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

**逗逗游戏伙伴（ 2.5.2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 | 逗逗游戏伙伴 |
| 版本 | 2.5.2 |
| 包名 | fun.doudou.pal |
| 域名线索 | 86条 |
| URL线索 | 79条 |
| APP图标 |  |
| 分析日期 | 2025年1月10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 | 逗逗游戏伙伴.apk |
| 文件大小 | 90.98MB |
| MD5值 | fb2b0a3dc509b5298ebd1f40c0873386 |
| SHA1值 | 3dd940aaa2dff0acfd302ecf6d9fe55d40d4e0ad |
| SHA256值 | 1a3eccd7cf5d00e2e0d01477cfc605febd3223fc60df09e25c71247c79979647 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 逗逗游戏伙伴 |
| 包名 | fun.doudou.pal |
| 主活动Activity | com.huoban.ai.huobanai.MainActivity |
| 安卓版本名称 | 2.5.2 |
| 安卓版本 | 74 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| h.trace.qq.com | IP: 113.56.189.246 所属国家: China 地区: Hubei 城市: Huangshi  |
| rtlog.snssdk.com | IP: 60.222.11.202 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| docs.flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| loggw-exsdk.alipay.com | IP: 119.42.231.3 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| 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.  |
| data-drru.push.dbankcloud.com | IP: 159.138.202.31 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| cgi.connect.qq.com | IP: 60.28.215.27 所属国家: China 地区: Tianjin 城市: Tianjin  |
| metrics5.dt.dbankcloud.ru | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| resolver.msg.xiaomi.net | IP: 114.247.154.13 所属国家: China 地区: Beijing 城市: Beijing  |
| developer.mozilla.org | IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| grs.dbankcloud.cn | IP: 49.4.35.251 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| grs.dbankcloud.asia | IP: 49.4.35.251 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| imapi-boe.sinf.net | IP: 10.27.207.218 所属国家: - 地区: - 城市: -  |
| abtest.volceapplog.com | IP: 221.194.162.226 所属国家: China 地区: Hebei 城市: Langfang  |
| metrics5.data.hicloud.com | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| tobapplog.volceapplog.com | IP: 60.9.1.105 所属国家: China 地区: Hebei 城市: Hengshui  |
| issuetracker.google.com | IP: 142.251.33.78 所属国家: Canada 地区: Ontario 城市: Toronto  |
| play.google.com | IP: 46.82.174.69 所属国家: Germany 地区: Niedersachsen 城市: Braunschweig  |
| stackoverflow.com | IP: 104.18.32.7 所属国家: United States of America 地区: California 城市: San Francisco  |
| metrics1-drcn.dt.dbankcloud.cn | IP: 111.202.16.252 所属国家: China 地区: Beijing 城市: Beijing  |
| app.mi.com | IP: 123.125.102.202 所属国家: China 地区: Beijing 城市: Beijing  |
| cgi.qplus.com | 没有服务器地理信息.  |
| neptune-platform.zijieapi.com | IP: 101.26.38.241 所属国家: China 地区: Hebei 城市: Handan  |
| dashif.org | IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| klink.volceapplog.com | IP: 220.194.69.119 所属国家: China 地区: Tianjin 城市: Tianjin  |
| api.magicneko.com | IP: 101.126.44.28 所属国家: China 地区: Beijing 城市: Beijing  |
| dev.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| openmobile.qq.com | IP: 60.28.215.27 所属国家: China 地区: Tianjin 城市: Tianjin  |
| alink.volceapplog.com | IP: 120.52.77.206 所属国家: China 地区: Hebei 城市: Langfang  |
| rtapplog.snssdk.com | IP: 106.74.132.38 所属国家: China 地区: Shandong 城市: Jinan  |
| h5.m.taobao.com | IP: 218.11.15.29 所属国家: China 地区: Hebei 城市: Shijiazhuang  |
