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

**鸽友宝（ 3.0.6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 | 鸽友宝 |
| 版本 | 3.0.6 |
| 包名 | com.shyl.dps |
| 域名线索 | 74条 |
| URL线索 | 75条 |
| APP图标 |  |
| 分析日期 | 2024年10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 | geyoubao.apk |
| 文件大小 | 61.59MB |
| MD5值 | 345310c1469be42af0815e00478cf71a |
| SHA1值 | f657aebc35eef2e0e76bd85540feb30f289155a1 |
| SHA256值 | 4443fc60f938ca315176326965f09c6d473f2b233cb8465734fe07df06ff6626 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 鸽友宝 |
| 包名 | com.shyl.dps |
| 主活动Activity | com.shyl.dps.ui.LauncherActivity |
| 安卓版本名称 | 3.0.6 |
| 安卓版本 | 307100 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| yuntuapi.amap.com | 没有服务器地理信息.  |
| lbs-3dtiles-service.amap.com | IP: 203.119.204.133 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| mpsapi.amap.com | IP: 59.82.112.213 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| oss-cn-hangzhou.aliyuncs.com | IP: 118.31.219.189 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| mobile.unionpay.com | 没有服务器地理信息.  |
| image.cnamedomain.com | 没有服务器地理信息.  |
| astat.bugly.qcloud.com | IP: 119.28.121.133 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| web.dps-pigeonloft.com | IP: 60.205.189.6 所属国家: China 地区: Beijing 城市: Beijing  |
| g.co | IP: 172.217.160.78 所属国家: United States of America 地区: California 城市: Mountain View  |
| vod.cn-shanghai.aliyuncs.com | IP: 106.15.83.32 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| oss-cn-.aliyuncs.comor | 没有服务器地理信息.  |
| apistore.amap.com | IP: 110.253.189.212 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| dove-base.dps-pigeonloft.com | IP: 123.57.55.210 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| cs-v3.dps-pigeonloft.com | IP: 60.205.189.6 所属国家: China 地区: Beijing 城市: Beijing  |
| mps.amap.com | IP: 59.82.112.213 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| api.dps-pigeonloft.com | IP: 60.205.189.6 所属国家: China 地区: Beijing 城市: Beijing  |
| open.weixin.qq.com | IP: 220.196.154.28 所属国家: China 地区: Jiangsu 城市: Wuxi  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| mst01.is.autonavi.com | IP: 110.253.189.211 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| apilocate.amap.com | IP: 59.82.31.183 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| astat.bugly.cros.wr.pvp.net | IP: 170.106.118.26 所属国家: United States of America 地区: California 城市: San Francisco  |
| ultravideo.cs.tut.fi | IP: 130.230.203.118 所属国家: Finland 地区: Pirkanmaa 城市: Tampere  |
| m5.amap.com | IP: 59.82.113.187 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| uri.amap.com | IP: 203.119.175.235 所属国家: China 地区: Beijing 城市: Beijing  |
| www.95516.com | IP: 106.74.11.232 所属国家: China 地区: Shandong 城市: Jinan  |
| xml.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| android.bugly.qq.com | IP: 124.95.225.146 所属国家: China 地区: Liaoning 城市: Shenyang  |
| h.trace.qq.com | IP: 113.56.189.246 所属国家: China 地区: Hubei 城市: Huangshi  |
| wap.amap.com | IP: 112.26.156.111 所属国家: China 地区: Anhui 城市: Lu'an  |
| dualstack-arestapi.amap.com | IP: 39.98.22.142 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| zgxt.com | 没有服务器地理信息.  |
| zg.dps-pigeonloft.com | IP: 60.205.189.6 所属国家: China 地区: Beijing 城市: Beijing  |
