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

**星河影视（ 4.2.0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 | 星河影视 |
| 版本 | 4.2.0 |
| 包名 | com.ganfantv.xx |
| 域名线索 | 86条 |
| URL线索 | 95条 |
| APP图标 |  |
| 分析日期 | 2025年7月22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 | 星河影视.apk |
| 文件大小 | 51.15MB |
| MD5值 | ec682c3222a1238069d27d8bfc10eeec |
| SHA1值 | 4fa46f9968029196e27ab778f6a6d41685b46769 |
| SHA256值 | f695522454ab91a59de939dff47f9699b6e8ffee5d43662b022fbb2f530ce285 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 星河影视 |
| 包名 | com.ganfantv.xx |
| 主活动Activity | com.ganfantv.xx.MainActivity |
| 安卓版本名称 | 4.2.0 |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| d1tru86qrby720.cloudfront.net | IP: 99.86.195.163 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| webcast.amemv.com | IP: 123.125.216.223 所属国家: China 地区: Beijing 城市: Beijing  |
| dc.sigmob.cn | IP: 112.126.7.24 所属国家: China 地区: Beijing 城市: Beijing  |
| m.sigmob.com | IP: 39.107.65.119 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| aomedia.org | IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| net.rayjump.com | IP: 39.107.225.241 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| pslog.umeng.com | IP: 59.82.29.162 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| developer.apple.com | IP: 17.253.85.205 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| configure.rayjump.com | IP: 59.110.124.183 所属国家: China 地区: Beijing 城市: Beijing  |
| changemaker.hzsanjiaomao.com | IP: 82.157.26.175 所属国家: China 地区: Beijing 城市: Beijing  |
| ads.oway.mobi | IP: 47.98.30.91 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| static.yximgs.com | IP: 39.91.183.221 所属国家: China 地区: Shandong 城市: Linyi  |
| webcast-open.douyin.com | IP: 61.48.83.235 所属国家: China 地区: Beijing 城市: Beijing  |
| api.yky.qq.com | IP: 116.130.223.28 所属国家: China 地区: Beijing 城市: Beijing  |
| alogsus.umeng.com | IP: 223.109.148.177 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| policy.rayjump.com | IP: 59.110.124.183 所属国家: China 地区: Beijing 城市: Beijing  |
| whatwg.org | IP: 165.227.248.76 所属国家: United States of America 地区: New Jersey 城市: Clifton  |
| dns.qq.com | IP: 119.29.29.229 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| hmma.baidu.com | IP: 110.242.68.196 所属国家: China 地区: Hebei 城市: Baoding  |
| i.snssdk.com | IP: 123.125.216.198 所属国家: China 地区: Beijing 城市: Beijing  |
| exoplayer.dev | IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| api.hzsanjiaomao.com | IP: 121.199.61.218 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| grs.dbankcloud.com | IP: 113.201.107.54 所属国家: China 地区: Shaanxi 城市: Baoji  |
| hybird.rayjump.com | IP: 111.161.121.2 所属国家: China 地区: Tianjin 城市: Tianjin  |
| open.e.kuaishou.com | IP: 116.136.162.35 所属国家: China 地区: Nei Mongol 城市: Hohhot  |
| 119.29.29.29 | IP: 119.29.29.29 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| test.com | IP: 67.225.146.248 所属国家: United States of America 地区: Michigan 城市: Lansing  |
| 211.151.146.65 | IP: 211.151.146.65 所属国家: China 地区: Beijing 城市: Beijing  |
| datax.baidu.com | 没有服务器地理信息.  |
| www.jsdelivr.com | IP: 104.21.23.24 所属国家: United States of America 地区: California 城市: San Francisco  |
| analytics.rayjump.com | IP: 123.56.168.170 所属国家: China 地区: Beijing 城市: Beijing  |
| dashif.org | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| cpro.baidustatic.com | IP: 101.72.203.35 所属国家: China 地区: Hebei 城市: Langfang  |
| check.rayjump.com | IP: 59.110.124.183 所属国家: China 地区: Beijing 城市: Beijing  |
