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

**翰林优商（ 2.4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 | 翰林优商 |
| 版本 | 2.4 |
| 包名 | com.hanlingyoushang |
| 域名线索 | 117条 |
| URL线索 | 168条 |
| APP图标 |  |
| 分析日期 | 2025年7月1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 | base.apk |
| 文件大小 | 33.14MB |
| MD5值 | 1e36a824636c56a6556311340258a4b5 |
| SHA1值 | 11dd7a728f671d09ffd5d167e05235800b48c416 |
| SHA256值 | 49a2c22203547ce978f4d557a26932793475b2f7070b6697dcab6b0afdb08621 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 翰林优商 |
| 包名 | com.hanlingyoushang |
| 主活动Activity | com.hanlingyoushang.MainActivity |
| 安卓版本名称 | 2.4 |
| 安卓版本 | 10 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| spare-beiaei.fleast.cn | IP: 119.188.210.197  所属国家: China  地区: Shandong  城市: Jinan |
| api.hzsanjiaomao.com | IP: 120.55.191.200  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| apps.samsung.com | IP: 103.254.189.69  所属国家: China  地区: Beijing  城市: Beijing |
| www.chengzijianzhan.com | IP: 42.81.213.230  所属国家: China  地区: Tianjin  城市: Tianjin |
| github.com | IP: 20.205.243.166  所属国家: United States of America  地区: Washington  城市: Redmond |
| crbug.com | IP: 216.239.32.29  所属国家: United States of America  地区: California  城市: Mountain View |
| ip.taobao.com | IP: 203.119.144.26  所属国家: China  地区: Beijing  城市: Beijing |
| cdn-adn-https.rayjump.com | IP: 42.81.147.71  所属国家: China  地区: Tianjin  城市: Tianjin |
| wx.tenpay.com | IP: 121.51.73.119  所属国家: China  地区: Guangdong  城市: Shenzhen |
| www.ipadview.com | IP: 47.96.135.117  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| 10.138.32.176 | IP: 10.138.32.176  所属国家: -  地区: -  城市: - |
| www.ibookstar.com | IP: 121.40.40.140  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| ucc.umeng.com | IP: 203.119.169.175  所属国家: China  地区: Beijing  城市: Beijing |
| soft.tbs.imtt.qq.com | IP: 121.51.175.60  所属国家: China  地区: Guangdong  城市: Shenzhen |
| alogus.umeng.com | IP: 223.109.148.130  所属国家: China  地区: Beijing  城市: Beijing |
| union.baidu.com | IP: 111.206.208.169  所属国家: China  地区: Beijing  城市: Beijing |
| mdc.html5.qq.com | IP: 175.27.9.46  所属国家: China  地区: Beijing  城市: Beijing |
| tbsrecovery.imtt.qq.com | IP: 109.244.244.237  所属国家: China  地区: Beijing  城市: Beijing |
| h5iad.sp-card.com | IP: 124.239.227.225  所属国家: China  地区: Hebei  城市: Langfang |
| 47.97.36.81 | IP: 47.97.36.81  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| upl.baidu.com | IP: 111.206.208.71  所属国家: China  地区: Beijing  城市: Beijing |
| www.samsungapps.com | IP: 52.31.24.56  所属国家: Ireland  地区: Dublin  城市: Dublin |
| hb.rayjump.com | IP: 123.57.65.212  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| play.google.com | IP: 172.217.160.78  所属国家: United States of America  地区: California  城市: Mountain View |
| spare.fleast.cn | IP: 119.188.210.197  所属国家: China  地区: Shandong  城市: Jinan |
| cfg.imtt.qq.com | IP: 109.244.173.227  所属国家: China  地区: Beijing  城市: Beijing |
| verify.cmpassport.com | IP: 120.232.169.172  所属国家: China  地区: Guangdong  城市: Guangzhou |
| lazy.rayjump.com | IP: 150.158.228.37  所属国家: China  地区: Beijing  城市: Beijing |
| debugx5.qq.com | IP: 175.27.9.46  所属国家: China  地区: Beijing  城市: Beijing |
| m.sigmob.com | IP: 39.103.12.64  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| beibei.fleast.cn | IP: 119.188.210.197  所属国家: China  地区: Shandong  城市: Jinan |
| opencloud.wostore.cn | IP: 210.22.123.92  所属国家: China  地区: Shanghai  城市: Shanghai |
| dc.sigmob.cn | IP: 112.126.7.24  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| sdk.e.qq.com | IP: 119.147.13.93  所属国家: China  地区: Guangdong  城市: Shenzhen |
| app.qubiankeji.com | IP: 47.99.59.103  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| androidquery.appspot.com | IP: 108.160.170.52  所属国家: United States of America  地区: California  城市: San Francisco |
| developer.umeng.com | IP: 59.82.29.249  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| whatwg.org | IP: 165.227.248.76  所属国家: United States of America  地区: New Jersey  城市: Clifton |
| errlogos.umeng.com | IP: 47.246.110.96  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| js-ad.a.yximgs.com | IP: 1.180.10.45  所属国家: China  地区: Nei Mongol  城市: Baotou |
| spare-bei.fleast.cn | IP: 119.188.210.197  所属国家: China  地区: Shandong  城市: Jinan |
| detect.rayjump.com | IP: 18.235.19.204  所属国家: United States of America  地区: Virginia  城市: Ashburn |
| api-sdk.brily.cn | IP: 120.78.207.132  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| ulogs.umengcloud.com | IP: 223.109.148.177  所属国家: China  地区: Beijing  城市: Beijing |