| api.hcharts.cn | IP: 118.31.2.95 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| img.alicdn.com | IP: 123.125.216.243 所属国家: China 地区: Beijing 城市: Beijing  |
| asr.cloud.tencent.com | IP: 120.53.97.39 所属国家: China 地区: Beijing 城市: Beijing  |
| adiu.amap.com | IP: 59.82.118.236 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| cgicol.amap.com | IP: 60.222.200.219 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| www.slf4j.org | IP: 195.15.222.169 所属国家: Switzerland 地区: Geneve 城市: Carouge  |
| wprd0d.is.autonavi.com | 没有服务器地理信息.  |
| api.seniverse.com | IP: 116.62.81.138 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| lbs.amap.com | IP: 110.253.189.211 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| cs-zg-v3.dps-pigeonloft.com | IP: 60.205.189.6 所属国家: China 地区: Beijing 城市: Beijing  |
| android.googlesource.com | IP: 74.125.203.82 所属国家: United States of America 地区: California 城市: Mountain View  |
| vsp.allinpay.com | IP: 111.161.122.56 所属国家: China 地区: Tianjin 城市: Tianjin  |
| dualstack-a.apilocate.amap.com | IP: 106.11.40.50 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| match-base.dps-pigeonloft.com | IP: 123.57.55.210 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| dovecote-base.dps-pigeonloft.com | IP: 123.57.55.210 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| app.com | IP: 157.240.9.36 所属国家: Bulgaria 地区: Sofia (stolitsa) 城市: Sofia  |
| journeyapps.com | IP: 18.65.168.90 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| cs.dps-pigeonloft.com | IP: 60.205.189.6 所属国家: China 地区: Beijing 城市: Beijing  |
| api.weixin.qq.com | IP: 116.128.170.42 所属国家: China 地区: Shanghai 城市: Shanghai  |
| standards.iso.org | IP: 138.81.131.111 所属国家: Switzerland 地区: Geneve 城市: Geneva  |
| mp.weixin.qq.com | IP: 220.196.154.28 所属国家: China 地区: Jiangsu 城市: Wuxi  |
| dps.com | IP: 13.69.68.22 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam  |
| www.windy.com | IP: 18.64.123.56 所属国家: United States of America 地区: Washington 城市: Seattle  |
| openrcv.baidu.com | IP: 111.206.209.112 所属国家: China 地区: Beijing 城市: Beijing  |
| dxp.baidu.com | IP: 110.242.68.94 所属国家: China 地区: Hebei 城市: Baoding  |
| abroad.apilocate.amap.com | IP: 59.82.44.11 所属国家: China 地区: Shanghai 城市: Shanghai  |
| restsdk.amap.com | IP: 59.82.132.217 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| faas-image.amap.com | IP: 42.56.82.208 所属国家: China 地区: Liaoning 城市: Shenyang  |
| hmma.baidu.com | IP: 110.242.68.196 所属国家: China 地区: Hebei 城市: Baoding  |
| cs-api.dps-pigeonloft.com | IP: 60.205.189.6 所属国家: China 地区: Beijing 城市: Beijing  |
| restapi.amap.com | IP: 59.82.132.217 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| www.highcharts.com | IP: 104.18.9.9 所属国家: United States of America 地区: California 城市: San Francisco  |
| wb.amap.com | IP: 110.253.189.212 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| cs-zg.dps-pigeonloft.com | IP: 60.205.189.6 所属国家: China 地区: Beijing 城市: Beijing  |
| maps.testing.amap.com | IP: 140.205.69.9 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| user-base.dps-pigeonloft.com | IP: 123.57.55.210 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| dps-pigeonloft.com | IP: 123.57.55.210 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| dashif.org | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| long.open.weixin.qq.com | IP: 112.65.193.170 所属国家: China 地区: Shanghai 城市: Shanghai  |