| tl.oway.mobi | IP: 118.178.152.152 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| tdsdk.cpatrk.net | IP: 116.198.16.229 所属国家: China 地区: Beijing 城市: Beijing  |
| sdk.hzsanjiaomao.com | IP: 221.195.216.36 所属国家: China 地区: Hebei 城市: Cangzhou  |
| cloud.tgpa.qq.com | IP: 153.3.50.50 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| v.behe.com | 没有服务器地理信息.  |
| d.alipay.com | IP: 119.167.188.187 所属国家: China 地区: Shandong 城市: Qingdao  |
| dxp.baidu.com | IP: 110.242.68.94 所属国家: China 地区: Hebei 城市: Baoding  |
| 118.178.152.152 | IP: 118.178.152.152 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| test.api.yky.qq.com | IP: 123.125.0.201 所属国家: China 地区: Beijing 城市: Beijing  |
| sf6-ttcdn-tos.pstatp.com | IP: 103.3.115.129 所属国家: China 地区: Zhejiang 城市: Taizhou  |
| apps.samsung.com | IP: 221.193.246.123 所属国家: China 地区: Hebei 城市: Handan  |
| api.htp.ad-scope.com.cn | IP: 47.94.43.167 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| tl.oneway.mobi | IP: 47.98.30.91 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| utoken.umeng.com | IP: 112.85.139.76 所属国家: China 地区: Jiangsu 城市: Nantong  |
| lazy.rayjump.com | IP: 59.110.124.183 所属国家: China 地区: Beijing 城市: Beijing  |
| detect.rayjump.com | IP: 52.21.161.152 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| me.cpatrk.net | IP: 116.198.14.142 所属国家: China 地区: Beijing 城市: Beijing  |
| developer.android.com | IP: 142.251.42.142 所属国家: United States of America 地区: California 城市: Mountain View  |
| static.yky.qq.com | IP: 221.204.209.156 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| gist.github.com | IP: 159.24.3.173 所属国家: United States of America 地区: North Carolina 城市: Cary  |
| testcloud.tgpa.qq.com | IP: 114.222.114.87 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| ulogs.umengcloud.com | IP: 223.109.148.141 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| crbug.com | IP: 216.239.32.29 所属国家: United States of America 地区: California 城市: Mountain View  |
| api.ipify.org | IP: 173.231.16.77 所属国家: United States of America 地区: Utah 城市: Ogden  |
| union.baidu.com | IP: 111.206.208.169 所属国家: China 地区: Beijing 城市: Beijing  |
| apps.oceanengine.com | IP: 123.125.216.203 所属国家: China 地区: Beijing 城市: Beijing  |
| ads.oneway.mobi | IP: 118.178.152.152 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| cdn-adn-https.rayjump.com | IP: 121.18.168.32 所属国家: China 地区: Hebei 城市: Baoding  |
| js-ad.a.yximgs.com | IP: 112.83.167.2 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| alogus.umeng.com | IP: 223.109.148.141 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| developer.umeng.com | IP: 59.82.31.210 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| grs.dbankcloud.eu | 没有服务器地理信息.  |
| ns.adobe.com | 没有服务器地理信息.  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| ulogs.umeng.com | IP: 223.109.148.177 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| schemas.microsoft.com | IP: 13.107.213.74 所属国家: United States of America 地区: Washington 城市: Redmond  |
| play.google.com | IP: 46.82.174.69 所属国家: Germany 地区: Niedersachsen 城市: Braunschweig  |
| adservice.sigmob.cn | IP: 101.200.125.221 所属国家: China 地区: Beijing 城市: Beijing  |
| owtk.audioadx.com | IP: 8.136.116.120 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| android.asset | 没有服务器地理信息.  |
| passport.kuaishou.com | IP: 103.102.202.120 所属国家: China 地区: Beijing 城市: Beijing  |
| plbslog.umeng.com | IP: 36.156.202.78 所属国家: China 地区: Jiangsu 城市: Yangzhou  |
| cloud.cpatrk.net | IP: 116.198.14.42 所属国家: China 地区: Beijing 城市: Beijing  |
| grs.dbankcloud.cn | IP: 121.36.116.8 所属国家: China 地区: Beijing 城市: Beijing  |