| appspe.qubiankeji.com | IP: 47.99.59.103  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| utoken.umeng.com | IP: 218.91.197.67  所属国家: China  地区: Jiangsu  城市: Nantong |
| pms.mb.qq.com | IP: 109.244.173.227  所属国家: China  地区: Beijing  城市: Beijing |
| hybird.rayjump.com | IP: 42.81.147.71  所属国家: China  地区: Tianjin  城市: Tianjin |
| www.google.com | IP: 108.160.169.174  所属国家: United States of America  地区: California  城市: San Francisco |
| brain.baidu.com | IP: 110.242.69.34  所属国家: China  地区: Hebei  城市: Baoding |
| api.twitter.com | IP: 43.226.16.8  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| boardy.huanqiu.com | IP: 220.181.158.241  所属国家: China  地区: Beijing  城市: Beijing |
| adservice.sigmob.cn | IP: 47.94.254.145  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| ai.baidu.com | IP: 110.242.69.34  所属国家: China  地区: Hebei  城市: Baoding |
| yuyin.baidu.com | IP: 153.3.236.85  所属国家: China  地区: Jiangsu  城市: Nanjing |
| www.qq.com | IP: 175.27.8.138  所属国家: China  地区: Beijing  城市: Beijing |
| api.ads66.com | IP: 120.79.169.103  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| alogsus.umeng.com | IP: 223.109.148.178  所属国家: China  地区: Beijing  城市: Beijing |
| pslog.umeng.com | IP: 59.82.31.95  所属国家: China  地区: Beijing  城市: Beijing |
| e.189.cn | IP: 42.123.76.65  所属国家: China  地区: Beijing  城市: Beijing |
| ai.login.umeng.com | IP: 59.82.31.210  所属国家: China  地区: Beijing  城市: Beijing |
| ulogs.umeng.com | IP: 223.109.148.130  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 |
| dapi.zjbdl.cn | IP: 116.62.108.133  所属国家: China  地区: Beijing  城市: Beijing |
| www.facebook.com | IP: 162.125.18.129  所属国家: United States of America  地区: California  城市: San Francisco |
| dapi.sjmbdl.cn | 没有服务器地理信息. |
| log.tbs.qq.com | IP: 109.244.244.32  所属国家: China  地区: Beijing  城市: Beijing |
| passport.kuaishou.com | IP: 103.102.200.8  所属国家: China  地区: Beijing  城市: Beijing |
| nisportal.10010.com | IP: 123.125.99.214  所属国家: China  地区: Beijing  城市: Beijing |
| spare-aei.fleast.cn | IP: 119.188.210.197  所属国家: China  地区: Shandong  城市: Jinan |
| audiotest.baidu.com | IP: 180.101.49.122  所属国家: China  地区: Jiangsu  城市: Nanjing |
| d.alipay.com | IP: 203.209.245.74  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| www.w3.org | IP: 128.30.52.100  所属国家: United States of America  地区: Massachusetts  城市: Cambridge |
| vop.baidu.com | IP: 111.206.209.68  所属国家: China  地区: Beijing  城市: Beijing |
| eco.taobao.com | IP: 59.82.29.142  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| open.e.kuaishou.com | IP: 103.107.219.5  所属国家: China  地区: Beijing  城市: Beijing |
| ip.adipman.net | IP: 47.96.139.120  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| voicelog.xinliangxiang.com | IP: 118.31.53.183  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| mtg-native.rayjump.com | IP: 103.254.188.50  所属国家: China  地区: Beijing  城市: Beijing |
| configure.rayjump.com | IP: 150.158.239.85  所属国家: China  地区: Beijing  城市: Beijing |
| vse.baidu.com | IP: 111.206.208.71  所属国家: China  地区: Beijing  城市: Beijing |
| tools.ibookeee.com | IP: 120.55.60.77  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| d1tru86qrby720.cloudfront.net | IP: 18.65.214.101  所属国家: United States of America  地区: Washington  城市: Seattle |
| debugtbs.qq.com | IP: 175.27.9.46  所属国家: China  地区: Beijing  城市: Beijing |
| fleast.cn | IP: 110.42.6.7  所属国家: China  地区: Zhejiang  城市: Ningbo |
| cpro.baidustatic.com | IP: 119.167.254.35  所属国家: China  地区: Shandong  城市: Qingdao |
| check.rayjump.com | IP: 150.158.228.37  所属国家: China  地区: Beijing  城市: Beijing |
| saas.qubiankeji.com | IP: 121.41.30.96  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| rp.ipadview.com | IP: 121.40.56.194  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| adput.qubiankeji.com | IP: 47.99.59.103  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| errlog.umeng.com | IP: 223.109.148.180  所属国家: China  地区: Beijing  城市: Beijing |
| www.toutiaopage.com | IP: 42.81.213.227  所属国家: China  地区: Tianjin  城市: Tianjin |
| i.snssdk.com | IP: 220.181.132.229  所属国家: China  地区: Beijing  城市: Beijing |
| apps.oceanengine.com | IP: 42.81.213.226  所属国家: China  地区: Tianjin  城市: Tianjin |
| h5.ads66.com | IP: 111.225.217.129  所属国家: China  地区: Hebei  城市: Langfang |
| api-e189.21cn.com | IP: 222.93.106.185  所属国家: China  地区: Jiangsu  城市: Suzhou |
| mqqad.html5.qq.com | IP: 0.0.0.1  所属国家: -  地区: -  城市: - |
| voicefront.xinliangxiang.com | IP: 118.31.53.183  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| 211.151.146.65 | IP: 211.151.146.65  所属国家: China  地区: Beijing  城市: Beijing |
