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

**大师兄影视（ 3.1.0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 | 大师兄影视 |
| 版本 | 3.1.0 |
| 包名 | com.dogal.kenhuangzhe.geh.dashixiong |
| 域名线索 | 80条 |
| URL线索 | 76条 |
| APP图标 |  |
| 分析日期 | 2025年6月21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 | com.dogal.kenhuangzhe.geh.dashixiong\_3100.apk |
| 文件大小 | 54.58MB |
| MD5值 | 78e00ced794606f6c95d209a7915c6f8 |
| SHA1值 | 0ed0d0c0358af71807ff32e504d2ba6bd8458894 |
| SHA256值 | e6554656caec32bea6bcfce167a62da6378cedcc93f66d3ef66d3061662a82d4 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 大师兄影视 |
| 包名 | com.dogal.kenhuangzhe.geh.dashixiong |
| 主活动Activity | com.dogal.kenhuangzhe.geh.dashixiong.MainActivity |
| 安卓版本名称 | 3.1.0 |
| 安卓版本 | 3100 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| irc.native-ave2.com | IP: 118.31.168.72 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| irc.hpro2.com | IP: 112.124.5.225 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| graph.facebook.com | IP: 154.83.14.134 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| detect.rayjump.com | IP: 34.203.5.93 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| irc.magictop1.com | IP: 118.31.168.72 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| purl.org | IP: 207.241.239.241 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| configure.rayjump.com | IP: 39.105.219.82 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| mdc.html5.qq.com | IP: 175.27.9.46 所属国家: China 地区: Beijing 城市: Beijing  |
| irc.drapro2.com | IP: 118.31.168.72 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| apps.samsung.com | IP: 42.81.145.25 所属国家: China 地区: Tianjin 城市: Tianjin  |
| saas.qubiankeji.com | IP: 121.41.30.96 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| irc.avgnati.com | IP: 47.99.59.103 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| net.rayjump.com | IP: 39.107.225.241 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| api.htp.ad-scope.com.cn | IP: 123.57.16.151 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| whatwg.org | IP: 165.227.248.76 所属国家: United States of America 地区: New Jersey 城市: Clifton  |
| analytics.rayjump.com | IP: 123.56.168.170 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| plbslog.umeng.com | IP: 36.156.202.73 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  |
| debugx5.qq.com | IP: 175.27.9.46 所属国家: China 地区: Beijing 城市: Beijing  |
| i.snssdk.com | IP: 36.104.139.237 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| play.google.com | IP: 142.251.42.238 所属国家: United States of America 地区: California 城市: Mountain View  |
| open.e.kuaishou.com | IP: 103.102.202.74 所属国家: China 地区: Beijing 城市: Beijing  |
| crbug.com | IP: 216.239.32.29 所属国家: United States of America 地区: California 城市: Mountain View  |
| webcast-open.douyin.com | IP: 27.128.221.88 所属国家: China 地区: Hebei 城市: Langfang  |
| js-ad.a.yximgs.com | IP: 42.81.54.130 所属国家: China 地区: Tianjin 城市: Tianjin  |
| hybird.rayjump.com | IP: 103.254.188.166 所属国家: China 地区: Beijing 城市: Beijing  |
| irc.wprosvii.com | IP: 112.124.5.225 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| developer.android.com | IP: 142.251.43.14 所属国家: United States of America 地区: California 城市: Mountain View  |
| check.rayjump.com | IP: 59.110.124.183 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| www.sec.co.kr | IP: 112.106.187.200 所属国家: Korea (Republic of) 地区: Seoul-teukbyeolsi 城市: Seoul  |
| mqqad.html5.qq.com | IP: 0.0.0.1 所属国家: - 地区: - 城市: -  |
| pslog.umeng.com | IP: 59.82.29.249 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| androidquery.appspot.com | IP: 128.242.240.244 所属国家: United States of America 地区: California 城市: Milpitas  |
| irc.avgnatii.com | IP: 118.31.168.72 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| irc.native-ave1.com | IP: 112.124.5.225 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| irc.mprobrushh.com | IP: 47.99.59.103 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| alogus.umeng.com | IP: 223.109.148.179 所属国家: China 地区: Beijing 城市: Beijing  |
| webcast.amemv.com | IP: 106.117.244.232 所属国家: China 地区: Hebei 城市: Tangshan  |
| passport.kuaishou.com | IP: 103.107.219.22 所属国家: China 地区: Beijing 城市: Beijing  |
| www.facebook.com | IP: 108.160.170.26 所属国家: United States of America 地区: California 城市: San Francisco  |
| adput.qubiankeji.com | IP: 118.31.168.72 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| api.twitter.com | IP: 104.244.42.130 所属国家: United States of America 地区: California 城市: San Francisco  |
| log.tbs.qq.com | IP: 109.244.244.32 所属国家: China 地区: Beijing 城市: Beijing  |
| soft.tbs.imtt.qq.com | IP: 119.167.147.86 所属国家: China 地区: Shandong 城市: Qingdao  |
| irc.drapro1.com | IP: 47.99.59.103 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| v.behe.com | 没有服务器地理信息.  |
| schemas.microsoft.com | IP: 13.107.237.49 所属国家: United States of America 地区: Washington 城市: Redmond  |
