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

**首钢挚友（ 1.2.4版本）
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | 首钢挚友 |
| 版本 | 1.2.4 |
| 包名 | com.sgjt.gh |
| 域名线索 | 23条 |
| URL线索 | 26条 |
| APP图标 |  |
| 分析日期 | 2025年8月27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 | ghapp.apk |
| 文件大小 | 10.72MB |
| MD5值 | 3f7a2f2508cf574199f29a437578990d |
| SHA1值 | 495b8bdb57da2ca1ccaba5a8907739299540f98d |
| SHA256值 | f83722c7bc2ab7a641e5c90e5689b8dc86bc000431ee49500c175474dea4a6cf |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| 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 |

## **4. 线索情况**

### **4.1 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  |
| 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  |
| 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  |
| stream.mobihtml5.com | IP: 23.27.132.60 所属国家: United States of America 地区: California 城市: Santa Clara  |
| 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  |
| 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  |
| render.alipay.com | IP: 27.128.221.243 所属国家: China 地区: Hebei 城市: Langfang  |
| xmlpull.org | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| service.dcloud.net.cn | IP: 121.199.69.240 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| www.openssl.org | IP: 23.40.169.34 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| mobilegw.alipaydev.com | IP: 110.75.132.131 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| mobilegw.alipay.com | IP: 203.209.255.248 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| mclient.alipay.com | IP: 27.128.221.243 所属国家: China 地区: Hebei 城市: Langfang  |
| m.alipay.com | IP: 203.209.245.120 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| loggw-exsdk.alipay.com | IP: 203.209.238.2 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| mcgw.alipay.com | IP: 124.239.239.237 所属国家: China 地区: Hebei 城市: Langfang  |
| long.open.weixin.qq.com | IP: 109.244.216.15 所属国家: China 地区: Beijing 城市: Beijing  |
| ask.dcloud.net.cn | IP: 124.238.243.239 所属国家: China 地区: Hebei 城市: Langfang  |
| mobilegw.stable.alipay.net | 没有服务器地理信息.  |

### **4.2 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&timestamp=%s&scope=%s&signature=%s  | com/tencent/mm/opensdk/diffdev/a/b.java  |
| https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%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  |

### **4.3 邮箱线索**

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

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 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: 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**

## **6. 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"  |

## **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.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 | 系统需要 | 直接安装应用程序 | 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 |

## **10. 应用内通信**

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

**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。**