| schemas.microsoft.com | IP: 13.107.246.49  所属国家: Netherlands  地区: Noord-Holland  城市: Amsterdam |
| spare-beibei.fleast.cn | IP: 119.188.210.197  所属国家: China  地区: Shandong  城市: Jinan |
| analytics.rayjump.com | IP: 182.92.120.219  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| aip.baidubce.com | IP: 111.206.210.12  所属国家: China  地区: Beijing  城市: Beijing |
| policy.rayjump.com | IP: 150.158.228.37  所属国家: China  地区: Beijing  城市: Beijing |
| net.rayjump.com | IP: 39.107.66.26  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| plbslog.umeng.com | IP: 36.156.202.73  所属国家: China  地区: Beijing  城市: Beijing |
| sdk.hzsanjiaomao.com | IP: 124.239.227.227  所属国家: China  地区: Hebei  城市: Langfang |
| wap.cmpassport.com | IP: 120.197.235.27  所属国家: China  地区: Guangdong  城市: Guangzhou |
| s3-us-west-2.amazonaws.com | IP: 52.218.217.168  所属国家: United States of America  地区: Oregon  城市: Portland |
| static.yximgs.com | IP: 125.39.223.225  所属国家: China  地区: Tianjin  城市: Tianjin |
| news.fliduo.cn | IP: 116.62.108.133  所属国家: China  地区: Beijing  城市: Beijing |
| id6.me | IP: 42.123.77.138  所属国家: China  地区: Beijing  城市: Beijing |
| sf6-ttcdn-tos.pstatp.com | IP: 42.81.54.250  所属国家: China  地区: Tianjin  城市: Tianjin |
| voiceapi.xinliangxiang.com | IP: 118.31.53.183  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| graph.facebook.com | IP: 108.160.166.42  所属国家: United States of America  地区: California  城市: San Francisco |
| px-intl.ucweb.com | IP: 157.185.188.1  所属国家: United States of America  地区: California  城市: Monrovia |
| gist.github.com | IP: 243.185.187.39  所属国家: -  地区: -  城市: - |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| 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://github.com/lingochamp/FileDownloader/wiki/filedownloader.properties | com/kwai/filedownloader/services/a.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/ks\_so-appStatusArm64v8aRelease-3.3.14.apk | com/kwad/sdk/collector/d.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/ks\_so-appStatusArmeabiv7aRelease-3.3.14.apk | com/kwad/sdk/collector/d.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/ks\_so-exceptionArm64v8aRelease-3.3.23.apk | com/kwad/sdk/crash/f.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/ks\_so-exceptionArmeabiv7aRelease-3.3.23.apk | com/kwad/sdk/crash/f.java |
| http://apps.samsung.com/appquery/appDetail.as?appId= | com/kwad/sdk/utils/d.java |
| https://open.e.kuaishou.com/rest/e/v3/open/sdk2 | com/kwad/sdk/api/loader/v.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/so/ks\_so-kwaiPlayerArm64v8aRelease-3.3.20.apk | com/kwad/sdk/core/video/kwai/e.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/so/ks\_so-kwaiPlayerArmeabiv7aRelease-3.3.20.apk | com/kwad/sdk/core/video/kwai/e.java |
| http://%s:%d/%s | com/kwad/sdk/core/videocache/f.java |
| https://github.com/danikula/AndroidVideoCache/issues/43. | com/kwad/sdk/core/videocache/h.java |
| https://github.com/danikula/AndroidVideoCache/issues. | com/kwad/sdk/core/videocache/h.java |
| https://github.com/danikula/AndroidVideoCache/issues/88. | com/kwad/sdk/core/videocache/h.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/offline\_components/adLive/ks\_so-adLiveNoSoRelease-3.3.26.1-f20890.apk | com/kwad/components/offline/adLive/a.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/adLive/3.3.26.1/ks\_so-adLiveArm64v8aRelease-3.3.26.1.apk | com/kwad/components/offline/adLive/kwai/a.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/adLive/3.3.26.1/ks\_so-adLiveArmeabiv7aRelease-3.3.26.1.apk | com/kwad/components/offline/adLive/kwai/a.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/offline\_components/tk/ks\_so-tachikomaNoSoRelease-3.3.27.1.apk | com/kwad/components/offline/tk/a.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/tachikoma/3.3.24.2/ks\_so-tachikomaLiteArm64v8aRelease-3.3.24.2.apk | com/kwad/components/offline/tk/a/a.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/tachikoma/3.3.24.2/ks\_so-tachikomaArm64v8aRelease-3.3.24.2.apk | com/kwad/components/offline/tk/a/a.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/tachikoma/3.3.24.2/ks\_so-tachikomaLiteArmeabiv7aRelease-3.3.24.2.apk | com/kwad/components/offline/tk/a/a.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/tachikoma/3.3.24.2/ks\_so-tachikomaArmeabiv7aRelease-3.3.24.2.apk | com/kwad/components/offline/tk/a/a.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/offline\_components/obiwan/ks\_so-obiwanNoSoRelease-3.3.24.3.apk | com/kwad/components/offline/obiwan/a.java |