| datax.baidu.com | 没有服务器地理信息.  |
| cs-api-v3.dps-pigeonloft.com | IP: 60.205.189.6 所属国家: China 地区: Beijing 城市: Beijing  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://asr.cloud.tencent.com/server\_time  | ahskej/com/tencent/aai/task/net/networktime/QCloudServiceTimeClient.java  |
| https://github.com/Tencent/tinker/issues  | ahskej/com/tencent/tinker/lib/reporter/DefaultPatchReporter.java  |
| https://github.com/Tencent/tinker/issues  | ahskej/com/tencent/tinker/lib/reporter/DefaultLoadReporter.java  |
| http://restsdk.amap.com/v3  | ahskej/com/amap/api/col/s/m.java  |
| https://restsdk.amap.com/v3  | ahskej/com/amap/api/col/s/m.java  |
| http://restsdk.amap.com/v4  | ahskej/com/amap/api/col/s/m.java  |
| https://restsdk.amap.com/v4  | ahskej/com/amap/api/col/s/m.java  |
| http://restsdk.amap.com/v5  | ahskej/com/amap/api/col/s/m.java  |
| https://restsdk.amap.com/v5  | ahskej/com/amap/api/col/s/m.java  |
| http://yuntuapi.amap.com  | ahskej/com/amap/api/col/s/m.java  |
| https://yuntuapi.amap.com  | ahskej/com/amap/api/col/s/m.java  |
| http://restsdk.amap.com/rest/me/cpoint  | ahskej/com/amap/api/col/s/m.java  |
| https://restsdk.amap.com/rest/me/cpoint  | ahskej/com/amap/api/col/s/m.java  |
| http://apistore.amap.com  | ahskej/com/amap/api/col/s/m.java  |
| https://apistore.amap.com  | ahskej/com/amap/api/col/s/m.java  |
| http://m5.amap.com/ws/mapapi/shortaddress/transform  | ahskej/com/amap/api/col/s/m.java  |
| https://m5.amap.com/ws/mapapi/shortaddress/transform  | ahskej/com/amap/api/col/s/m.java  |
| https://restsdk.amap.com/sdk/compliance/params  | ahskej/com/amap/api/col/s/dh.java  |
| http://restsdk.amap.com/sdk/compliance/params  | ahskej/com/amap/api/col/s/dh.java  |
| https://restapi.amap.com/rest/aaid/get  | ahskej/com/amap/api/col/s/cq.java  |
| http://restapi.amap.com/rest/aaid/get  | ahskej/com/amap/api/col/s/cq.java  |
| https://api.weixin.qq.com/  | ahskej/com/shyl/dps/di/HttpModule.java  |
| https://restapi.amap.com/  | ahskej/com/shyl/dps/di/HttpModule.java  |
| https://api.seniverse.com/  | ahskej/com/shyl/dps/di/HttpModule.java  |
| https://user-base.dps-pigeonloft.com  | ahskej/com/shyl/grpc/GrpcInit.java  |
| https://dove-base.dps-pigeonloft.com  | ahskej/com/shyl/grpc/di/GRPCModule.java  |
| https://match-base.dps-pigeonloft.com  | ahskej/com/shyl/grpc/di/GRPCModule.java  |
| https://user-base.dps-pigeonloft.com  | ahskej/com/shyl/grpc/di/GRPCModule.java  |
| https://dovecote-base.dps-pigeonloft.com  | ahskej/com/shyl/grpc/di/GRPCModule.java  |
| https://vsp.allinpay.com/statichtml/webpub/sdk/icon/yinlian.png  | ahskej/com/allinpay/unifypay/sdk/e.java  |
| https://vsp.allinpay.com/apiweb/sdk/front  | ahskej/com/allinpay/unifypay/sdk/a/f.java  |
| http://www.slf4j.org/codes.html  | ahskej/org/slf4j/MDC.java  |
| http://www.slf4j.org/codes.html  | ahskej/org/slf4j/LoggerFactory.java  |
| https://github.com/arrow-kt/arrow-core/issues/new/choose  | arrow/core/ArrowCoreInternalException.java  |
| https://ip.  | com/alibaba/sdk/android/oss/OSSImpl.java  |