| track.oway.mobi | IP: 47.98.30.91 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| 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.asia | IP: 119.8.176.236 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| journeyapps.com | IP: 18.65.168.3 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| openrcv.baidu.com | IP: 111.206.209.112 所属国家: China 地区: Beijing 城市: Beijing  |
| owads.audioadx.com | IP: 8.136.116.120 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| www.samsungapps.com | IP: 52.31.24.56 所属国家: Ireland 地区: Dublin 城市: Dublin  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://crbug.com/581399  | aegon/chrome/net/impl/UrlRequestBuilderImpl.java  |
| https://d.alipay.com  | c5/a.java  |
| https://cpro.baidustatic.com/cpro/logo/sdk/mob-adIcon\_2x.png  | com/baidu/mobads/sdk/api/XAdEntryResponse.java  |
| https://cpro.baidustatic.com/cpro/logo/sdk/new-bg-logo.png  | com/baidu/mobads/sdk/api/XAdEntryResponse.java  |
| http://union.baidu.com/  | com/baidu/mobads/sdk/api/XAdEntryResponse.java  |
| https://cpro.baidustatic.com/cpro/logo/sdk/mob-adIcon\_2x.png  | com/baidu/mobads/sdk/api/XAdNativeResponse.java  |
| https://cpro.baidustatic.com/cpro/logo/sdk/new-bg-logo.png  | com/baidu/mobads/sdk/api/XAdNativeResponse.java  |
| http://union.baidu.com/  | com/baidu/mobads/sdk/api/XAdNativeResponse.java  |
| http://211.151.146.65:8080/wlantest/shanghai\_sun/mock\_ad\_server\_intersitial\_video.json  | com/baidu/mobads/sdk/internal/dj.java  |
| http://hmma.baidu.com/app.gif  | com/baidu/mobstat/h.java  |
| https://hmma.baidu.com/app.gif  | com/baidu/mobstat/h.java  |
| https://dxp.baidu.com/vizParser  | com/baidu/mobstat/f3.java  |
| https://dxp.baidu.com/autoTracker  | com/baidu/mobstat/f3.java  |
| https://dxp.baidu.com/circleConfig?  | com/baidu/mobstat/f3.java  |
| http://openrcv.baidu.com/1010/bplus.gif  | com/baidu/mobstat/r5.java  |
| https://openrcv.baidu.com/1010/bplus.gif  | com/baidu/mobstat/r5.java  |
| https://hmma.baidu.com/auto.gif  | com/baidu/mobstat/u.java  |
| http://datax.baidu.com/xs.gif  | com/baidu/mobstat/y5.java  |
| https://datax.baidu.com/xs.gif  | com/baidu/mobstat/y5.java  |
| http://dxp.baidu.com/upgrade  | com/baidu/mobstat/y5.java  |
| https://dxp.baidu.com/upgrade  | com/baidu/mobstat/y5.java  |
| https://github.com/danikula/AndroidVideoCache/issues/43.  | com/beizi/ad/internal/c/h.java  |
| https://github.com/danikula/AndroidVideoCache/issues.  | com/beizi/ad/internal/c/h.java  |
| https://github.com/danikula/AndroidVideoCache/issues  | com/beizi/ad/internal/c/j.java  |
| https://v.behe.com/dsp20/ad/2017/5/5/28d147ed3e96a3ba8ac90703e4d66de2.jpg\  | com/beizi/ad/internal/network/ServerResponse.java  |
| https://v.behe.com/dsp20/ad/2017/5/5/28d147ed3e96a3ba8ac90703e4d66de2.jpg  | com/beizi/ad/internal/network/ServerResponse.java  |
| https://api.htp.ad-scope.com.cn/mb/sdk/event/v1?extInfo=wBLQeP8bmq6AuJ5DaZyc5xQQU\_92OWkSUdy\_6V4n2RA3Mbgehw6J67ZfwcDQCmj3uTyhCkrT8nMAsQ&requestUuid=\_\_REQUESTUUID\_\_&eventType=\_\_EVENTTYPE\_\_&appID=\_\_APPID\_\_&spaceID=\_\_SPACEID\_\_&channelID=\_\_CHANNELID\_\_&channelAppID=\_\_CHANNELAPPID\_\_&channelSpaceID=\_\_CHANNELSPACEID\_\_&ts=\_\_TS\_\_&ip=\_\_IP\_\_&netType=\_\_NETTYPE\_\_&carrier=\_\_CARRIER\_\_&errInfo=\_\_ERRINFO\_\_&sdkExtInfo=\_\_SDKEXTINFO\_\_&imei=\_\_IMEI\_\_&androidID=\_\_ANDROIDID\_\_&idfa=\_\_IDFA\_\_&idfv=\_\_IDFV\_\_&mac=\_\_MAC\_\_&uid=\_\_UID\_\_&sdkVersion=\_\_SDKVERSION\_\_&appVerison=\_\_APPVERSION\_\_  | com/beizi/ad/internal/view/AdViewImpl.java  |