| https://passport.kuaishou.com/account-h5/login?smallWebview=true&sid=kuaishou.unioncontent.wallpaper | com/kwad/components/ct/b/a.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/wallpaper/kwai\_wallpaper\_plugin\_1.4.apk | com/kwad/components/ct/wallpaper/c/b.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/wallpaper/kwai\_wallpaper\_plugin\_1.5.apk | com/kwad/components/ct/wallpaper/c/b.java |
| https://static.yximgs.com/udata/pkg/KSAdSDK/ksad\_page\_loading\_data\_limit\_error.png | com/kwad/components/ct/tube/view/EpisodeChooseLoadingView.java |
| https://static.yximgs.com/udata/pkg/KSAdSDK/ksad\_no\_video\_img.png | com/kwad/components/ct/tube/view/EpisodeChooseLoadingView.java |
| https://static.yximgs.com/udata/pkg/KSAdSDK/ksad\_page\_loading\_data\_error.png | com/kwad/components/ct/tube/view/EpisodeChooseLoadingView.java |
| https://static.yximgs.com/udata/pkg/KSAdSDK/ksad\_no\_data\_img.png | com/kwad/components/ct/tube/view/EpisodeChooseLoadingView.java |
| https://static.yximgs.com/udata/pkg/KSAdSDK/ksad\_page\_loading\_data\_limit\_error.png | com/kwad/components/ct/widget/KSPageLoadingView.java |
| https://static.yximgs.com/udata/pkg/KSAdSDK/ksad\_no\_video\_img.png | com/kwad/components/ct/widget/KSPageLoadingView.java |
| https://static.yximgs.com/udata/pkg/KSAdSDK/ksad\_page\_loading\_data\_error.png | com/kwad/components/ct/widget/KSPageLoadingView.java |
| https://static.yximgs.com/udata/pkg/KSAdSDK/ksad\_no\_data\_img.png | com/kwad/components/ct/widget/KSPageLoadingView.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/ks\_so-webpArm64v8aRelease-3.3.9.apk | com/kwad/components/ct/a/c.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/ks\_so-webpArmeabiv7aRelease-3.3.9.apk | com/kwad/components/ct/a/c.java |
| https://js-ad.a.yximgs.com/kos/nlav10933/ksad\_profile\_header\_bg.png | com/kwad/components/ct/profile/home/b/c.java |
| https://static.yximgs.com/udata/pkg/KSAdSDK/coupon/ksad\_coupon\_entry\_status\_3.webp | com/kwad/components/ct/coupon/entry/CouponEntryContainer.java |
| https://static.yximgs.com/udata/pkg/KSAdSDK/coupon/ksad\_coupon\_entry\_status\_2.webp | com/kwad/components/ct/coupon/entry/CouponEntryContainer.java |
| https://static.yximgs.com/udata/pkg/KSAdSDK/coupon/ksad\_coupon\_entry\_status\_1.webp | com/kwad/components/ct/coupon/entry/CouponEntryContainer.java |
| https://static.yximgs.com/udata/pkg/KSAdSDK/coupon/ksad\_coupon\_entry\_status\_4.webp | com/kwad/components/ct/coupon/entry/CouponEntryContainer.java |
| https://static.yximgs.com/udata/pkg/KSAdSDK/coupon/ksad\_coupon\_entry\_status\_0.webp | com/kwad/components/ct/coupon/entry/CouponEntryContainer.java |
| https://h5.ads66.com/ | com/duoyou/task/pro/b/a.java |
| https://h5.ads66.com/index.php/click/log | com/duoyou/task/pro/b/a.java |
| https://api.ads66.com/index.php/cpa/play | com/duoyou/task/pro/b/a.java |
| https://h5.ads66.com/ball | com/duoyou/task/pro/d/e.java |
| https://api.ads66.com/api/list | com/duoyou/task/pro/g/d.java |
| https://h5.ads66.com/index.php/tasks | com/duoyou/task/pro/g/d.java |
| https://wx.tenpay.com | com/duoyou/task/sdk/PlayGameActivity.java |
| https://h5.ads66.com/index.php/index/init | com/duoyou/task/sdk/PlayGameActivity.java |
| https://api.ads66.com//api/recommends | com/duoyou/task/sdk/view/dialog/ExitRecommendDialog.java |
| https://api.ads66.com/api/list | com/duoyou/task/openapi/DyAdApi.java |
| https://h5.ads66.com/index.php/tasks | com/duoyou/task/openapi/DyAdApi.java |
| http://wap.cmpassport.com/resources/html/contract.html | com/cmic/sso/sdk/activity/LoginAuthActivity.java |
| https://e.189.cn/sdk/agreement/detail.do | com/cmic/sso/sdk/activity/LoginAuthActivity.java |
| https://opencloud.wostore.cn/authz/resource/html/disclaimer.html?fromsdk=true | com/cmic/sso/sdk/activity/LoginAuthActivity.java |
| https://eco.taobao.com/router/rest | com/mobile/auth/BuildConfig.java |
| https://opencloud.wostore.cn/authz/resource/html/disclaimer.html?fromsdk=true | com/mobile/auth/q/a.java |
| https://wap.cmpassport.com/resources/html/contract.html | com/mobile/auth/o/d.java |
| https://api-e189.21cn.com/gw/client/accountMsg.do | com/mobile/auth/c/d.java |
| https://wap.cmpassport.com/resources/html/contract.html | com/mobile/auth/gatewayauth/Constant.java |
| https://e.189.cn/sdk/agreement/detail.do?isWap=true&hidetop=true&appKey=8138111118 | com/mobile/auth/gatewayauth/Constant.java |