| http://oss-cn-\*\*\*\*.aliyuncs.com',or  | com/alibaba/sdk/android/oss/OSSImpl.java  |
| http://image.cnamedomain.com'!  | com/alibaba/sdk/android/oss/OSSImpl.java  |
| http://oss-cn-hangzhou.aliyuncs.com  | com/alibaba/sdk/android/oss/common/OSSConstants.java  |
| http://oss-cn-\*\*\*\*.aliyuncs.com',or  | com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java  |
| http://image.cnamedomain.com'!  | com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java  |
| http://xml.apache.org/xslt  | com/aliyun/vod/common/logger/LoggerPrinter.java  |
| https://videocloud.  | com/aliyun/vod/log/core/AliyunLogCommon.java  |
| http://vod.  | com/aliyun/vod/log/report/AliyunReportParam.java  |
| https://vod.cn-shanghai.aliyuncs.com/  | com/aliyun/auth/common/AliyunVodHttpCommon.java  |
| https://vod.  | com/aliyun/auth/common/AliyunVodHttpCommon.java  |
| https://adiu.amap.com/ws/device/adius  | com/amap/api/col/p0003l/hx.java  |
| http://cgicol.amap.com/collection/collectData?src=baseCol&ver=v74&  | com/amap/api/col/p0003l/js.java  |
| http://restsdk.amap.com  | com/amap/api/col/p0003l/fv.java  |
| https://restsdk.amap.com/sdk/compliance/params  | com/amap/api/col/p0003l/hh.java  |
| http://restsdk.amap.com/sdk/compliance/params  | com/amap/api/col/p0003l/hh.java  |
| http://restsdk.amap.com/v3/place/text?  | com/amap/api/col/p0003l/a.java  |
| http://restsdk.amap.com/v3/place/around?  | com/amap/api/col/p0003l/a.java  |
| http://restsdk.amap.com/v3/config/district?  | com/amap/api/col/p0003l/a.java  |
| https://restapi.amap.com/rest/aaid/get  | com/amap/api/col/p0003l/gf.java  |
| http://restapi.amap.com/rest/aaid/get  | com/amap/api/col/p0003l/gf.java  |
| https://restsdk.amap.com/v3/iasdkauth  | com/amap/api/col/p0003l/fm.java  |
| https://dualstack-arestapi.amap.com/v3/iasdkauth  | com/amap/api/col/p0003l/fm.java  |
| http://restsdk.amap.com/v4/gridmap?  | com/amap/api/col/p0003l/df.java  |
| http://restsdk.amap.com/v4/grasproad/driving?  | com/amap/api/col/p0003l/fg.java  |
| http://wprd0%d.is.autonavi.com/appmaptile?  | com/amap/api/col/p0003l/de.java  |
| http://restsdk.amap.com/v4/gridmap?  | com/amap/api/col/p0003l/de.java  |
| http://restsdk.amap.com/v4  | com/amap/api/col/p0003l/s.java  |
| http://restsdk.amap.com/v4  | com/amap/api/col/p0003l/cr.java  |
| http://restsdk.amap.com  | com/amap/api/col/p0003l/v.java  |
| http://mpsapi.amap.com/ws/mps/lyrdata/ugc/\  | com/amap/api/col/p0003l/l.java  |
| https://restapi.amap.com/rest/lbs/geohub/3d/tiles?z=%d&x=%d&y=%d&id=  | com/amap/api/col/p0003l/k.java  |
| https://adiu.amap.com/ws/device/adius  | com/amap/api/col/s/ds.java  |
| https://restsdk.amap.com/v3/iasdkauth  | com/amap/api/col/s/bx.java  |
| https://dualstack-arestapi.amap.com/v3/iasdkauth  | com/amap/api/col/s/bx.java  |
| http://wb.amap.com/?r=%f,%f,%s,%f,%f,%s,%d,%d,%d,%s,%s,%s&sourceapplication=openapi/0  | com/amap/api/col/s/bt.java  |
| http://wb.amap.com/?q=%f,%f,%s&sourceapplication=openapi/0  | com/amap/api/col/s/bt.java  |
| http://wb.amap.com/?n=%f,%f,%f,%f,%d&sourceapplication=openapi/0  | com/amap/api/col/s/bt.java  |
| http://wb.amap.com/?p=%s,%f,%f,%s,%s&sourceapplication=openapi/0  | com/amap/api/col/s/bt.java  |
| http://wap.amap.com/  | com/amap/api/maps/AMapUtils.java  |