| imgcache.qq.com | IP: 116.196.145.220 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| open.weixin.qq.com | IP: 140.207.191.167 所属国家: China 地区: Shanghai 城市: Shanghai  |
| mobilegw.alipaydev.com | IP: 110.75.132.131 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| data-dre.push.dbankcloud.com | IP: 80.158.49.244 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| grs.dbankcloud.com | IP: 60.28.193.195 所属国家: China 地区: Tianjin 城市: Tianjin  |
| www.google.com | IP: 31.13.112.9 所属国家: Ireland 地区: Dublin 城市: Dublin  |
| ns.adobe.com | 没有服务器地理信息.  |
| xmlpull.org | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| mobilegwpre.alipay.com | IP: 110.75.138.35 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| www.slf4j.org | IP: 159.100.250.151 所属国家: Switzerland 地区: Zurich 城市: Zurich  |
| android.bugly.qq.com | IP: 124.95.225.169 所属国家: China 地区: Liaoning 城市: Shenyang  |
| schemas.microsoft.com | IP: 13.107.246.73 所属国家: United States of America 地区: Washington 城市: Redmond  |
| log.snssdk.com | IP: 123.125.216.194 所属国家: China 地区: Beijing 城市: Beijing  |
| 10.38.162.35 | IP: 10.38.162.35 所属国家: - 地区: - 城市: -  |
| wappaygw.alipay.com | IP: 123.125.216.192 所属国家: China 地区: Beijing 城市: Beijing  |
| www.volcengine.com | IP: 61.182.131.176 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| mp.weixin.qq.com | IP: 220.196.132.78 所属国家: China 地区: Jiangsu 城市: Zhenjiang  |
| mclient.alipay.com | IP: 116.142.234.200 所属国家: China 地区: Beijing 城市: Beijing  |
| astat.bugly.qcloud.com | IP: 119.28.121.133 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| mcgw.alipay.com | IP: 123.125.216.192 所属国家: China 地区: Beijing 城市: Beijing  |
| apmplus.volces.com | IP: 61.182.131.160 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| default.url | 没有服务器地理信息.  |
| databyterangers.com.cn | 没有服务器地理信息.  |
| toblog.ctobsnssdk.com | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| 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  |
| applog.snssdk.com | IP: 61.182.131.172 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| toblog.volceapplog.com | IP: 61.182.131.161 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| www.example.com | IP: 93.184.215.14 所属国家: United States of America 地区: California 城市: Los Angeles  |
| gator.volces.com | IP: 120.52.77.224 所属国家: China 地区: Hebei 城市: Langfang  |
| tobapplog.ctobsnssdk.com | IP: 101.26.38.241 所属国家: China 地区: Hebei 城市: Handan  |
| toblog-alink.ctobsnssdk.com | IP: 120.52.77.207 所属国家: China 地区: Hebei 城市: Langfang  |
| a.app.qq.com | IP: 60.28.219.32 所属国家: China 地区: Tianjin 城市: Tianjin  |
| developer.apple.com | IP: 17.253.87.200 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| cn.register.xmpush.xiaomi.com | IP: 221.194.179.52 所属国家: China 地区: Hebei 城市: Langfang  |
| developer.android.com | IP: 142.251.215.238 所属国家: United States of America 地区: California 城市: Mountain View  |
| mobilegw.alipay.com | IP: 203.209.255.238 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| 10.0.2.2 | IP: 10.0.2.2 所属国家: - 地区: - 城市: -  |
| www.gnu.org | IP: 209.51.188.116 所属国家: United States of America 地区: Massachusetts 城市: Somerville  |
| grs.platform.dbankcloud.ru | 没有服务器地理信息.  |
| metrics-dra.dt.hicloud.com | IP: 94.74.88.100 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| paulbakaus.com | IP: 167.172.18.193 所属国家: United States of America 地区: New Jersey 城市: Clifton  |