| https://webcast.amemv.com/falcon/webcast\_douyin/page/anchor\_task\_v2/panel/index.html?web\_bg\_color=%23ff161823  | com/bytedance/android/live/base/api/BuildConfig.java  |
| https://webcast.amemv.com/falcon/webcast\_douyin/page/recharge\_v1/index.html  | com/bytedance/android/live/base/api/BuildConfig.java  |
| https://webcast-open.douyin.com  | com/bytedance/android/openliveplugin/material/LiveInitMaterialManager.java  |
| https://webcast-open.douyin.com/webcast/openapi/pangle/setting/?app\_id=  | com/bytedance/android/openliveplugin/material/LiveInitMaterialManager.java  |
| https://dc.sigmob.cn/log  | com/czhj/sdk/common/models/Config.java  |
| https://)([\\s\\S]+)  | com/huawei/hms/scankit/p/C0564bd.java  |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/ks\_so-webpArm64v8aRelease-3.3.9.apk  | com/kwad/components/ct/a/c.java  |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/ks\_so-webpArmeabiv7aRelease-3.3.9.apk  | com/kwad/components/ct/a/c.java  |
| https://passport.kuaishou.com/account-h5/login?smallWebview=true&sid=kuaishou.unioncontent.wallpaper  | com/kwad/components/ct/b/a.java  |
| https://static.yximgs.com/udata/pkg/KSAdSDK/coupon/ksad\_coupon\_entry\_status\_3.webp  | com/kwad/components/ct/coupon/entry/CouponEntryContainer.java  |
| https://static.yximgs.com/udata/pkg/KSAdSDK/coupon/ksad\_coupon\_entry\_status\_2.webp  | com/kwad/components/ct/coupon/entry/CouponEntryContainer.java  |
| https://static.yximgs.com/udata/pkg/KSAdSDK/coupon/ksad\_coupon\_entry\_status\_1.webp  | com/kwad/components/ct/coupon/entry/CouponEntryContainer.java  |
| https://static.yximgs.com/udata/pkg/KSAdSDK/coupon/ksad\_coupon\_entry\_status\_4.webp  | com/kwad/components/ct/coupon/entry/CouponEntryContainer.java  |
| https://static.yximgs.com/udata/pkg/KSAdSDK/coupon/ksad\_coupon\_entry\_status\_0.webp  | com/kwad/components/ct/coupon/entry/CouponEntryContainer.java  |
| https://js-ad.a.yximgs.com/kos/nlav10933/ksad\_profile\_header\_bg.png  | com/kwad/components/ct/profile/home/b/c.java  |
| https://static.yximgs.com/udata/pkg/KSAdSDK/ksad\_page\_loading\_data\_limit\_error.png  | com/kwad/components/ct/tube/view/EpisodeChooseLoadingView.java  |
| https://static.yximgs.com/udata/pkg/KSAdSDK/ksad\_no\_video\_img.png  | com/kwad/components/ct/tube/view/EpisodeChooseLoadingView.java  |
| https://static.yximgs.com/udata/pkg/KSAdSDK/ksad\_page\_loading\_data\_error.png  | com/kwad/components/ct/tube/view/EpisodeChooseLoadingView.java  |
| https://static.yximgs.com/udata/pkg/KSAdSDK/ksad\_no\_data\_img.png  | com/kwad/components/ct/tube/view/EpisodeChooseLoadingView.java  |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/wallpaper/kwai\_wallpaper\_plugin\_1.4.apk  | com/kwad/components/ct/wallpaper/c/b.java  |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/wallpaper/kwai\_wallpaper\_plugin\_1.5.apk  | com/kwad/components/ct/wallpaper/c/b.java  |
| https://static.yximgs.com/udata/pkg/KSAdSDK/ksad\_page\_loading\_data\_limit\_error.png  | com/kwad/components/ct/widget/KSPageLoadingView.java  |
| https://static.yximgs.com/udata/pkg/KSAdSDK/ksad\_no\_video\_img.png  | com/kwad/components/ct/widget/KSPageLoadingView.java  |
| https://static.yximgs.com/udata/pkg/KSAdSDK/ksad\_page\_loading\_data\_error.png  | com/kwad/components/ct/widget/KSPageLoadingView.java  |