| https://lbs-3dtiles-service.amap.com/basemap/tiles/staging?compose=building@1669011850923&compose=tree@1668678765481&z=%d&x=%d&y=%d  | com/amap/api/maps/model/amap3dmodeltile/AMap3DModelTileProvider.java  |
| http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/  | com/amap/api/location/AMapLocation.java  |
| http://apilocate.amap.com/mobile/binary  | com/autonavi/aps/amapapi/utils/b.java  |
| http://dualstack-a.apilocate.amap.com/mobile/binary  | com/autonavi/aps/amapapi/utils/b.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | com/autonavi/aps/amapapi/utils/b.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | com/autonavi/aps/amapapi/utils/h.java  |
| http://dualstack-arestapi.amap.com/v3/geocode/regeo  | com/autonavi/aps/amapapi/trans/c.java  |
| http://restsdk.amap.com/v3/geocode/regeo  | com/autonavi/aps/amapapi/trans/c.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | com/autonavi/aps/amapapi/trans/a.java  |
| http://restsdk.amap.com/rest/lbs/dem/data?z=%d&x=%d&y=%d&type=2  | com/autonavi/base/ae/gmap/TerrainOverlayProvider.java  |
| http://mst01.is.autonavi.com/appmaptile?z=%d&x=%d&y=%d&lang=zh\_cn&size=1&scale=1&style=6  | com/autonavi/base/ae/gmap/TerrainOverlayProvider.java  |
| http://mpsapi.amap.com/  | com/autonavi/base/ae/gmap/GLMapEngine.java  |
| http://m5.amap.com/  | com/autonavi/base/ae/gmap/GLMapEngine.java  |
| http://m5.amap.com/  | com/autonavi/base/amap/mapcore/maploader/AMapLoader.java  |
| https://datax.baidu.com/xs.gif  | com/baidu/mobstat/y.java  |
| https://dxp.baidu.com/upgrade  | com/baidu/mobstat/y.java  |
| https://hmma.baidu.com/auto.gif  | com/baidu/mobstat/Config.java  |
| http://hmma.baidu.com/app.gif  | com/baidu/mobstat/Config.java  |
| https://hmma.baidu.com/app.gif  | com/baidu/mobstat/Config.java  |
| https://openrcv.baidu.com/1010/bplus.gif  | com/baidu/mobstat/r.java  |
| https://api.dps-pigeonloft.com/  | com/dps/net/BuildConfig.java  |
| https://dps-pigeonloft.com/  | com/dps/net/BuildConfig.java  |
| https://zg.dps-pigeonloft.com/api-zg/  | com/dps/net/BuildConfig.java  |
| https://web.dps-pigeonloft.com/privacy/logoff.html  | com/shyl/dps/ui/mine/DeleteAccountActivity.java  |
| http://uri.amap.com/navigation?to=  | com/shyl/dps/utils/MapNaviUtils.java  |
| https://cs-v3.dps-pigeonloft.com/  | com/nly/main/DebugMMKVUtils.java  |
| https://cs-api-v3.dps-pigeonloft.com/  | com/nly/main/DebugMMKVUtils.java  |
| https://cs-zg-v3.dps-pigeonloft.com/api-zg/  | com/nly/main/DebugMMKVUtils.java  |
| https://cs.dps-pigeonloft.com/  | com/nly/main/DebugMMKVUtils.java  |
| https://cs-api.dps-pigeonloft.com/  | com/nly/main/DebugMMKVUtils.java  |
| https://cs-zg.dps-pigeonloft.com/api-zg/  | com/nly/main/DebugMMKVUtils.java  |
| http://dps.com/  | com/nly/main/DebugMMKVUtils.java  |
| http://app.com/  | com/nly/main/DebugMMKVUtils.java  |
| http://zgxt.com/  | com/nly/main/DebugMMKVUtils.java  |
| https://h.trace.qq.com/kv  | com/tencent/bugly/proguard/ad.java  |
| https://astat.bugly.qcloud.com/rqd/async  | com/tencent/bugly/proguard/ac.java  |
| https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async  | com/tencent/bugly/proguard/ac.java  |
| https://android.bugly.qq.com/rqd/async  | com/tencent/bugly/crashreport/common/strategy/StrategyBean.java  |
