MoGua

逗逗游戏伙伴 2.5.2.APK 分析报告

APP名称:	逗逗游戏伙伴
包名:	fun.doudou.pal
域名线索:	86条

URL线索:	79条
邮箱线索:	2条
分析日期:	2025年1月9日
分析平台:	摸瓜APK反编译平台

文件信息

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

APP 信息

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

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 **纬度**: 30.204170 **经度**: 115.077606
rtlog.snssdk.com	**IP**: 60.222.11.202 **所属国家**: China **地区**: Shanxi **城市**: Taiyuan **纬度**: 37.869438 **经度**: 112.561508
docs.flutter.dev	**IP**: 199.36.158.100 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
loggw-exsdk.alipay.com	**IP**: 119.42.231.3 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
data-dra.push.dbankcloud.com	**IP**: 119.8.163.189 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
grs.dbankcloud.eu	没有服务器地理信息.
	IP: 159.138.202.31

data-drru.push.dbankcloud.com	**所属国家**: Russian Federation **地区**: Sverdlovskaya oblast' **城市**: Yekaterinburg **纬度**: 56.857498 **经度**: 60.612499
cgi.connect.qq.com	IP: 60.28.215.27 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
metrics5.dt.dbankcloud.ru	IP: 159.138.203.215 **所属国家**: Russian Federation **地区**: Sverdlovskaya oblast' **城市**: Yekaterinburg **纬度**: 56.857498 **经度**: 60.612499
resolver.msg.xiaomi.net	IP: 114.247.154.13 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
developer.mozilla.org	IP: 34.111.97.67 **所属国家**: United States of America **地区**: Missouri **城市**: Kansas City **纬度**: 39.099731 **经度**: -94.578568
grs.dbankcloud.cn	IP: 49.4.35.251 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
grs.dbankcloud.asia	IP: 49.4.35.251 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572

imapi-boe.sinf.net	IP: 10.27.207.218 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
abtest.volceapplog.com	IP: 221.194.162.226 **所属国家**: China **地区**: Hebei **城市**: Langfang **纬度**: 39.509720 **经度**: 116.694717
metrics5.data.hicloud.com	IP: 159.138.203.215 **所属国家**: Russian Federation **地区**: Sverdlovskaya oblast' **城市**: Yekaterinburg **纬度**: 56.857498 **经度**: 60.612499
tobapplog.volceapplog.com	IP: 60.9.1.105 **所属国家**: China **地区**: Hebei **城市**: Hengshui **纬度**: 37.732220 **经度**: 115.701157
issuetracker.google.com	IP: 142.251.33.78 **所属国家**: Canada **地区**: Ontario **城市**: Toronto **纬度**: 43.653660 **经度**: -79.382927
play.google.com	IP: 46.82.174.69 **所属国家**: Germany **地区**: Niedersachsen **城市**: Braunschweig **纬度**: 52.266121 **经度**: 10.526730
stackoverflow.com	IP: 104.18.32.7 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700

	经度: -122.395203
metrics1-drcn.dt.dbankcloud.cn	**IP**: 111.202.16.252 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
app.mi.com	**IP**: 123.125.102.202 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
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 **纬度**: 36.600559 **经度**: 114.467781
dashif.org	**IP**: 185.199.108.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
klink.volceapplog.com	**IP**: 220.194.69.119 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
api.magicneko.com	**IP**: 101.126.44.28 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102

dev.w3.org	**IP**: 104.18.22.19 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
openmobile.qq.com	**IP**: 60.28.215.27 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
alink.volceapplog.com	**IP**: 120.52.77.206 **所属国家**: China **地区**: Hebei **城市**: Langfang **纬度**: 39.509720 **经度**: 116.694717
rtapplog.snssdk.com	**IP**: 106.74.132.38 **所属国家**: China **地区**: Shandong **城市**: Jinan **纬度**: 36.668331 **经度**: 116.997223
h5.m.taobao.com	**IP**: 218.11.15.29 **所属国家**: China **地区**: Hebei **城市**: Shijiazhuang **纬度**: 38.041599 **经度**: 114.478081
imgcache.qq.com	**IP**: 116.196.145.220 **所属国家**: China **地区**: Zhejiang **城市**: Jinhua **纬度**: 30.013470 **经度**: 120.288658
www.w3.org	**IP**: 104.18.22.19 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700

	经度: -122.395203
open.weixin.qq.com	**IP**: 140.207.191.167 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
mobilegw.alipaydev.com	**IP**: 110.75.132.131 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
data-dre.push.dbankcloud.com	**IP**: 80.158.49.244 **所属国家**: Germany **地区**: Schleswig-Holstein **城市**: Kiel **纬度**: 54.321358 **经度**: 10.134532
grs.dbankcloud.com	**IP**: 60.28.193.195 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
www.google.com	**IP**: 31.13.112.9 **所属国家**: Ireland **地区**: Dublin **城市**: Dublin **纬度**: 53.344151 **经度**: -6.267249
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 **纬度**: 40.065647 **经度**: -79.891724
	IP: 20.205.243.166