| https://static.yximgs.com/udata/pkg/KSAdSDK/ksad\_no\_data\_img.png  | com/kwad/components/ct/widget/KSPageLoadingView.java  |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/offline\_components/adLive/ks\_so-adLiveNoSoRelease-3.3.32.1-f1f921211-59.zip  | com/kwad/components/offline/adLive/a.java  |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/adLive/3.3.26.1/ks\_so-adLiveArm64v8aRelease-3.3.26.1.apk  | com/kwad/components/offline/adLive/kwai/a.java  |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/adLive/3.3.26.1/ks\_so-adLiveArmeabiv7aRelease-3.3.26.1.apk  | com/kwad/components/offline/adLive/kwai/a.java  |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/offline\_components/obiwan/ks\_so-obiwanNoSoRelease-3.3.31.1-261163b35a-47.zip  | com/kwad/components/offline/obiwan/a.java  |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/offline\_components/tk/ks\_so-tachikomaNoSoRelease-3.3.32.1-c07a870c9-58.zip  | com/kwad/components/offline/tk/b.java  |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/tachikoma/3.3.24.2/ks\_so-tachikomaLiteArm64v8aRelease-3.3.24.2.apk  | com/kwad/components/offline/tk/a/a.java  |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/tachikoma/3.3.24.2/ks\_so-tachikomaArm64v8aRelease-3.3.24.2.apk  | com/kwad/components/offline/tk/a/a.java  |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/tachikoma/3.3.24.2/ks\_so-tachikomaLiteArmeabiv7aRelease-3.3.24.2.apk  | com/kwad/components/offline/tk/a/a.java  |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/tachikoma/3.3.24.2/ks\_so-tachikomaArmeabiv7aRelease-3.3.24.2.apk  | com/kwad/components/offline/tk/a/a.java  |
| https://open.e.kuaishou.com/rest/e/v3/open/sdk2  | com/kwad/sdk/api/loader/v.java  |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/ks\_so-appStatusArm64v8aRelease-3.3.14.apk  | com/kwad/sdk/collector/d.java  |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/ks\_so-appStatusArmeabiv7aRelease-3.3.14.apk  | com/kwad/sdk/collector/d.java  |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/so/ks\_so-kwaiPlayerArm64v8aRelease-3.3.20.apk  | com/kwad/sdk/core/video/kwai/e.java  |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/so/ks\_so-kwaiPlayerArmeabiv7aRelease-3.3.20.apk  | com/kwad/sdk/core/video/kwai/e.java  |
| http://%s:%d/%s  | com/kwad/sdk/core/videocache/f.java  |
| https://github.com/danikula/AndroidVideoCache/issues/43.  | com/kwad/sdk/core/videocache/h.java  |
| https://github.com/danikula/AndroidVideoCache/issues.  | com/kwad/sdk/core/videocache/h.java  |
| https://github.com/danikula/AndroidVideoCache/issues/88.  | com/kwad/sdk/core/videocache/h.java  |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/ks\_so-exceptionArm64v8aRelease-3.3.23.apk  | com/kwad/sdk/crash/f.java  |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/ks\_so-exceptionArmeabiv7aRelease-3.3.23.apk  | com/kwad/sdk/crash/f.java  |
| http://apps.samsung.com/appquery/appDetail.as?appId=  | com/kwad/sdk/utils/d.java  |
| https://github.com/lingochamp/FileDownloader/wiki/filedownloader.properties  | com/kwai/filedownloader/services/a.java  |
| https://hybird.rayjump.com/rv/authoriztion.html  | com/mbridge/msdk/a.java  |
| https://cdn-adn-https.rayjump.com/cdn-adn/v2/portal/19/08/20/11/06/5d5b63cb457e2.js  | com/mbridge/msdk/b/b.java  |
| http://whatwg.org/html/common-microsyntaxes.html  | com/mbridge/msdk/b/b/c.java  |
| http://whatwg.org/html/webappapis.html  | com/mbridge/msdk/b/b/c.java  |
| https://gist.github.com/atk/1020396\n  | com/mbridge/msdk/b/b/c.java  |
| http://whatwg.org/C  | com/mbridge/msdk/b/b/c.java  |
| https://play.google.com/  | com/mbridge/msdk/click/b.java  |
| https://cdn-adn-https.rayjump.com/cdn-adn/v2/portal/19/08/20/11/06/5d5b63cb457e2.js  | com/mbridge/msdk/foundation/controller/b.java  |
| https://analytics.rayjump.com  | com/mbridge/msdk/foundation/same/net/g/d.java  |