| https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s  | com/tencent/mm/opensdk/diffdev/a/c.java  |
| https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s  | com/tencent/mm/opensdk/diffdev/a/b.java  |
| https://mp.weixin.qq.com/publicpoc/opensdkconf?action=GetShareConf&appid=%s&sdkVersion=%s&buffer=%s  | com/tencent/mm/opensdk/openapi/WXAPiSecurityHelper.java  |
| https://mobile.unionpay.com/getclient?platform=android&type=securepayplugin\  | com/unionpay/UPPayAssistEx.java  |
| https://www.windy.com/  | dps/map/MapLookForWindActivity$url$2.java  |
| https://www.windy.com/  | dps/map/TrainingMapActivity.java  |
| http://uri.amap.com/navigation?to=  | dps/map/viewmodel/TrainingMapViewModel.java  |
| https://journeyapps.com/  | 摸瓜V1引擎  |
| https://github.com/journeyapps/zxing-android-embedded  | 摸瓜V1引擎  |
| https://www.95516.com/portal/open/init.do?entry=open  | 摸瓜V1引擎  |
| https://api.hcharts.cn/highcharts  | 摸瓜V2引擎  |
| https://www.highcharts.com?credits  | 摸瓜V2引擎  |
| https://github.com/arrow-kt/arrow-core/issues/new/choose  | 摸瓜V3引擎  |
| http://restsdk.amap.com/v3/place/around?  | 摸瓜V3引擎  |
| https://api.seniverse.com/  | 摸瓜V3引擎  |
| https://initializationhttp://dashif.org/guidelines/last-segment-numberframeRatedash:profile:isoff-li  | 摸瓜V3引擎  |
| api.dps-pigeonloft.com  | 摸瓜V3引擎  |
| http://schemas.android.com/aapt  | 摸瓜V3引擎  |
| https://dualstack-arestapi.amap.com/v3/iasdkauth  | 摸瓜V3引擎  |
| https://adiu.amap.com/ws/device/adius  | 摸瓜V3引擎  |
| http://restsdk.amap.com/v3/place/text?  | 摸瓜V3引擎  |
| http://standards.iso.org/ittf/PubliclyAvailableStandards/MPEG-DASH\_schema\_files/DASH-MPD.xsd  | 摸瓜V3引擎  |
| http://uri.amap.com/navigation?to=  | 摸瓜V3引擎  |
| https://user-base.dps-pigeonloft.com  | 摸瓜V3引擎  |
| https://restapi.amap.com/  | 摸瓜V3引擎  |
| https://restsdk.amap.com/v3/iasdkauth  | 摸瓜V3引擎  |
| https://android.googlesource.com/toolchain/llvm  | 摸瓜V3引擎  |
| http://restsdk.amap.com/v4  | 摸瓜V3引擎  |
| http://restapi.amap.com/rest/aaid/get  | 摸瓜V3引擎  |
| https://vsp.allinpay.com/apiweb/sdk/front  | 摸瓜V3引擎  |
| www.googleapis.com  | 摸瓜V3引擎  |
| https://android.googlesource.com/toolchain/llvm-project  | 摸瓜V3引擎  |
| https://restsdk.amap.com/sdk/compliance/params  | 摸瓜V3引擎  |
| https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signatur  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res-auto  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/android((layout/specify\_\_item\_result\_third\_dove\_0  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/android&&layout/item\_specify\_order\_dove\_match\_0  | 摸瓜V3引擎  |
| http://mpsapi.amap.com/ws/mps/lyrdata/ugc/  | 摸瓜V3引擎  |
| http://dashif.org/guidelines/last-segment-number  | 摸瓜V3引擎  |
| http://g.co/dev/packagevisibility.  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/androidP  | 摸瓜V3引擎  |
| https://restapi.amap.com/rest/lbs/geohub/3d/tiles?z=%d&x=%d&y=%d  | 摸瓜V3引擎  |
| http://wprd0%d.is.autonavi.com/appmaptile?  | 摸瓜V3引擎  |
| https://web.dps-pigeonloft.com/privacy/logoff.html  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/android$$layout/activity\_dove\_image\_manager\_0))pictureLabel1  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/android  | 摸瓜V3引擎  |