github.com	**所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
mobilegwpre.alipay.com	**IP**: 110.75.138.35 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
www.slf4j.org	**IP**: 159.100.250.151 **所属国家**: Switzerland **地区**: Zurich **城市**: Zurich **纬度**: 47.366825 **经度**: 8.549790
android.bugly.qq.com	**IP**: 124.95.225.169 **所属国家**: China **地区**: Liaoning **城市**: Shenyang **纬度**: 41.792221 **经度**: 123.432877
schemas.microsoft.com	**IP**: 13.107.246.73 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
log.snssdk.com	**IP**: 123.125.216.194 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
10.38.162.35	**IP**: 10.38.162.35 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000

wappaygw.alipay.com	IP: 123.125.216.192 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
www.volcengine.com	IP: 61.182.131.176 **所属国家**: China **地区**: Hebei **城市**: Zhangjiakou **纬度**: 40.810024 **经度**: 114.879349
mp.weixin.qq.com	IP: 220.196.132.78 **所属国家**: China **地区**: Jiangsu **城市**: Zhenjiang **纬度**: 32.209366 **经度**: 119.434372
mclient.alipay.com	IP: 116.142.234.200 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
astat.bugly.qcloud.com	IP: 119.28.121.133 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
mcgw.alipay.com	IP: 123.125.216.192 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
apmplus.volces.com	IP: 61.182.131.160 **所属国家**: China **地区**: Hebei **城市**: Zhangjiakou **纬度**: 40.810024

	经度: 114.879349
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**: - **纬度**: 0.000000 **经度**: 0.000000
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 **纬度**: 37.774929 **经度**: -122.419418
applog.snssdk.com	**IP**: 61.182.131.172 **所属国家**: China **地区**: Hebei **城市**: Zhangjiakou **纬度**: 40.810024 **经度**: 114.879349
toblog.volceapplog.com	**IP**: 61.182.131.161 **所属国家**: China **地区**: Hebei **城市**: Zhangjiakou **纬度**: 40.810024 **经度**: 114.879349
www.example.com	**IP**: 93.184.215.14 **所属国家**: United States of America **地区**: California **城市**: Los Angeles **纬度**: 34.052570 **经度**: -118.243904
gator.volces.com	**IP**: 120.52.77.224 **所属国家**: China **地区**: Hebei **城市**: Langfang **纬度**: 39.509720

	经度: 116.694717
tobapplog.ctobsnssdk.com	**IP**: 101.26.38.241 **所属国家**: China **地区**: Hebei **城市**: Handan **纬度**: 36.600559 **经度**: 114.467781
toblog-alink.ctobsnssdk.com	**IP**: 120.52.77.207 **所属国家**: China **地区**: Hebei **城市**: Langfang **纬度**: 39.509720 **经度**: 116.694717
a.app.qq.com	**IP**: 60.28.219.32 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
developer.apple.com	**IP**: 17.253.87.200 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
cn.register.xmpush.xiaomi.com	**IP**: 221.194.179.52 **所属国家**: China **地区**: Hebei **城市**: Langfang **纬度**: 39.509720 **经度**: 116.694717
developer.android.com	**IP**: 142.251.215.238 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
	IP: 203.209.255.238 **所属国家**: China **地区**: Zhejiang

mobilegw.alipay.com	**城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
10.0.2.2	**IP**: 10.0.2.2 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
www.gnu.org	**IP**: 209.51.188.116 **所属国家**: United States of America **地区**: Massachusetts **城市**: Somerville **纬度**: 42.387600 **经度**: -71.099503
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 **纬度**: 1.289987 **经度**: 103.850281
paulbakaus.com	**IP**: 167.172.18.193 **所属国家**: United States of America **地区**: New Jersey **城市**: Clifton **纬度**: 40.858585 **经度**: -74.163605
data-drcn.push.dbankcloud.com	**IP**: 49.4.40.58 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
appsupport.qq.com	**IP**: 60.28.215.27 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181

	经度: 117.176102
g.co	**IP**: 127.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
metrics2.data.hicloud.com	**IP**: 80.158.2.190 **所属国家**: Germany **地区**: Schleswig-Holstein **城市**: Kiel **纬度**: 54.321358 **经度**: 10.134532
ichannel.snssdk.com	**IP**: 123.125.216.196 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
aomedia.org	**IP**: 69.171.247.71 **所属国家**: United States of America **地区**: New York **城市**: New York City **纬度**: 40.713192 **经度**: -74.006065
imapi.bytepluses.com	**IP**: 92.122.166.238 **所属国家**: France **地区**: Ile-de-France **城市**: Paris **纬度**: 48.859077 **经度**: 2.293486
long.open.weixin.qq.com	**IP**: 112.65.193.150 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
imapi.volcvideo.com	**IP**: 221.204.58.138 **所属国家**: China **地区**: Shanxi

	城市: Taiyuan **纬度**: 37.869438 **经度**: 112.561508
mobilegw.dl.alipaydev.com	**IP**: 110.75.132.25 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
pagead2.googlesyndication.com	**IP**: 114.250.65.38 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102

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

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

摸瓜V2引擎

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	

手机线索

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

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

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"

加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

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

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://,