| irc.magictop2.com | IP: 112.124.5.225 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| schemas.xmlsoap.org | IP: 13.107.238.49 所属国家: United States of America 地区: Washington 城市: Redmond  |
| dc.sigmob.cn | IP: 112.126.7.24 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| github.com | IP: 20.205.243.166 所属国家: United States of America 地区: Washington 城市: Redmond  |
| ulogs.umengcloud.com | IP: 223.109.148.130 所属国家: China 地区: Beijing 城市: Beijing  |
| sdk.e.qq.com | IP: 119.147.13.93 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| gist.github.com | IP: 203.98.7.65 所属国家: New Zealand 地区: Auckland 城市: Auckland  |
| policy.rayjump.com | IP: 39.105.219.82 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| pms.mb.qq.com | IP: 175.27.12.246 所属国家: China 地区: Beijing 城市: Beijing  |
| apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| tbsrecovery.imtt.qq.com | IP: 109.244.244.237 所属国家: China 地区: Beijing 城市: Beijing  |
| irc.mprobrush.com | IP: 47.99.59.103 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| xml.org | IP: 104.239.240.11 所属国家: United States of America 地区: Texas 城市: Windcrest  |
| adservice.sigmob.cn | IP: 47.94.254.145 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| sf6-ttcdn-tos.pstatp.com | IP: 61.147.216.109 所属国家: China 地区: Jiangsu 城市: Nantong  |
| d1tru86qrby720.cloudfront.net | IP: 13.32.54.11 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| ulogs.umeng.com | IP: 223.109.148.178 所属国家: China 地区: Beijing 城市: Beijing  |
| cdn-adn-https.rayjump.com | IP: 103.254.188.166 所属国家: China 地区: Beijing 城市: Beijing  |
| cfg.imtt.qq.com | IP: 175.27.12.246 所属国家: China 地区: Beijing 城市: Beijing  |
| 47.97.36.81 | IP: 47.97.36.81 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| irc.hpro1.com | IP: 112.124.5.225 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| alogsus.umeng.com | IP: 223.109.148.176 所属国家: China 地区: Beijing 城市: Beijing  |
| aaid.umeng.com | IP: 218.91.197.68 所属国家: China 地区: Jiangsu 城市: Nantong  |
| h5iad.sp-card.com | IP: 106.117.249.167 所属国家: China 地区: Hebei 城市: Tangshan  |
| www.samsungapps.com | IP: 52.18.136.34 所属国家: Ireland 地区: Dublin 城市: Dublin  |
| developer.umeng.com | IP: 59.82.31.160 所属国家: China 地区: Beijing 城市: Beijing  |
| static.yximgs.com | IP: 110.249.196.214 所属国家: China 地区: Hebei 城市: Shijiazhuang  |
| lazy.rayjump.com | IP: 39.105.219.82 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| debugtbs.qq.com | IP: 175.27.9.46 所属国家: China 地区: Beijing 城市: Beijing  |
| irc.wprosvi.com | IP: 118.31.168.72 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| apps.oceanengine.com | IP: 124.238.245.122 所属国家: China 地区: Hebei 城市: Langfang  |
| ouplog.umeng.com | IP: 47.246.110.93 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://www.sec.co.kr/dlna  | m3/h.java  |
| http://schemas.xmlsoap.org/soap/envelope/  | i4/p.java  |
| http://schemas.xmlsoap.org/soap/encoding/  | i4/p.java  |
| https://developer.android.com/guide/topics/permissions/overview  | io/flutter/plugin/platform/PlatformPlugin.java  |
| http://adput.qubiankeji.com:7071  | i0/b.java  |
| http://xml.org/sax/features/external-general-entities  | e1/a.java  |
| http://xml.org/sax/features/external-parameter-entities  | e1/a.java  |
| http://www.w3.org/2001/xml.xsd  | s4/c.java  |
| http://xml.org/sax/features/external-general-entities  | s4/c.java  |
| http://xml.org/sax/features/external-parameter-entities  | s4/c.java  |
| http://apache.org/xml/features/disallow-doctype-decl  | s4/c.java  |
| http://www.w3.org/2001/XMLSchema  | s4/c.java  |
| https://sdk.e.qq.com/launch  | com/qq/e/comm/b/a.java  |
| https://sdk.e.qq.com/activate  | com/qq/e/comm/b/a.java  |
| http://purl.org/dc/elements/1.1/\  | com/xht/flutter/flutter\_dlna/screening/DLNAPlayer.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  |
| 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://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://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.twitter.com/oauth/access\_token  | com/androidquery/auth/TwitterHandle.java  |
| https://api.twitter.com/oauth/authorize  | com/androidquery/auth/TwitterHandle.java  |
| https://api.twitter.com/oauth/request\_token  | com/androidquery/auth/TwitterHandle.java  |
| https://graph.facebook.com/oauth/authorize  | com/androidquery/auth/FacebookHandle.java  |
| https://www.facebook.com/connect/login\_success.html  | com/androidquery/auth/FacebookHandle.java  |
| https://graph.facebook.com/oauth/authorize?  | com/androidquery/auth/FacebookHandle.java  |
| https://graph.facebook.com/me  | com/androidquery/auth/FacebookHandle.java  |
| https://androidquery.appspot.com  | com/androidquery/service/MarketService.java  |
| http://irc.wprosvi.com  | com/tb/tb\_lib/b/a.java  |
| http://irc.wprosvii.com  | com/tb/tb\_lib/b/a.java  |
| http://irc.mprobrush.com  | com/tb/tb\_lib/b/a.java  |
| http://irc.mprobrushh.com  | com/tb/tb\_lib/b/a.java  |
| http://irc.avgnati.com  | com/tb/tb\_lib/b/a.java  |
