\_NOTIFICATION\_LISTENER\_SERVICE | 合法 |  | NotificationListenerService 必须要求,以确保只有系统可以绑定到它 |
| 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\_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.BLUETOOTH\_ADMIN | 正常 | 蓝牙管理 | 允许应用程序发现和配对蓝牙设备。  |
| 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.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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| 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 |
| com.spyg.yigou.mall.permission.MIPUSH\_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.vivo.notification.permission.BADGE\_ICON | 未知 | Unknown permission | Unknown permission from android reference |
| com.hihonor.android.launcher.permission.CHANGE\_BADGE | 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.spyg.yigou.mall.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| com.spyg.yigou.mall.permission.PUSH\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.gms.permission.AD\_ID | 未知 | Unknown permission | Unknown permission from android reference |
| com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| com.asus.permission.READ\_SDID\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| freemme.permission.msa | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BLUETOOTH\_CONNECT | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.ghsc.yigou.live.ui.MainActivity | **Schemes**: um.666bef77cac2a664de4ac44c://,  |

**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。**