| https://opencloud.wostore.cn/authz/resource/html/disclaimer.html?fromsdk=true | com/mobile/auth/gatewayauth/Constant.java |
| https://id6.me/auth/preauth.do | com/mobile/auth/d/a.java |
| https://opencloud.wostore.cn/openapi/netauth/precheck/wp? | com/mobile/auth/x/a.java |
| https://opencloud.wostore.cn/client/sdk/receive | com/mobile/auth/z/d.java |
| https://opencloud.wostore.cn/openapi/netauth/precheck/wp? | com/mobile/auth/y/b.java |
| https://e.189.cn/sdk/agreement/detail.do?isWap=true&hidetop=true&appKey=8138111118 | com/mobile/auth/p/a.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://alogus.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://pslog.umeng.com/ablog | com/umeng/cconfig/UMRemoteConfig.java |
| https://ucc.umeng.com/v1/fetch | com/umeng/cconfig/UMRemoteConfig.java |
| https://ucc.umeng.com/v1/fetch | com/umeng/cconfig/c/b.java |
| https://pslog.umeng.com/ablog | com/umeng/cconfig/c/b.java |
| http://developer.umeng.com/docs/66650/cate/66650 | com/umeng/analytics/pro/j.java |
| https://wap.cmpassport.com/resources/html/contract.html | com/umeng/umverify/UMConstant.java |
| https://e.189.cn/sdk/agreement/detail.do?isWap=true&hidetop=true&appKey=8138111118 | com/umeng/umverify/UMConstant.java |
| https://opencloud.wostore.cn/authz/resource/html/disclaimer.html?fromsdk=true | com/umeng/umverify/UMConstant.java |
| https://ai.login.umeng.com/api/umed/cache | com/umeng/umverify/utils/g.java |
| https://ai.login.umeng.com/api/umed/v2/mobile/log | com/umeng/umverify/utils/g.java |
| https://utoken.umeng.com/api/postZdata/v4 | com/umeng/umzid/ZIDManager.java |
| https://utoken.umeng.com/api/updateZdata/v4 | com/umeng/umzid/ZIDManager.java |
| https://m.sigmob.com | com/sigmob/sdk/mraid/b.java |
| https://adservice.sigmob.cn/sigmob/config | com/sigmob/sdk/base/h.java |
| https://adservice.sigmob.cn/sigmob/config? | com/sigmob/sdk/base/i.java |
| https://adservice.sigmob.cn/extconfig? | com/sigmob/sdk/base/i.java |
| https://dc.sigmob.cn/log | com/sigmob/sdk/base/i.java |
| https://adservice.sigmob.cn/ad/v4 | com/sigmob/sdk/base/i.java |
| https://adservice.sigmob.cn/hb/v2/ad | com/sigmob/sdk/base/i.java |
| http://%s:%d/%s | com/sigmob/sdk/videocache/h.java |
| http://%s:%d/%s | com/sigmob/sdk/videocache/m.java |
| https://github.com/danikula/AndroidVideoCache/issues/134. | com/sigmob/sdk/videocache/m.java |
| https://github.com/danikula/AndroidVideoCache/issues/43. | com/sigmob/sdk/videocache/j.java |
| https://github.com/danikula/AndroidVideoCache/issues. | com/sigmob/sdk/videocache/j.java |
| https://github.com/danikula/AndroidVideoCache/issues/88. | com/sigmob/sdk/videocache/j.java |
| https://fleast.cn/public/getAppid.php | com/hanlingyoushang/config.java |
| https://spare.fleast.cn/public/getAppid.php | com/hanlingyoushang/config.java |
| https://beibei.fleast.cn/public/getAppid.php | com/hanlingyoushang/config.java |
| https://spare-beiaei.fleast.cn/public/getAppid.php | com/hanlingyoushang/config.java |
| https://spare-beibei.fleast.cn/public/getAppid.php | com/hanlingyoushang/config.java |
| https://spare-aei.fleast.cn/public/getAppid.php | com/hanlingyoushang/config.java |
| https://spare-bei.fleast.cn/public/getAppid.php | com/hanlingyoushang/config.java |
| https://hybird.rayjump.com/rv/authoriztion.html | com/mbridge/msdk/a.java |
| http://www.w3.org/ns/ttml#parameter | com/mbridge/msdk/playercommon/exoplayer2/text/ttml/TtmlDecoder.java |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense | com/mbridge/msdk/playercommon/exoplayer2/drm/HttpMediaDrmCallback.java |
| https://cdn-adn-https.rayjump.com/cdn-adn/v2/portal/19/08/20/11/06/5d5b63cb457e2.js | com/mbridge/msdk/c/b.java |
| https://mtg-native.rayjump.com/omsdk/omsdkjs\_common\_js.txt | com/mbridge/msdk/c/b.java |
| http://whatwg.org/html/common-microsyntaxes.html#space-character | com/mbridge/msdk/c/b/c.java |
| http://whatwg.org/html/webappapis.html#dom-windowbase64-atob | com/mbridge/msdk/c/b/c.java |
| https://gist.github.com/atk/1020396 | com/mbridge/msdk/c/b/c.java |
| http://whatwg.org/C#alphanumeric-ascii-characters | com/mbridge/msdk/c/b/c.java |
| http://whatwg.org/html/webappapis.html#dom-windowbase64-btoa | com/mbridge/msdk/c/b/c.java |
| https://s3-us-west-2.amazonaws.com/omsdk-files/compliance-js/omid-validation-verification-script-v1.js | com/mbridge/msdk/a/b.java |
| https://play.google.com/ | com/mbridge/msdk/click/b.java |
| https://cdn-adn-https.rayjump.com/cdn-adn/v2/portal/19/08/20/11/06/5d5b63cb457e2.js | com/mbridge/msdk/foundation/controller/b.java |