| https://developer.android.com/guide/topics/media/issues/cleartext-not-permitted  | 摸瓜V3引擎  |
| http://restsdk.amap.com/v4/gridmap?  | 摸瓜V3引擎  |
| https://android.googlesource.com/toolchain/clang  | 摸瓜V3引擎  |
| https://restapi.amap.com/rest/aaid/get  | 摸瓜V3引擎  |
| http://restsdk.amap.com/v3/config/district?  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/android$$layout/apply\_\_fragment\_pager\_third\_0  | 摸瓜V3引擎  |
| http://restsdk.amap.com/sdk/compliance/params  | 摸瓜V3引擎  |
| https://api.weixin.qq.com/  | 摸瓜V3引擎  |
| http://restsdk.amap.com/v4/grasproad/driving?  | 摸瓜V3引擎  |
| https://dovecote-base.dps-pigeonloft.com  | 摸瓜V3引擎  |
| https://dove-base.dps-pigeonloft.com  | 摸瓜V3引擎  |
| http://restsdk.amap.com  | 摸瓜V3引擎  |
| https://match-base.dps-pigeonloft.com  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/android##layout/activity\_search\_proxy\_user\_0  | 摸瓜V3引擎  |
| http://dashif.org/guidelines/trickmode  | 摸瓜V3引擎  |
| http://cgicol.amap.com/collection/collectData?src=baseCol&ver=v74&  | 摸瓜V3引擎  |
| https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s  | 摸瓜V3引擎  |
| https://lbs-3dtiles-service.amap.com/basemap/tiles/staging?compose=building  | 摸瓜V3引擎  |
| http://mpsapi.amap.com/ws/mps/vmap/  | lib/arm64-v8a/libAMapSDK\_MAP\_v10\_0\_600.so  |
| http://mpsapi.amap.com/ws/mps/rtt/  | lib/arm64-v8a/libAMapSDK\_MAP\_v10\_0\_600.so  |
| http://mpsapi.amap.com/ws/mps/smap  | lib/arm64-v8a/libAMapSDK\_MAP\_v10\_0\_600.so  |
| http://m5.amap.com/ws/transfer/auth/map/indoor\_maps  | lib/arm64-v8a/libAMapSDK\_MAP\_v10\_0\_600.so  |
| http://mpsapi.amap.com/ws/mps/lyrdata/ugc/  | lib/arm64-v8a/libAMapSDK\_MAP\_v10\_0\_600.so  |
| http://mpsapi.amap.com/  | lib/arm64-v8a/libAMapSDK\_MAP\_v10\_0\_600.so  |
| http://m5.amap.com  | lib/arm64-v8a/libAMapSDK\_MAP\_v10\_0\_600.so  |
| https://mps.amap.com/ws/mps/rtt  | lib/arm64-v8a/libAMapSDK\_MAP\_v10\_0\_600.so  |
| https://mps.amap.com/ws/mps/vmap  | lib/arm64-v8a/libAMapSDK\_MAP\_v10\_0\_600.so  |
| https://maps.testing.amap.com/ws/transfer/auth/map/indoor\_maps  | lib/arm64-v8a/libAMapSDK\_MAP\_v10\_0\_600.so  |
| https://mps.amap.com/ws/mps/smap  | lib/arm64-v8a/libAMapSDK\_MAP\_v10\_0\_600.so  |
| https://mps.amap.com/ws/mps/spot  | lib/arm64-v8a/libAMapSDK\_MAP\_v10\_0\_600.so  |
| https://mps.amap.com/ws/mps/hot  | lib/arm64-v8a/libAMapSDK\_MAP\_v10\_0\_600.so  |
| http://maps.testing.amap.com/ws/mps/vmap  | lib/arm64-v8a/libAMapSDK\_MAP\_v10\_0\_600.so  |
| http://maps.testing.amap.com/ws/mps/rtt  | lib/arm64-v8a/libAMapSDK\_MAP\_v10\_0\_600.so  |
| https://faas-image.amap.com/acornCompressImageProd/%2523merge%2523%25402x-a2b2ad2c-50f4-46cc-9a68-9ef6a7c3d1be.png  | lib/arm64-v8a/libAMapSDK\_MAP\_v10\_0\_600.so  |
| https://img.alicdn.com/imgextra/i3/O1CN01BnLPsP1kjLlMfyzmX\_!!6000000004719-2-tps-64-64.png  | lib/arm64-v8a/libAMapSDK\_MAP\_v10\_0\_600.so  |
| https://m5.amap.com/  | lib/arm64-v8a/libAMapSDK\_MAP\_v10\_0\_600.so  |
| http://ultravideo.cs.tut.fi/  | lib/arm64-v8a/libavcodec.so  |
| http://%s:%d%s  | lib/arm64-v8a/libavformat.so  |
| http://%s%s  | lib/arm64-v8a/libavformat.so  |
| http://dashif.org/guidelines/last-segment-number  | lib/arm64-v8a/libavformat.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| twolame-discuss@lists.sourceforg  | lib/arm64-v8a/libavcodec.so  |