| http://irc.avgnatii.com  | com/tb/tb\_lib/b/a.java  |
| http://irc.native-ave1.com  | com/tb/tb\_lib/b/a.java  |
| http://irc.native-ave2.com  | com/tb/tb\_lib/b/a.java  |
| http://irc.hpro1.com  | com/tb/tb\_lib/b/a.java  |
| http://irc.hpro2.com  | com/tb/tb\_lib/b/a.java  |
| http://irc.drapro1.com  | com/tb/tb\_lib/b/a.java  |
| http://irc.drapro2.com  | com/tb/tb\_lib/b/a.java  |
| http://irc.magictop1.com  | com/tb/tb\_lib/b/a.java  |
| http://irc.magictop2.com  | com/tb/tb\_lib/b/a.java  |
| http://saas.qubiankeji.com:18013  | com/tb/mob/saas/SaasConfigInfo.java  |
| http://47.97.36.81:8090/PrivacyLink  | com/tb/mob/more/TbWebViewActivity.java  |
| https://h5iad.sp-card.com/games/launch/?appSecret=  | com/tb/mob/h5/BaseWebActivity.java  |
| https://hybird.rayjump.com/rv/authoriztion.html  | com/mbridge/msdk/a.java  |
| https://play.google.com/  | com/mbridge/msdk/click/b.java  |
| http://www.w3.org/ns/ttml  | com/mbridge/msdk/playercommon/exoplayer2/text/ttml/TtmlDecoder.java  |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense  | com/mbridge/msdk/playercommon/exoplayer2/drm/HttpMediaDrmCallback.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  |
| 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://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  |
| http://apps.samsung.com/appquery/appDetail.as?appId=  | com/kwad/sdk/utils/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  |
| 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  |
| http://%s:%d/%s  | com/kwad/sdk/core/videocache/f.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-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  |
| 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/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/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/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://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://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/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://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/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://github.com/lingochamp/FileDownloader/wiki/filedownloader.properties  | com/kwai/filedownloader/services/a.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://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://aaid.umeng.com/api/postZdata  | com/umeng/umzid/ZIDManager.java  |
| https://aaid.umeng.com/api/updateZdata  | com/umeng/umzid/ZIDManager.java  |
| https://plbslog.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://ulogs.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://ouplog.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://developer.umeng.com/docs/66632/detail/  | com/umeng/commonsdk/debug/UMLogUtils.java  |
| http://developer.umeng.com/docs/66650/cate/66650  | com/umeng/analytics/pro/i.java  |
| https://log.tbs.qq.com/ajax?c=pu&v=2&k=  | com/tencent/smtt/utils/n.java  |
| https://log.tbs.qq.com/ajax?c=pu&tk=  | com/tencent/smtt/utils/n.java  |
| https://log.tbs.qq.com/ajax?c=dl&k=  | com/tencent/smtt/utils/n.java  |
| https://cfg.imtt.qq.com/tbs?v=2&mk=  | com/tencent/smtt/utils/n.java  |
| https://log.tbs.qq.com/ajax?c=ul&v=2&k=  | com/tencent/smtt/utils/n.java  |
| https://mqqad.html5.qq.com/adjs  | com/tencent/smtt/utils/n.java  |
| https://log.tbs.qq.com/ajax?c=ucfu&k=  | com/tencent/smtt/utils/n.java  |
| https://tbsrecovery.imtt.qq.com/getconfig  | com/tencent/smtt/utils/n.java  |
| https://soft.tbs.imtt.qq.com/17421/tbs\_res\_imtt\_tbs\_DebugPlugin\_DebugPlugin.tbs  | com/tencent/smtt/utils/d.java  |
| https://pms.mb.qq.com/rsp204  | com/tencent/smtt/sdk/m.java  |
| https://debugtbs.qq.com  | com/tencent/smtt/sdk/WebView.java  |
| https://debugx5.qq.com  | com/tencent/smtt/sdk/WebView.java  |
| https://debugtbs.qq.com?10000\  | com/tencent/smtt/sdk/WebView.java  |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=50079  | com/tencent/smtt/sdk/stat/MttLoader.java  |
| https://mdc.html5.qq.com/mh?channel\_id=50079&u=  | com/tencent/smtt/sdk/stat/MttLoader.java  |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11041  | com/tencent/smtt/sdk/ui/dialog/d.java  |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11047  | com/tencent/smtt/sdk/ui/dialog/d.java  |
| https://www.samsungapps.com/appquery/appDetail.as?appId=  | com/ss/android/downloadlib/utils/a.java  |
| https://apps.oceanengine.com/customer/api/app/pkg\_info?  | com/ss/android/downloadlib/addownload/compliance/u.java  |
| https://sf6-ttcdn-tos.pstatp.com/obj/ad-tetris-site/personal-privacy-page.html  | com/ss/android/downloadlib/addownload/compliance/AppPrivacyPolicyActivity.java  |
| https://i.snssdk.com/  | com/ss/android/downloadad/api/constant/AdBaseConstants.java  |
| https://dc.sigmob.cn/log  | com/czhj/sdk/common/models/Config.java  |
| https://crbug.com/581399  | aegon/chrome/net/impl/UrlRequestBuilderImpl.java  |

