



MoGua

首钢挚友 1.2.4.APK 分析报告



APP名称:

首钢挚友

包名:	com.sgjt.gh
域名线索:	23条
URL线索:	26条
邮箱线索:	1条
分析日期:	2025年8月27日
分析平台:	摸瓜APK反编译平台

文件名: ghapp.apk
文件大小: 10.72MB
MD5值: 3f7a2f2508cf574199f29a437578990d
SHA1值: 495b8bdb57da2ca1ccaba5a8907739299540f98d
SHA256值: f83722c7bc2ab7a641e5c90e5689b8dc86bc000431ee49500c175474dea4a6cf

i APP 信息

App名称: 首钢挚友
包名: com.sgjt.gh
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 1.2.4
安卓版本: 124

🔍 域名线索

域名	服务器信息
m3w.cn	IP: 124.238.243.234 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
mobilegw-1-64.test.alipay.net	没有服务器地理信息.
wappaygw.alipay.com	IP: 124.239.239.236 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717

mobilegw.aaa.alipay.net	没有服务器地理信息.
open.weixin.qq.com	IP: 109.244.144.48 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
stream.mobihtml5.com	IP: 23.27.132.60 所属国家: United States of America 地区: California 城市: Santa Clara 纬度: 37.352100 经度: -121.958199
schemas.android.com	没有服务器地理信息.
stream.dcloud.net.cn	IP: 47.99.97.167 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com	没有服务器地理信息.
h5.m.taobao.com	IP: 220.181.165.199 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
render.alipay.com	IP: 27.128.221.243 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720

	经度: 116.694717
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
service.dcloud.net.cn	IP: 121.199.69.240 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
www.openssl.org	IP: 23.40.169.34 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
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
mobilegw.alipay.com	IP: 203.209.255.248 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
	IP: 27.128.221.243 所属国家: China

mclient.alipay.com	地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
m.alipay.com	IP: 203.209.245.120 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
loggw-exsdk.alipay.com	IP: 203.209.238.2 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
mcgw.alipay.com	IP: 124.239.239.237 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
long.open.weixin.qq.com	IP: 109.244.216.15 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
ask.dcloud.net.cn	IP: 124.238.243.239 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717

 URL线索

URL信息	Url所在文件
http://ask.dcloud.net.cn/article/283	io/dcloud/h/b.java
https://96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com/http/splash-screen/report	io/dcloud/feature/ad/dcloud/ADHandler.java
http://ask.dcloud.net.cn/article/35058	io/dcloud/feature/audio/AudioRecorderMgr.java
http://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.java
https://ask.dcloud.net.cn/article/35627	io/dcloud/f/a/a.java
https://ask.dcloud.net.cn/article/35877	io/dcloud/f/a/a.java
https://service.dcloud.net.cn/sta/so?p=a&pn=%s&ver=%s&appid=%s	io/dcloud/f/b/c.java
https://service.dcloud.net.cn/pdz	io/dcloud/f/b/e/a.java
https://96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com/http/rewarded-video/report?p=a&t=	io/dcloud/f/b/e/a.java
http://m3w.cn/s/	io/dcloud/common/util/ShortCutUtil.java
https://stream.mobihtml5.com/	io/dcloud/common/constant/StringConst.java
https://stream.dcloud.net.cn/	io/dcloud/common/constant/StringConst.java
http://ask.dcloud.net.cn/article/282	io/dcloud/common/constant/DOMException.java

http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifViewUtils.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/sdk/cons/a.java
https://mobilegw.alipaydev.com/mgw.htm	com/alipay/sdk/cons/a.java
https://mcgw.alipay.com/sdklog.do	com/alipay/sdk/cons/a.java
https://loggw-exsdk.alipay.com/loggw/logUpload.do	com/alipay/sdk/cons/a.java
http://m.alipay.com/?action=h5quit	com/alipay/sdk/cons/a.java
https://wappaygw.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/cons/a.java
https://mclient.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/cons/a.java
https://h5.m.taobao.com/mlapp/olist.html	com/alipay/sdk/data/a.java
https://render.alipay.com/p/s/i?scheme=%s	com/alipay/sdk/app/OpenAuthTask.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://mobilegw.alipay.com/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw.aaa.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw-1-64.test.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw.stable.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://xmlpull.org/v1/doc/features.html	com/ta/utdid2/core/persistent/XmlUtils.java
http://xmlpull.org/v1/doc/features.html	com/ta/utdid2/core/persistent/FastXmlSerializer.java
https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s×tamp=%s&scope=%s&signature=%s	com/tencent/mm/opensdk/diffdev/a/b.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuiid=%s	com/tencent/mm/opensdk/diffdev/a/c.java
https://ask.dcloud.net.cn/article/36199	Mogua Engine V1
http://www.openssl.org/support/faq.html	lib/armeabi-v7a/libijkffmpeg.so