| https://net.rayjump.com  | com/mbridge/msdk/foundation/same/net/g/d.java  |
| https://configure.rayjump.com  | com/mbridge/msdk/foundation/same/net/g/d.java  |
| https://detect.rayjump.com/mapi/find  | com/mbridge/msdk/foundation/same/net/g/d.java  |
| https://detect.rayjump.com/mapi/result  | com/mbridge/msdk/foundation/same/net/g/d.java  |
| https://d1tru86qrby720.cloudfront.net/hostsetting  | com/mbridge/msdk/foundation/same/net/g/d.java  |
| https://policy.rayjump.com  | com/mbridge/msdk/foundation/same/net/g/d.java  |
| https://lazy.rayjump.com  | com/mbridge/msdk/foundation/same/net/g/d.java  |
| https://check.rayjump.com  | com/mbridge/msdk/foundation/same/net/g/d.java  |
| https://play.google.com/store/apps/details?id=  | com/mbridge/msdk/foundation/tools/v.java  |
| https://play.google.com/  | com/mbridge/msdk/foundation/tools/v.java  |
| https://play.google.com  | com/mbridge/msdk/mbjscommon/windvane/WindVaneWebView.java  |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense  | com/mbridge/msdk/playercommon/exoplayer2/drm/HttpMediaDrmCallback.java  |
| http://www.w3.org/ns/ttml  | com/mbridge/msdk/playercommon/exoplayer2/text/ttml/TtmlDecoder.java  |
| https://adservice.sigmob.cn/sigmob/config  | com/sigmob/sdk/base/h.java  |
| https://adservice.sigmob.cn/sigmob/config?  | com/sigmob/sdk/base/i.java  |
| https://adservice.sigmob.cn/extconfig?  | com/sigmob/sdk/base/i.java  |
| https://dc.sigmob.cn/log  | com/sigmob/sdk/base/i.java  |
| https://adservice.sigmob.cn/ad/v4  | com/sigmob/sdk/base/i.java  |
| https://adservice.sigmob.cn/hb/v2/ad  | com/sigmob/sdk/base/i.java  |
| https://m.sigmob.com  | com/sigmob/sdk/mraid/b.java  |
| http://%s:%d/%s  | com/sigmob/sdk/videocache/h.java  |
| http://%s:%d/%s  | com/sigmob/sdk/videocache/m.java  |
| https://github.com/danikula/AndroidVideoCache/issues/134.  | com/sigmob/sdk/videocache/m.java  |
| https://github.com/danikula/AndroidVideoCache/issues/43.  | com/sigmob/sdk/videocache/j.java  |
| https://github.com/danikula/AndroidVideoCache/issues.  | com/sigmob/sdk/videocache/j.java  |
| https://github.com/danikula/AndroidVideoCache/issues/88.  | com/sigmob/sdk/videocache/j.java  |
| http://changemaker.hzsanjiaomao.com:6688/105009  | com/sjm/sjmdsp/adCore/a.java  |
| http://sdk.hzsanjiaomao.com/sspconfig/%s.txt  | com/sjm/sjmdsp/adCore/a.java  |
| https://i.snssdk.com/  | com/ss/android/downloadad/api/constant/AdBaseConstants.java  |
| https://sf6-ttcdn-tos.pstatp.com/obj/ad-tetris-site/personal-privacy-page.html  | com/ss/android/downloadlib/addownload/compliance/AppPrivacyPolicyActivity.java  |
| https://apps.oceanengine.com/customer/api/app/pkg\_info?  | com/ss/android/downloadlib/addownload/compliance/ox.java  |
| https://www.samsungapps.com/appquery/appDetail.as?appId=  | com/ss/android/downloadlib/utils/ko.java  |
| https://test.api.yky.qq.com/  | com/tencent/klevin/c/e/a.java  |
| https://api.yky.qq.com/  | com/tencent/klevin/c/e/a.java  |
| https://static.yky.qq.com/bridge-h5/latest/dist/js-bridge-h5.umd.js  | com/tencent/klevin/config/b/a.java  |
| https://test.api.yky.qq.com/  | com/tencent/klevin/config/b/b.java  |
| https://api.yky.qq.com/  | com/tencent/klevin/config/b/b.java  |
| http://119.29.29.29/d?dn=  | com/tencent/klevin/download/b/s/a.java  |
| https://test.com  | com/tencent/klevin/download/b/w/e.java  |
| https://test.api.yky.qq.com/  | com/tencent/klevin/e/b/a.java  |
| https://api.yky.qq.com/  | com/tencent/klevin/e/b/a.java  |
| https://github.com/danikula/AndroidVideoCache/issues/43.  | com/tencent/klevin/e/j/d.java  |