| https://mtg-native.rayjump.com/omsdk/omsdkjs\_common\_js.txt | com/mbridge/msdk/foundation/controller/b.java |
| https://{}hb.rayjump.com | com/mbridge/msdk/foundation/same/net/f/d.java |
| https://analytics.rayjump.com | com/mbridge/msdk/foundation/same/net/f/d.java |
| https://net.rayjump.com | com/mbridge/msdk/foundation/same/net/f/d.java |
| https://configure.rayjump.com | com/mbridge/msdk/foundation/same/net/f/d.java |
| https://detect.rayjump.com/mapi/find | com/mbridge/msdk/foundation/same/net/f/d.java |
| https://detect.rayjump.com/mapi/result | com/mbridge/msdk/foundation/same/net/f/d.java |
| https://d1tru86qrby720.cloudfront.net/hostsetting | com/mbridge/msdk/foundation/same/net/f/d.java |
| https://policy.rayjump.com | com/mbridge/msdk/foundation/same/net/f/d.java |
| https://lazy.rayjump.com | com/mbridge/msdk/foundation/same/net/f/d.java |
| https://check.rayjump.com | com/mbridge/msdk/foundation/same/net/f/d.java |
| https://play.google.com/store/apps/details?id= | com/mbridge/msdk/foundation/tools/z.java |
| https://play.google.com/ | com/mbridge/msdk/foundation/tools/z.java |
| https://play.google.com | com/mbridge/msdk/mbjscommon/windvane/WindVaneWebView.java |
| http://47.97.36.81:8090/PrivacyLink | com/tb/mob/more/TbWebViewActivity.java |
| http://saas.qubiankeji.com:18013 | com/tb/mob/saas/SaasConfigInfo.java |
| https://h5iad.sp-card.com/games/launch/?appSecret= | com/tb/mob/h5/BaseWebActivity.java |
| http://adput.qubiankeji.com:7071 | com/tb/zkmob/a/b.java |
| https://appspe.qubiankeji.com | com/tb/tb\_lib/b/c.java |
| https://app.qubiankeji.com | com/tb/tb\_lib/b/c.java |
| https://appspe.qubiankeji.com:8443 | com/tb/tb\_lib/b/c.java |
| https://app.qubiankeji.com:8443 | com/tb/tb\_lib/b/c.java |
| www.qq.com | com/tencent/smtt/sdk/m.java |
| https://pms.mb.qq.com/rsp204 | com/tencent/smtt/sdk/m.java |
| https://debugtbs.qq.com | com/tencent/smtt/sdk/WebView.java |
| https://debugx5.qq.com | com/tencent/smtt/sdk/WebView.java |
| https://debugtbs.qq.com?10000 | com/tencent/smtt/sdk/WebView.java |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=50079 | com/tencent/smtt/sdk/stat/MttLoader.java |
| https://mdc.html5.qq.com/mh?channel\_id=50079&u= | com/tencent/smtt/sdk/stat/MttLoader.java |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11041 | com/tencent/smtt/sdk/ui/dialog/d.java |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11047 | com/tencent/smtt/sdk/ui/dialog/d.java |
| https://log.tbs.qq.com/ajax?c=pu&v=2&k= | com/tencent/smtt/utils/n.java |
| https://log.tbs.qq.com/ajax?c=pu&tk= | com/tencent/smtt/utils/n.java |
| https://log.tbs.qq.com/ajax?c=dl&k= | com/tencent/smtt/utils/n.java |
| https://cfg.imtt.qq.com/tbs?v=2&mk= | com/tencent/smtt/utils/n.java |
| https://log.tbs.qq.com/ajax?c=ul&v=2&k= | com/tencent/smtt/utils/n.java |
| https://mqqad.html5.qq.com/adjs | com/tencent/smtt/utils/n.java |
| https://log.tbs.qq.com/ajax?c=ucfu&k= | com/tencent/smtt/utils/n.java |
| https://tbsrecovery.imtt.qq.com/getconfig | com/tencent/smtt/utils/n.java |
| https://soft.tbs.imtt.qq.com/17421/tbs\_res\_imtt\_tbs\_DebugPlugin\_DebugPlugin.tbs | com/tencent/smtt/utils/d.java |
| https://ai.baidu.com/activation/key/activate | com/baidu/vis/unified/license/BDLicenseActivator.java |
| http://10.138.32.176:8518/api/v3/person/verify\_sec?appid=7758258 | com/baidu/idl/face/platform/ui/utils/SecRequest.java |
| https://aip.baidubce.com/rest/2.0/face/v4/faceverify | com/baidu/idl/face/api/manager/APIService.java |
| https://aip.baidubce.com/rest/2.0/face/v4/mingjing/verify | com/baidu/idl/face/api/manager/APIService.java |
| https://ai.baidu.com/activation/key/activate | com/baidu/idl/main/facesdk/FaceAuth.java |
| http://brain.baidu.com/record/api | com/baidu/idl/main/facesdk/statistic/PostDeviceInfo.java |
| https://vse.baidu.com/v2 | com/baidu/speech/asr/SpeechConstant.java |
| https://vse.baidu.com/echo.fcgi | com/baidu/speech/asr/SpeechConstant.java |
| https://upl.baidu.com//words/add | com/baidu/speech/asr/SlotControl.java |
| https://yuyin.baidu.com/voice?osname=voiceopen&action=usereventflow& | com/baidu/speech/utils/analysis/Analysis.java |
| https://audiotest.baidu.com/auth/ | com/baidu/speech/utils/auth/UrlEnum.java |
| https://vop.baidu.com/v2 | com/baidu/speech/core/ASREngine.java |
| http://211.151.146.65:8080/wlantest/shanghai\_sun/mock\_ad\_server\_intersitial\_video.json | com/baidu/mobads/sdk/internal/cr.java |
| https://cpro.baidustatic.com/cpro/logo/sdk/mob-adIcon\_2x.png | com/baidu/mobads/sdk/api/XAdNativeResponse.java |