 邮箱线索

邮箱地址	所在文件
ffmpeg-devel@ffmpeg.org	lib/armeabi-v7a/libijkplayer.so

☰ 手机线索

手机号	所在文件
17179869184	tv/danmaku/ijk/media/player/IjkMediaMeta.java

☼ 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: C=CN, ST=河北省, L=唐山市迁安市, O=首钢集团有限公司矿业公司, OU=首钢集团有限公司矿业公司, CN=dongweiwang
签名算法: rsassa_pkcs1v15
有效期自: 2018-04-09 07:34:23+00:00
有效期至: 2118-03-16 07:34:23+00:00
发行人: C=CN, ST=河北省, L=唐山市迁安市, O=首钢集团有限公司矿业公司, OU=首钢集团有限公司矿业公司, CN=dongweiwang
序列号: 0x5acb177f
哈希算法: sha1
md5值: bf788211412c33c00b44e24565ddfb56
sha1值: 71ee460e9b1842e8fca71bf1a746777a2e27cd05
sha256值: 45035ce08fa6acbecf880553199f454450272fbd36855b2f412fd0374ca6a2d8
sha512值: 9cce54412140881e8acdbcbd1652fb066769445ec1341cd4938de0b36974c96234e82ddada0a6b81402881ad3aa3a90b84f3035b5dc5a5836d7ec1fd089cf421
公钥算法: rsa
密钥长度: 1024
指纹: b7525952f86df03cc94e62c311f28d704e89d27d5903c1653c03f93c7ca74211

🔑 硬编码敏感信息

可能的敏感信息

"dcloud_common_user_refuse_api" : "the user denies access to the API"
"dcloud_io_without_authorization" : "not authorized"
"dcloud_oauth_authentication_failed" : "failed to obtain authorization to log in to the authentication service"
"dcloud_oauth_empower_failed" : "the Authentication Service operation to obtain authorized logon failed"
"dcloud_oauth_logout_tips" : "not logged in or logged out"
"dcloud_oauth_oauth_not_empower" : "oAuth authorization has not been obtained"
"dcloud_oauth_token_failed" : "failed to get token"
"dcloud_permissions_reauthorization" : "reauthorize"
"dcloud_common_user_refuse_api" : "用户拒绝该API访问"
"dcloud_io_without_authorization" : "没有获得授权"
"dcloud_oauth_authentication_failed" : "获取授权登录认证服务操作失败"
"dcloud_oauth_empower_failed" : "获取授权登录认证服务操作失败"
"dcloud_oauth_logout_tips" : "未登录或登录已注销"
"dcloud_oauth_oauth_not_empower" : "尚未获取oauth授权"
"dcloud_oauth_token_failed" : "获取token失败"
"dcloud_permissions_reauthorization" : "重新授权"

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.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.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.INSTALL_PACKAGES	系统	直接安装应用	允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任

	需要	程序	意强大权限的新应用程序
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.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.CALL_PHONE	危险	直接拨打电话号码	允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码
android.permission.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
android.permission.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由
android.permission.READ_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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.WAKE_LOCK	正常	防止手机睡眠	允许应用程序防止手机进入睡眠状态
android.permission.ACCESS_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
com.huawei.android.launcher.permission.CHANGE_BADGE	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.vivo.notification.permission.BADGE_ICON	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_EXTERNAL_STORAGE	危险	读取外部存储器内容	允许应用程序从外部存储读取

com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
--------------------------------------	----	--------------------	---

应用内通信

活动(ACTIVITY)	通信(INTENT)
io.dcloud.PandoraEntry	Schemes: h5d52ef42://,