| https://github.com/danikula/AndroidVideoCache/issues.  | com/tencent/klevin/e/j/d.java  |
| https://github.com/danikula/AndroidVideoCache/issues/88.  | com/tencent/klevin/e/j/d.java  |
| https://cloud.tgpa.qq.com  | com/tencent/tgpa/lite/InitConfig.java  |
| https://cloud.tgpa.qq.com  | com/tencent/tgpa/lite/f/a.java  |
| https://testcloud.tgpa.qq.com  | com/tencent/tgpa/lite/f/a.java  |
| https://cloud.cpatrk.net/configcloud/rest/sdk/gdprCheck  | com/tendcloud/tenddata/aa.java  |
| https://tdsdk.cpatrk.net/n/a/v1  | com/tendcloud/tenddata/aa.java  |
| https://cloud.cpatrk.net/configcloud/rest/sdk/match  | com/tendcloud/tenddata/aa.java  |
| https://me.cpatrk.net  | com/tendcloud/tenddata/a.java  |
| https://dns.qq.com  | com/tendcloud/tenddata/aj.java  |
| http://developer.umeng.com/docs/66650/cate/66650  | com/umeng/analytics/pro/j.java  |
| https://developer.umeng.com/docs/119267/detail/182050  | com/umeng/commonsdk/debug/UMLogCommon.java  |
| https://developer.umeng.com/docs/66632/detail/  | com/umeng/commonsdk/debug/UMLogUtils.java  |
| https://plbslog.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://ulogs.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://alogus.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://ulogs.umeng.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://alogus.umeng.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://alogsus.umeng.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://ulogs.umengcloud.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://pslog.umeng.com  | com/umeng/commonsdk/vchannel/a.java  |
| https://pslog.umeng.com/  | com/umeng/commonsdk/vchannel/a.java  |
| https://utoken.umeng.com/api/postZdata/v4  | com/umeng/umzid/ZIDManager.java  |
| https://utoken.umeng.com/api/updateZdata/v4  | com/umeng/umzid/ZIDManager.java  |
| https://adservice.sigmob.cn/strategy/v5  | com/windmill/sdk/c/c.java  |
| https://dc.sigmob.cn/log  | com/windmill/sdk/c/c.java  |
| https://adservice.sigmob.cn/extconfig?  | com/windmill/sdk/c/c.java  |
| https://adservice.sigmob.cn/windmill/config?  | com/windmill/sdk/c/c.java  |
| https://aomedia.org/emsg/ID3  | g0/a.java  |
| https://developer.apple.com/streaming/emsg-id3  | g0/a.java  |
| https://exoplayer.dev/issues/cleartext-not-permitted  | g1/m.java  |
| https://developer.android.com/guide/topics/permissions/overview  | io/flutter/plugin/platform/PlatformPlugin.java  |
| http://sdk.hzsanjiaomao.com/sjmconfig/%s.json  | j6/c.java  |
| https://d.alipay.com  | k6/b.java  |
| http://api.hzsanjiaomao.com/api/adEvent  | l5/d.java  |
| https://tl.oneway.mobi  | mobi/oneway/export/a/a.java  |
| http://track.oway.mobi  | mobi/oneway/export/a/a.java  |
| http://tl.oway.mobi  | mobi/oneway/export/a/a.java  |
| http://owtk.audioadx.com  | mobi/oneway/export/a/a.java  |
| http://118.178.152.152  | mobi/oneway/export/a/a.java  |
| https://ads.oneway.mobi  | mobi/oneway/export/a/a.java  |
| http://ads.oway.mobi  | mobi/oneway/export/a/a.java  |
| http://owads.audioadx.com  | mobi/oneway/export/a/a.java  |
| http://android.asset/  | mobi/oneway/sd/core/runtime/ShadowWebView.java  |
| http://dashif.org/guidelines/last-segment-number  | s0/d.java  |
| http://dashif.org/guidelines/trickmode  | s0/d.java  |
| http://dashif.org/thumbnail\_tile  | s0/d.java  |
| http://dashif.org/guidelines/thumbnail\_tile  | s0/d.java  |
| http://ns.adobe.com/xap/1.0/  | w/a.java  |
| https://api.ipify.org  | z4/f.java  |
| https://journeyapps.com/  | Mogua Engine V1  |
| https://github.com/journeyapps/zxing-android-embedded  | Mogua Engine V1  |