| https://cpro.baidustatic.com/cpro/logo/sdk/new-bg-logo.png | com/baidu/mobads/sdk/api/XAdNativeResponse.java |
| http://union.baidu.com/ | com/baidu/mobads/sdk/api/XAdNativeResponse.java |
| https://sdk.e.qq.com/launch | com/qq/e/comm/b/a.java |
| https://sdk.e.qq.com/activate | com/qq/e/comm/b/a.java |
| https://px.ucweb.com/upload | com/nirvana/tools/crash/BuildConfig.java |
| https://verify.cmpassport.com/h5/getMobile | com/nirvana/tools/logger/UaidTracker.java |
| https://nisportal.10010.com:9001/api | com/nirvana/tools/logger/UaidTracker.java |
| https://nisportal.10010.com:9001/api? | com/nirvana/tools/logger/UaidTracker.java |
| https://voicelog.xinliangxiang.com | com/xlx/speech/i/b.java |
| https://voiceapi.xinliangxiang.com | com/xlx/speech/i/a.java |
| https://voicefront.xinliangxiang.com?sdk=1&versionCode= | com/xlx/speech/v/a.java |
| https://dc.sigmob.cn/log | com/czhj/sdk/common/models/Config.java |
| http://www.google.com | com/zj/zjdsp/net/security/ParamSec.java |
| http://www.google.com? | com/zj/zjdsp/net/security/ParamSec.java |
| http://dapi.zjbdl.cn | com/zj/zjdsp/net/task/NetConfig.java |
| http://dapi.zjbdl.cn/api/android/v1/events | com/zj/zjdsp/net/task/NetConfig.java |
| http://dapi.zjbdl.cn/api/android/v2/adload | com/zj/zjdsp/net/task/NetConfig.java |
| http://dapi.zjbdl.cn/api/app/statistics | com/zj/zjdsp/net/task/NetConfig.java |
| http://dapi.zjbdl.cn/api/app/v2/log | com/zj/zjdsp/net/task/NetConfig.java |
| http://dapi.zjbdl.cn/api/android/v1/init | com/zj/zjdsp/net/task/NetConfig.java |
| https://d.alipay.com | com/zj/zjdsp/web/ZjAdPageWebViewSetting.java |
| http://news.fliduo.cn/api/v2/news\_list | com/zj/news/f.java |
| http://news.fliduo.cn/api/v2/getType | com/zj/news/ZjNewsFragment.java |
| http://news.fliduo.cn/api/v2/getType | com/zj/news/ZjNewsFragmentActivity.java |
| https://d.alipay.com | com/zj/news/e.java |
| https://aip.baidubce.com/oauth/2.0/token? | com/baidujieru/AuthService.java |
| https://aip.baidubce.com/rest/2.0/ocr/v1/accurate\_basic | com/baidujieru/AccurateBasic.java |
| https://aip.baidubce.com/rest/2.0/face/v3/detect | com/baidujieru/FaceDetect.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 |
| http://boardy.huanqiu.com | com/iBookStar/views/X5WebView.java |
| http://rp.ipadview.com/alipay/account/transferpage?bpid=%s&buid=%s | com/iBookStar/views/YmWebView.java |
| http://boardy.huanqiu.com | com/iBookStar/views/InnerWebView.java |
| www.ibookstar.com | com/iBookStar/activityComm/DownloadService.java |
| http://rp.ipadview.com/alipay/account/transferpage?bpid=%s&buid=%s | com/iBookStar/activityComm/CoinWebViewFragment.java |
| http://rp.ipadview.com/alipay/account/transferpage?bpid=%s&buid=%s | com/iBookStar/activityComm/WebViewFragment.java |
| www.ibookstar.com | com/iBookStar/activityComm/AppInstallReceiver.java |
| http://ip.taobao.com/outGetIpInfo?accessKey=alibaba-inc&ip=myip | com/iBookStar/utils/n.java |
| https://ip.adipman.net/ip/refresh?ts= | com/iBookStar/utils/n.java |
| http://tools.ibookeee.com?ymlandpage=1 | com/iBookStar/utils/v.java |
| www.ipadview.com/rpads/score/passAwardFailed? | com/iBookStar/utils/l.java |
| www.ipadview.com/rpads/score/taskCenterAward? | com/iBookStar/utils/l.java |
| www.ipadview.com/rpads/score/extraAdsAward | com/iBookStar/utils/l.java |
| www.ipadview.com/rpads/score/award | com/iBookStar/utils/l.java |
| www.ipadview.com/rpads/score/beginRead | com/iBookStar/utils/l.java |
| www.ipadview.com/rpads/score\_task/list?userId= | com/iBookStar/utils/l.java |
| www.ipadview.com/rpads/book\_coin/view?userId= | com/iBookStar/utils/l.java |
| www.ipadview.com/rpads/score\_task/videoCanAward? | com/iBookStar/utils/l.java |
| www.ipadview.com/rpads/score/videoAward? | com/iBookStar/utils/l.java |
| www.ipadview.com/rpads/book\_coin/cur\_task\_status? | com/iBookStar/utils/l.java |
| https://api.twitter.com/oauth/access\_token | com/androidquery/auth/TwitterHandle.java |
| https://api.twitter.com/oauth/authorize | com/androidquery/auth/TwitterHandle.java |
| https://api.twitter.com/oauth/request\_token | com/androidquery/auth/TwitterHandle.java |
| https://graph.facebook.com/oauth/authorize | com/androidquery/auth/FacebookHandle.java |
| https://www.facebook.com/connect/login\_success.html | com/androidquery/auth/FacebookHandle.java |
| https://graph.facebook.com/oauth/authorize? | com/androidquery/auth/FacebookHandle.java |
| https://graph.facebook.com/me | com/androidquery/auth/FacebookHandle.java |
| https://androidquery.appspot.com | com/androidquery/service/MarketService.java |