| data-drcn.push.dbankcloud.com | IP: 49.4.40.58 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| appsupport.qq.com | IP: 60.28.215.27 所属国家: China 地区: Tianjin 城市: Tianjin  |
| g.co | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| metrics2.data.hicloud.com | IP: 80.158.2.190 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| ichannel.snssdk.com | IP: 123.125.216.196 所属国家: China 地区: Beijing 城市: Beijing  |
| aomedia.org | IP: 69.171.247.71 所属国家: United States of America 地区: New York 城市: New York City  |
| imapi.bytepluses.com | IP: 92.122.166.238 所属国家: France 地区: Ile-de-France 城市: Paris  |
| long.open.weixin.qq.com | IP: 112.65.193.150 所属国家: China 地区: Shanghai 城市: Shanghai  |
| imapi.volcvideo.com | IP: 221.204.58.138 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| mobilegw.dl.alipaydev.com | IP: 110.75.132.25 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| pagead2.googlesyndication.com | IP: 114.250.65.38 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://developer.android.com/guide/topics/media/issues/cleartext-not-permitted  | a1/p.java  |
| http://g.co/dev/packagevisibility.  | a1/v.java  |
| https://developer.android.com/guide/topics/media/issues/player-accessed-on-wrong-thread  | bd/b1.java  |
| http://undefined/  | bn/d.java  |
| https://developer.android.com/guide/topics/media/issues/player-accessed-on-wrong-thread  | c1/r0.java  |
| https://mobilegw.alipay.com/mgw.htm  | com/alipay/apmobilesecuritysdk/b/a.java  |
| https://mobilegwpre.alipay.com/mgw.htm  | com/alipay/apmobilesecuritysdk/b/a.java  |
| https://wappaygw.alipay.com/home/exterfaceAssign.htm?  | com/alipay/sdk/app/PayTask.java  |
| https://mclient.alipay.com/home/exterfaceAssign.htm?  | com/alipay/sdk/app/PayTask.java  |
| https://wappaygw.alipay.com/service/rest.htm  | com/alipay/sdk/app/PayTask.java  |
| http://wappaygw.alipay.com/service/rest.htm  | com/alipay/sdk/app/PayTask.java  |
| https://mclient.alipay.com/service/rest.htm  | com/alipay/sdk/app/PayTask.java  |
| http://mclient.alipay.com/service/rest.htm  | com/alipay/sdk/app/PayTask.java  |
| https://mclient.alipay.com/home/exterfaceAssign.htm  | com/alipay/sdk/app/PayTask.java  |
| http://mclient.alipay.com/home/exterfaceAssign.htm  | com/alipay/sdk/app/PayTask.java  |
| https://mclient.alipay.com/cashier/mobilepay.htm  | com/alipay/sdk/app/PayTask.java  |
| http://mclient.alipay.com/cashier/mobilepay.htm  | com/alipay/sdk/app/PayTask.java  |
| https://apmplus.volces.com/monitor/collect/c/cloudcontrol/file  | com/apm/insight/runtime/ConfigManager.java  |
| https://apmplus.volces.com/monitor/collect/c/native\_bin\_crash  | com/apm/insight/runtime/ConfigManager.java  |
| https://apmplus.volces.com/settings/get  | com/apm/insight/runtime/ConfigManager.java  |
| https://apmplus.volces.com/monitor/collect/c/core\_dump\_collect  | com/apm/insight/runtime/ConfigManager.java  |
| https://apmplus.volces.com/monitor/collect/c/exception  | com/apm/insight/runtime/ConfigManager.java  |
| https://apmplus.volces.com/monitor/collect/c/logcollect  | com/apm/insight/runtime/ConfigManager.java  |
| https://apmplus.volces.com/monitor/collect/c/crash  | com/apm/insight/runtime/ConfigManager.java  |