### **4.3 邮箱线索**

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

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869184  | com/kwai/video/player/KsMediaMeta.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=hn, L=hn, O=hn, OU=hn, CN=hn 签名算法: rsassa\_pkcs1v15 有效期自: 2021-04-09 02:19:29+00:00 有效期至: 2046-04-03 02:19:29+00:00 发行人: C=cn, ST=hn, L=hn, O=hn, OU=hn, CN=hn 序列号: 0x43d07869 哈希算法: sha256 md5值: 6d8f7f66b7988440350d38b83f47aa5f sha1值: f58d269e146de39ae6076b1ac7d6071a4ca9a75c sha256值: c17b905b3ca90d4713cb0ac03845a683a63a8d7357ff2cefeb96f59aa802fc6b sha512值: 5fc7e51398f4652740d373dd9404aa3a5abeb8ac7ca45c1307fb5554177fcc040c801e74d1b11ae952ab38f4c38c475dd08c3e68fd5d4c003025f2cfcd0c94b3 公钥算法: rsa 密钥长度: 2048 指纹: 121fbc225f79bb2fd075cb75825a917d49c9f8eca15bf0ceeee61537aa51f24d**

## **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"  |

## **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.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.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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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.CHANGE\_WIFI\_STATE | 正常 | 更改Wi-Fi状态 | 允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改 |
| 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.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.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.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.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\_WIFI\_MULTICAST\_STATE | 正常 | 允许Wi-Fi多播接收  | 允许应用程序接收不是直接发送到您设备的数据包。这在发现附近提供的服务时很有用。它比非多播模式使用更多的功率 |
| 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.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 |
| android.permission.SET\_WALLPAPER | 正常 | 设置壁纸 | 允许应用程序设置系统壁纸 |
| 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 |
| com.dogal.kenhuangzhe.geh.dashixiong.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.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 |
| freemme.permission.msa | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

**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。**