| www.chengzijianzhan.com | com/ss/android/downloadlib/addownload/compliance/b.java |
| www.toutiaopage.com/tetris/page | com/ss/android/downloadlib/addownload/compliance/b.java |
| https://apps.oceanengine.com/customer/api/app/pkg\_info? | com/ss/android/downloadlib/addownload/compliance/b.java |
| https://sf6-ttcdn-tos.pstatp.com/obj/ad-tetris-site/personal-privacy-page.html | com/ss/android/downloadlib/addownload/compliance/AppPrivacyPolicyActivity.java |
| https://www.samsungapps.com/appquery/appDetail.as?appId= | com/ss/android/downloadlib/g/h.java |
| https://i.snssdk.com/ | com/ss/android/downloadad/api/constant/AdBaseConstants.java |
| http://www.google.com | com/sjm/sjmdsp/net/security/ParamSec.java |
| http://www.google.com? | com/sjm/sjmdsp/net/security/ParamSec.java |
| http://dapi.sjmbdl.cn | com/sjm/sjmdsp/net/task/NetConfig.java |
| http://dapi.sjmbdl.cn/api/android/v1/events | com/sjm/sjmdsp/net/task/NetConfig.java |
| http://sdk.hzsanjiaomao.com/sspconfig/%s.txt | com/sjm/sjmdsp/net/task/NetConfig.java |
| http://dapi.sjmbdl.cn/api/app/statistics | com/sjm/sjmdsp/net/task/NetConfig.java |
| http://dapi.sjmbdl.cn/api/app/v2/log | com/sjm/sjmdsp/net/task/NetConfig.java |
| http://dapi.sjmbdl.cn/api/android/v1/init | com/sjm/sjmdsp/net/task/NetConfig.java |
| https://d.alipay.com | com/sjm/sjmdsp/web/SjmAdPageWebViewSetting.java |
| https://d.alipay.com | com/sjm/sjmsdk/js/b.java |
| http://api.hzsanjiaomao.com/api/adEvent | com/sjm/sjmsdk/a/f/d.java |
| http://sdk.hzsanjiaomao.com/sjmconfig/%s.json | com/sjm/sjmsdk/core/c/c.java |
| https://crbug.com/581399 | aegon/chrome/net/impl/UrlRequestBuilderImpl.java |
| https://api-sdk.brily.cn | lib/armeabi-v7a/libnative.so |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| danikula@gmail.com | com/kwad/sdk/core/videocache/h.java |
| danikula@gmail.com | com/sigmob/sdk/videocache/j.java |
| .apk@classes.dex | com/kuaishou/weapon/p0/d0.java |
| xxx@email.elided | aegon/chrome/base/PiiElider.java |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869184 | com/kwai/video/player/KsMediaMeta.java |
| 13000000000 | com/baidu/idl/face/platform/ui/utils/SecRequest.java |

## **5. 签名证书**

**APK is signed v1 signature: True v2 signature: True v3 signature: False Found 1 unique certificates Subject: C=chn, ST=zj, L=hz, O=hlys, OU=hlys, CN=hlys Signature Algorithm: rsassa\_pkcs1v15 Valid From: 2022-09-09 12:30:25+00:00 Valid To: 2122-08-16 12:30:25+00:00 Issuer: C=chn, ST=zj, L=hz, O=hlys, OU=hlys, CN=hlys Serial Number: 0x10c1c19f Hash Algorithm: sha256 md5: 93561e33dc94304ec913ff35410254fb sha1: 2a2e818d2fc1b9e9b289bde7b6ab18bf76837e17 sha256: d2f68e603aad6ad0ba093c60b601bcd1441e150fd7848b1cd2b7fa3d59bdb93a sha512: a8ee754b2e87fdf6bb54846e213f8d330ac736262c51ba67bc49b538cf37833e01b25337beb05476630bde2b149792a9dead4855a35ac5d0a354f98a3c9eaebc PublicKey Algorithm: rsa Bit Size: 2048 Fingerprint: c7bb3fa3200ae96cb308df2483dc3a1e74ea92261f4e381557ef756b6ec7aca9**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "dyStrategy.privateAddress" : "privateAddress" |
| "ksad\_ad\_default\_author" : "@可爱的广告君创造的原声" |
| "ksad\_ad\_default\_username" : "@可爱的广告君" |

## **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.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.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.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\_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.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.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.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.hanlingyoushang.permission.liantian.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| 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.REQUEST\_DELETE\_PACKAGES | 正常 |  | 允许应用程序请求删除包 |
| com.android.launcher.permission.INSTALL\_SHORTCUT | 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 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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.SET\_WALLPAPER | 正常 | 设置壁纸 | 允许应用程序设置系统壁纸 |
| 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 |
| com.hanlingyoushang.openadsdk.permission.TT\_PANGOLIN | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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.READ\_PRIVILEGED\_PHONE\_STATE | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.iBookStar.activityComm.SchemeActivity | **Schemes**: com.hanlingyoushang.novel://, yuemeng://, |

**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。**