| https://apmplus.volces.com/monitor/collect/c/exception/dump\_collection  | com/apm/insight/runtime/ConfigManager.java  |
| https://apmplus.volces.com/monitor/collect/c/rapheal\_file\_collect  | com/apm/insight/runtime/ConfigManager.java  |
| https://www.volcengine.com/docs/6348/291089  | com/bytedance/im/core/api/expand/ExpandManager.java  |
| https://gator.volces.com  | com/bytedance/im/log/managers/ALogEventManager.java  |
| https://imapi.volcvideo.com/  | com/bytedance/im/env/BIMEnvService.java  |
| https://imapi-boe.sinf.net/  | com/bytedance/im/env/BIMEnvService.java  |
| https://imapi.bytepluses.com/  | com/bytedance/im/env/BIMEnvService.java  |
| http://www.example.com  | com/pichillilorenzo/flutter\_inappwebview\_android/chrome\_custom\_tabs/CustomTabsHelper.java  |
| https://android.bugly.qq.com/rqd/async  | com/tencent/bugly/crashreport/common/strategy/StrategyBean.java  |
| https://astat.bugly.qcloud.com/rqd/async  | com/tencent/bugly/crashreport/common/strategy/c.java  |
| https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async  | com/tencent/bugly/crashreport/common/strategy/c.java  |
| https://openmobile.qq.com/oauth2.0/me  | com/tencent/connect/UnionInfo.java  |
| https://cgi.qplus.com/report/report  | com/tencent/connect/avatar/ImageActivity.java  |
| https://openmobile.qq.com/oauth2.0/m\_jump\_by\_version?  | com/tencent/connect/common/BaseApi.java  |
| https://imgcache.qq.com/ptlogin/static/qzsjump.html?  | com/tencent/connect/common/BaseApi.java  |
| https://imgcache.qq.com/ptlogin/static/qzsjump.html?  | com/tencent/connect/auth/a.java  |
| https://openmobile.qq.com/oauth2.0/m\_authorize?  | com/tencent/connect/auth/AuthAgent.java  |
| https://openmobile.qq.com/v3/user/get\_info  | com/tencent/connect/auth/AuthAgent.java  |
| https://appsupport.qq.com/cgi-bin/qzapps/mapp\_addapp.cgi  | com/tencent/connect/auth/AuthAgent.java  |
| https://openmobile.qq.com/user/user\_login\_statis  | com/tencent/connect/auth/AuthAgent.java  |
| https://imgcache.qq.com/open/mobile/invite/sdk\_invite.html?  | com/tencent/open/SocialApiIml.java  |
| https://imgcache.qq.com/open/mobile/sendstory/sdk\_sendstory\_v1.3.html?  | com/tencent/open/SocialApiIml.java  |
| https://imgcache.qq.com  | com/tencent/open/SocialApiIml.java  |
| https://imgcache.qq.com/open/mobile/request/sdk\_request.html?  | com/tencent/open/SocialApiIml.java  |
| https://openmobile.qq.com/cgi-bin/qunopensdk/check\_group  | com/tencent/open/SocialOperation.java  |
| https://openmobile.qq.com/cgi-bin/qunopensdk/unbind  | com/tencent/open/SocialOperation.java  |
| https://appsupport.qq.com/cgi-bin/appstage/mstats\_batch\_report  | com/tencent/open/b/h.java  |
| https://h.trace.qq.com/kv  | com/tencent/open/b/b.java  |
| https://cgi.connect.qq.com/qqconnectopen/openapi/policy\_conf  | com/tencent/open/utils/i.java  |
| https://openmobile.qq.com/  | com/tencent/open/utils/HttpUtils.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://gator.volces.com/v2/event/json  | com/huoban/ai/huobanai/utils/TraceApi.java  |
| https://api.magicneko.com:8760  | com/huoban/ai/huobanai/utils/HttpUtils.java  |
| http://10.38.162.35:9085  | com/xiaomi/push/service/v0.java  |
| https://cn.register.xmpush.xiaomi.com  | com/xiaomi/push/service/v0.java  |
| https://resolver.msg.xiaomi.net/psc/?t=a  | com/xiaomi/push/service/z.java  |