| appro@openssl.org  | lib/arm64-v8a/libconscrypt\_jni.so  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 18222222222  | com/amap/api/col/p0003l/fm.java  |
| 15060355040  | com/unionpay/UPPayAssistEx.java  |
| 17179869184  | tv/danmaku/ijk/media/player/IjkMediaMeta.java  |

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: L=TianJin, OU=纳兰云, CN=Jin 签名算法: rsassa\_pkcs1v15 有效期自: 2022-05-09 05:50:40+00:00 有效期至: 2072-04-26 05:50:40+00:00 发行人: L=TianJin, OU=纳兰云, CN=Jin 序列号: 0x2c8320 哈希算法: sha256 md5值: ca4cbb930eab77cd94b4b199c59a1adc sha1值: 1d5ade3073587bf915a7b61369e249a304eab58d sha256值: b4eaba913d44e5a644d9ab6a6cc379b81d49eb0e174a98bf8353635bff73da2f sha512值: 8b060f90d895c02e163058a1724c6c2dfe4696220b035449ffb92274e5ed915d05e2bcbb8ff079f8a84df2b516b2fd02cb3ea203a8b4d192290ff925bc2bf2fa 公钥算法: rsa 密钥长度: 2048 指纹: 6f1ca166a07c23a38adf841ccd818e7df9517145a01022bf26fd4ebb463907f5**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "err\_auth\_dented" : "认证被否决"  |
| "forget\_pwd" : "忘记密码"  |
| "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？"  |
| "pleaseInputPassword" : "请输入密码"  |
| "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\_timeout" : "会话超时,请重新登录"  |
| "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"  |

## **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.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.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.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.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.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 |
| android.permission.USE\_EXACT\_ALARM | 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.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.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.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 |
| 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.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.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 |
| org.simalliance.openmobileapi.SMARTCARD | 未知 | Unknown permission | Unknown permission from android reference |
| 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.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| com.google.android.c2dm.permission.RECEIVE | 合法 | C2DM 权限 | 云到设备消息传递的权限 |
| 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 |
| com.shyl.dps.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 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 |
| com.shyl.dps.permission.JPUSH\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| 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\_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.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 |
| android.permission.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.shyl.dps.ui.H5RoutActivity | **Schemes**: dps://, **Hosts:** com.dps.h5,  |
| com.shyl.dps.ui.LauncherActivity | **Schemes**: dps://, **Hosts:** com.shyl.dps,  |
| com.allinpay.unifypay.sdk.ui.PaymentActivity | **Schemes**: allinpaysdk://, **Hosts:** com.shyl.dps, **Paths:** /result,  |

**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。**