| https://grs.dbankcloud.com  | Mogua Engine V2  |
| https://grs.dbankcloud.cn  | Mogua Engine V2  |
| https://grs.dbankcloud.eu  | Mogua Engine V2  |
| https://grs.dbankcloud.asia  | Mogua Engine V2  |
| https://www.jsdelivr.com/using-sri-with-dynamic-files  | Mogua Engine V2  |
| https://github.com/apvarun/toastify-js  | Mogua Engine V2  |
| https://github.com/richtr/NoSleep.js/issues/15  | Mogua Engine V2  |
| https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released)  | Mogua Engine V2  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| xxx@email.elided  | aegon/chrome/base/PiiElider.java  |
| .apk@classes.dex  | com/kuaishou/weapon/p0/ac.java  |
| danikula@gmail.com  | com/kwad/sdk/core/videocache/h.java  |
| danikula@gmail.com  | com/sigmob/sdk/videocache/j.java  |
| danikula@gmail.com  | com/tencent/klevin/e/j/d.java  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869184  | com/kwai/video/player/KsMediaMeta.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: True 找到 1 个唯一证书 主题: C=C, ST=ST, L=L, O=O, OU=OU, CN=CN 签名算法: rsassa\_pkcs1v15 有效期自: 2024-01-04 04:12:41+00:00 有效期至: 2051-05-22 04:12:41+00:00 发行人: C=C, ST=ST, L=L, O=O, OU=OU, CN=CN 序列号: 0x70cf279e 哈希算法: sha256 md5值: 4fa7cdcd8d15a0b775913aa5888a671b sha1值: 64b0c245140528c4fcebf1c506950906d9e15b60 sha256值: 4c7eb1318a4ac726f98423622a2a4bbc23c72bd8446f389af3b62781642764c4 sha512值: a45d982ce60a1c6d832886a4244d925f026611a3c053325b71bab2326ae1287a0878d02817b6c699b56e1652d24d17d215a820a4b0972c2aed6feab56dd42059 公钥算法: rsa 密钥长度: 2048 指纹: 20faa2414e1cab0b876adce1a53bdea7c80323eebcb85cf0e29dffabd5399093**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "ksad\_ad\_default\_author" : "@可爱的广告君创造的原声"  |
| "ksad\_ad\_default\_username" : "@可爱的广告君"  |
| "library\_zxingandroidembedded\_author" : "JourneyApps"  |
| "library\_zxingandroidembedded\_authorWebsite" : "https://journeyapps.com/"  |

## **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.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\_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.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.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.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.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.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 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.USE\_FULL\_SCREEN\_INTENT | 正常 |  | 针对想要使用通知全屏意图的 Build.VERSION\_CODES.Q 的应用程序是必需的 |
| 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.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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.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 |
| 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 |
| com.ganfantv.xx.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| com.ganfantv.xx.openadsdk.permission.TT\_PANGOLIN | 未知 | Unknown permission | Unknown permission from android reference |
| com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.REORDER\_TASKS | 正常 | 重新排序正在运行的应用程序 | 允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前 |
| freemme.permission.msa | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_PRIVILEGED\_PHONE\_STATE | 未知 | Unknown permission | Unknown permission from android reference |
| com.ganfantv.xx.permission.KW\_SDK\_BROADCAST | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.SET\_WALLPAPER | 正常 | 设置壁纸 | 允许应用程序设置系统壁纸 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.ganfantv.xx.MainActivity | **Schemes**: xhys://, **Hosts:** app,  |

**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。**