| http://www.slf4j.org/codes.html  | ao/b.java  |
| https://neptune-platform.zijieapi.com  | dj/d.java  |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense  | fd/g0.java  |
| https://x</LA\_URL>  | fd/f0.java  |
| https://default.url  | fd/f0.java  |
| http://dashif.org/guidelines/last-segment-number  | g1/d.java  |
| http://dashif.org/guidelines/trickmode  | g1/d.java  |
| http://dashif.org/thumbnail\_tile  | g1/d.java  |
| http://dashif.org/guidelines/thumbnail\_tile  | g1/d.java  |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense  | h1/i0.java  |
| https://x</LA\_URL>  | h1/h0.java  |
| https://default.url  | h1/h0.java  |
| https://play.google.com/store/apps/details?id=  | hb/a.java  |
| http://www.google.com  | hb/a.java  |
| https://a.app.qq.com/o/simple.jsp?pkgname=  | hb/b.java  |
| https://app.mi.com/details?id=  | hb/c.java  |
| https://app.mi.com  | hb/c.java  |
| http://dashif.org/guidelines/last-segment-number  | ie/d.java  |
| http://dashif.org/guidelines/trickmode  | ie/d.java  |
| http://dashif.org/thumbnail\_tile  | ie/d.java  |
| http://dashif.org/guidelines/thumbnail\_tile  | ie/d.java  |
| https://docs.flutter.dev/deployment/android  | io/flutter/embedding/engine/loader/FlutterLoader.java  |
| https://developer.android.com/guide/topics/permissions/overview  | io/flutter/plugin/platform/PlatformPlugin.java  |
| https://github.com/flutter/packages/blob/main/packages/in\_app\_purchase/in\_app\_purchase/README.md  | io/flutter/plugins/inapppurchase/MethodCallHandlerImpl.java  |
| http://10.0.2.2:8969/stream  | io/sentry/SpotlightIntegration.java  |
| http://xmlpull.org/v1/doc/features.html  | mk/s4.java  |
| http://xmlpull.org/v1/doc/features.html  | mk/h5.java  |
| https://%1$s/gslb/?ver=5.0  | mk/i1.java  |
| http://xmlpull.org/v1/doc/features.html  | mk/i5.java  |
| http://xmlpull.org/v1/doc/features.html  | mk/h4.java  |
| https://databyterangers.com.cn  | n9/p3.java  |
| https://issuetracker.google.com/issues/new?component=413107&template=1096568  | o3/c.java  |
| https://mobilegw.alipaydev.com/mgw.htm  | o6/l.java  |
| https://mobilegw.dl.alipaydev.com/mgw.htm  | o6/l.java  |
| https://github.com/Baseflow/flutter-permission-handler/issues  | t7/p.java  |
| https://log.snssdk.com/apm/device\_register  | w4/s.java  |
| https://ichannel.snssdk.com/service/2/app\_alert\_check/  | w4/s.java  |
| https://log.snssdk.com/monitor/collect/c/session  | w4/s.java  |
| https://applog.snssdk.com/monitor/collect/c/session  | w4/s.java  |
| https://rtlog.snssdk.com/monitor/collect/c/session  | w4/s.java  |
| https://rtapplog.snssdk.com/monitor/collect/c/session  | w4/s.java  |
| https://log.snssdk.com/service/2/log\_settings/  | w4/s.java  |
| https://toblog-alink.ctobsnssdk.com/service/2/attribution\_data  | w4/s.java  |
| https://toblog-alink.ctobsnssdk.com/service/2/alink\_data  | w4/s.java  |
| https://apmplus.volces.com/apm/device\_register  | w4/s.java  |
| https://apmplus.volces.com/monitor/collect/c/session  | w4/s.java  |
| https://developer.android.com/guide/topics/media/issues/cleartext-not-permitted  | xe/x.java  |
| https://mobilegw.alipay.com/mgw.htm  | z5/a.java  |
| https://issuetracker.google.com/issues/new?component=907884&template=1466542  | i0/m.java  |
| https://pagead2.googlesyndication.com/pagead/gen\_204?id=gmob-apps  | bf/b.java  |
| https://log.snssdk.com/service/2/device\_register/  | m9/c.java  |
| https://log.snssdk.com/service/2/device\_update  | m9/c.java  |
| https://ichannel.snssdk.com/service/2/app\_alert\_check/  | m9/c.java  |
| https://log.snssdk.com/service/2/app\_log/  | m9/c.java  |
| https://applog.snssdk.com/service/2/app\_log/  | m9/c.java  |
| https://log.snssdk.com/service/2/log\_settings/  | m9/c.java  |
| https://toblog-alink.ctobsnssdk.com/service/2/attribution\_data  | m9/c.java  |
| https://toblog-alink.ctobsnssdk.com/service/2/alink\_data  | m9/c.java  |
| https://toblog.ctobsnssdk.com/service/2/device\_register/  | m9/c.java  |
| https://toblog.ctobsnssdk.com/service/2/device\_update  | m9/c.java  |
| https://toblog.ctobsnssdk.com/service/2/app\_alert\_check/  | m9/c.java  |
| https://toblog.ctobsnssdk.com/service/2/app\_log/  | m9/c.java  |
| https://tobapplog.ctobsnssdk.com/service/2/app\_log/  | m9/c.java  |
| https://toblog.ctobsnssdk.com/service/2/profile/  | m9/c.java  |
| https://toblog.ctobsnssdk.com/service/2/log\_settings/  | m9/c.java  |
| https://toblog.ctobsnssdk.com/service/2/abtest\_config/  | m9/c.java  |
| https://klink.volceapplog.com/service/2/device\_register/  | m9/c.java  |
| https://klink.volceapplog.com/service/2/device\_update  | m9/c.java  |
| https://klink.volceapplog.com/service/2/app\_alert\_check/  | m9/c.java  |
| https://toblog.volceapplog.com/service/2/app\_log/  | m9/c.java  |
| https://tobapplog.volceapplog.com/service/2/app\_log/  | m9/c.java  |
| https://toblog.volceapplog.com/service/2/profile/  | m9/c.java  |
| https://toblog.volceapplog.com/service/2/log\_settings/  | m9/c.java  |
| https://abtest.volceapplog.com/service/2/abtest\_config/  | m9/c.java  |
| https://alink.volceapplog.com/service/2/attribution\_data  | m9/c.java  |
| https://alink.volceapplog.com/service/2/alink\_data  | m9/c.java  |
| http://ns.adobe.com/xap/1.0/  | j2/b.java  |
| http://ns.adobe.com/xap/1.0/  | ld/a.java  |
| https://aomedia.org/emsg/ID3  | m2/a.java  |
| https://developer.apple.com/streaming/emsg-id3  | m2/a.java  |
| https://aomedia.org/emsg/ID3  | vd/a.java  |
| https://developer.apple.com/streaming/emsg-id3  | vd/a.java  |
| https://h5.m.taobao.com/mlapp/olist.html  | b6/a.java  |
| https://mcgw.alipay.com/sdklog.do  | i6/c.java  |
| https://loggw-exsdk.alipay.com/loggw/logUpload.do  | i6/d.java  |
| https://databyterangers.com.cn  | o4/a.java  |
| https://data-drcn.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-dra.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-dre.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-drru.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://metrics1-drcn.dt.dbankcloud.cn:443  | 摸瓜V2引擎  |
| https://metrics-dra.dt.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics2.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics5.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics5.dt.dbankcloud.ru:6447  | 摸瓜V2引擎  |
| https://grs.dbankcloud.com  | 摸瓜V2引擎  |
| https://grs.dbankcloud.cn  | 摸瓜V2引擎  |
| https://grs.dbankcloud.asia  | 摸瓜V2引擎  |
| https://grs.platform.dbankcloud.ru  | 摸瓜V2引擎  |
| https://grs.dbankcloud.eu  | 摸瓜V2引擎  |
| http://paulbakaus.com/tutorials/html5/web-audio-on-ios/  | 摸瓜V2引擎  |
| http://stackoverflow.com/questions/24119684  | 摸瓜V2引擎  |
| https://www.gnu.org/licenses/>.  | 摸瓜V2引擎  |
| https://www.gnu.org/licenses/>.  | 摸瓜V2引擎  |
| https://www.gnu.org/licenses/>.  | 摸瓜V2引擎  |
| https://github.com/richtr/NoSleep.js/issues/15  | 摸瓜V2引擎  |
| https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released)  | 摸瓜V2引擎  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| u0013android@android.com0 u0013android@android.com  | ef/w.java  |
| bg\_dialog@2x.png bg\_login@2x.png bg\_set@2x.png bg\_update@2x.png chat\_audio\_play\_00@2x.png chat\_audio\_play\_01@2x.png chat\_audio\_play\_02@2x.png chat\_edit\_choose@2x.png chat\_edit\_not\_choose@2x.png chat\_sending@2x.png diamond@2x.png game\_back@2x.png header\_im@2x.png header\_img@2x.png help@2x.png home\_audition\_pause@2x.png home\_audition\_play@2x.png home\_call@2x.png home\_display\_ip@2x.png ome\_display\_official@2x.png home\_display\_user@2x.png home\_slogan\_cn@2x.png icon\_add\_green@2x.png icon\_app\_upgrade@2x.png icon\_apple\_login@2x.png icon\_arrow@2x.png icon\_avatar@2x.png icon\_back@2x.png icon\_back\_white@2x.png icon\_circle\_selected@2x.png on\_circle\_unselected@2x.png icon\_clear@2x.png icon\_clear\_text@2x.png icon\_clock@2x.png icon\_close\_gray@2x.png icon\_copy@2x.png icon\_copy\_white@2x.png icon\_edit@2x.png icon\_email@2x.png icon\_error@2x.png icon\_game\_btn@2x.png icon\_game\_selected@2x.png icon\_game\_unselect@2x.png icon\_google\_login@2x.png icon\_home\_selected@2x.png icon\_home\_unselect@2x.png icon\_interrupt\_talk@2x.png icon\_me\_selected@2x.png icon\_me\_unselect@2x.png icon\_message@2x.png icon\_message\_en@2x.png icon\_message\_ja@2x.png con\_message\_selected@2x.png con\_message\_unselect@2x.png icon\_or@2x.png icon\_password@2x.png icon\_qq\_login@2x.png icon\_refresh@2x.png icon\_rtc\_game@2x.png icon\_rtc\_handset\_off@2x.png icon\_rtc\_handset\_on@2x.png icon\_rtc\_time@2x.png icon\_selected@2x.png icon\_send\_msg@2x.png icon\_set@2x.png on\_transparency\_back@2x.png icon\_weixin\_login@2x.png on\_white\_apple\_login@2x.png n\_white\_google\_login@2x.png ne\_physical\_strength@2x.png my\_widget\_bg@2x.png open\_prop\_shop@2x.png open\_rtc\_call@2x.png prop\_shop\_a-level@2x.png prop\_shop\_d\_coin@2x.png prop\_shop\_lightning@2x.png \_shop\_lightning\_icon@2x.png prop\_shop\_n-level@2x.png prop\_shop\_neko\_icon@2x.png prop\_shop\_s-level@2x.png prop\_tip\_icon@2x.png reload\_topic@2x.png send\_enable@2x.png send\_fail@2x.png sending@2x.png task\_card\_bg@2x.png task\_reward\_bg@2x.png topup\_ali\_pay@2x.png opup\_double\_recharge@2x.png topup\_entrance@2x.png topup\_first\_recharge@2x.png imited\_time\_recharge@2x.png topup\_tick\_icon@2x.png widget\_close\_dialog@2x.png widget\_help@2x.png widget\_mine\_widget@2x.png t\_selected\_character@2x.png bg\_mine\_header@2x.png icon\_redeem@2x.png  | 摸瓜V2引擎  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17512775099  | bg/a.java  |
| 19222222222  | md/e.java  |
| 19222222222  | t2/e.java  |

## **5. 签名证书**

**APK已签名 v1 签名: False v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: CN=xinyingsuixing, OU=xinyingsuixing, O=xinyingsuixing, L=beijing, ST=beijing, C=cn 签名算法: rsassa\_pkcs1v15 有效期自: 2024-02-23 09:09:55+00:00 有效期至: 2049-02-16 09:09:55+00:00 发行人: CN=xinyingsuixing, OU=xinyingsuixing, O=xinyingsuixing, L=beijing, ST=beijing, C=cn 序列号: 0x1 哈希算法: sha256 md5值: 56d879841c1ca4fc512abc03d5de2237 sha1值: 35c67e7803ee238428a9c9a500154f6e3c5688be sha256值: 06abc151c1957e51b59e841d442da80208ecbe745d663689e3b98aa90c4efe10 sha512值: 5a176931f88a4ce52161eb9eb2a02cc1de24917628d2c62f80dda7bca3103fb4218c278f8cdda38725504bfd556c68b781f004be9ea4641d0f981c439fb731ae 公钥算法: rsa 密钥长度: 2048 指纹: 63603aab08f58c1b2dee77f54356accb2b233961d0e70831296296013cfcab47**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "google\_api\_key" : "AIzaSyAKrOzk4Up-r-47VhWIqDULkPHmFH5Wtso"  |
| "google\_crash\_reporting\_api\_key" : "AIzaSyAKrOzk4Up-r-47VhWIqDULkPHmFH5Wtso"  |

## **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.SYSTEM\_ALERT\_WINDOW | 危险 | 显示系统级警报 | 允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕 |
| android.permission.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.CAMERA | 危险 | 拍照和录像 | 允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像 |
| android.permission.READ\_EXTERNAL\_STORAGE | 危险 | 读取外部存储器内容 | 允许应用程序从外部存储读取 |
| android.permission.READ\_MEDIA\_IMAGES | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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 |
| com.android.launcher.permission.INSTALL\_SHORTCUT | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ACCESS\_NETWORK\_STATE | 正常 | 查看网络状态 | 允许应用程序查看所有网络的状态 |
| android.permission.ACCESS\_WIFI\_STATE | 正常 | 查看Wi-Fi状态 | 允许应用程序查看有关 Wi-Fi 状态的信息 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| fun.doudou.pal.permission.MIPUSH\_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.FOREGROUND\_SERVICE\_MEDIA\_PROJECTION | 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.CHANGE\_NETWORK\_STATE | 正常 | 更改网络连接 | 允许应用程序更改网络连接状态。 |
| com.vivo.aiengine.permission.READ\_AWARE\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| com.vivo.aiengine.permission.WRITE\_AWARE\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |
| Manifest.permission.CAPTURE\_AUDIO\_OUTPUT | 未知 | Unknown permission | Unknown permission from android reference |
| com.android.vending.BILLING | 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 |
| android.permission.ACCESS\_ADSERVICES\_ATTRIBUTION | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ACCESS\_ADSERVICES\_AD\_ID | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.finsky.permission.BIND\_GET\_INSTALL\_REFERRER\_SERVICE | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |
| fun.doudou.pal.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| fun.doudou.pal.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| fun.doudou.pal.permission.PUSH\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| com.hihonor.push.permission.READ\_PUSH\_NOTIFICATION\_INFO | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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。 |
| 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 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.huoban.ai.huobanai.MainActivity | **Schemes**: doudouyouxi://, **Hosts:** fun,  |
| com.tencent.tauth.AuthActivity | **Schemes**: tencent102097012://,  |

**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。**