



MoGua

大师兄影视 3.1.0.APK 分析报告



APP名称:	大师兄影视
包名:	com.dogal.kenhuangzhe.geh.dashixiong
域名线索:	80条
URL线索:	76条
邮箱线索:	4条
分析日期:	2025年6月21日
分析平台:	摸瓜APK反编译平台

文件信息

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

i APP 信息

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

🔍 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 纬度: 30.293650 经度: 120.161423
irc.hpro2.com	IP: 112.124.5.225 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
graph.facebook.com	IP: 154.83.14.134 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692

detect.rayjump.com	IP: 34.203.5.93 所属国家: United States of America 地区: Virginia 城市: Ashburn 纬度: 39.043720 经度: -77.487488
irc.magictop1.com	IP: 118.31.168.72 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
purl.org	IP: 207.241.239.241 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.781734 经度: -122.459435
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
configure.rayjump.com	IP: 39.105.219.82 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
mdc.html5.qq.com	IP: 175.27.9.46 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
irc.drapro2.com	IP: 118.31.168.72 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
apps.samsung.com	IP: 42.81.145.25 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142220 经度: 117.176666
saas.qubiankeji.com	IP: 121.41.30.96 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
	IP: 47.99.59.103

irc.avgnati.com	所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
net.rayjump.com	IP: 39.107.225.241 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
api.htp.ad-scope.com.cn	IP: 123.57.16.151 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
whatwg.org	IP: 165.227.248.76 所属国家: United States of America 地区: New Jersey 城市: Clifton 纬度: 40.858429 经度: -74.163757
analytics.rayjump.com	IP: 123.56.168.170 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
plbslog.umeng.com	IP: 36.156.202.73 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
m.sigmob.com	IP: 39.107.65.119 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
debugx5.qq.com	IP: 175.27.9.46 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
i.snssdk.com	IP: 36.104.139.237 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
	IP: 142.251.42.238

play.google.com	所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
open.e.kuaishou.com	IP: 103.102.202.74 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
crbug.com	IP: 216.239.32.29 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
webcast-open.douyin.com	IP: 27.128.221.88 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
js-ad.a.yximgs.com	IP: 42.81.54.130 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142220 经度: 117.176666
hybird.rayjump.com	IP: 103.254.188.166 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
irc.wprosui.com	IP: 112.124.5.225 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
developer.android.com	IP: 142.251.43.14 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
check.rayjump.com	IP: 59.110.124.183 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
	IP: 112.106.187.200 所属国家: Korea (Republic of)

www.sec.co.kr	地区: Seoul-teukbyeolsi 城市: Seoul 纬度: 37.568260 经度: 126.977829
mqqad.html5.qq.com	IP: 0.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
pslog.umeng.com	IP: 59.82.29.249 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
androidquery.appspot.com	IP: 128.242.240.244 所属国家: United States of America 地区: California 城市: Milpitas 纬度: 37.428268 经度: -121.906616
irc.avgnatii.com	IP: 118.31.168.72 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
irc.native-ave1.com	IP: 112.124.5.225 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
irc.mprobrushh.com	IP: 47.99.59.103 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
alogus.umeng.com	IP: 223.109.148.179 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
webcast.amemv.com	IP: 106.117.244.232 所属国家: China 地区: Hebei 城市: Tangshan 纬度: 39.633331 经度: 118.183327
	IP: 103.107.219.22 所属国家: China 地区: Beijing

passport.kuaishou.com	城市: Beijing 纬度: 39.907501 经度: 116.397232
www.facebook.com	IP: 108.160.170.26 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
adput.qubiankeji.com	IP: 118.31.168.72 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
api.twitter.com	IP: 104.244.42.130 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446
log.tbs.qq.com	IP: 109.244.244.32 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
soft.tbs.imtt.qq.com	IP: 119.167.147.86 所属国家: China 地区: Shandong 城市: Qingdao 纬度: 36.098610 经度: 120.371941
irc.drapro1.com	IP: 47.99.59.103 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
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 纬度: 47.682899 经度: -122.120903
irc.magictop2.com	IP: 112.124.5.225 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423

schemas.xmlsoap.org	IP: 13.107.238.49 所属国家: United States of America 地区: Washington 城市: Redmond 纬度: 47.682899 经度: -122.120903
dc.sigmob.cn	IP: 112.126.7.24 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
github.com	IP: 20.205.243.166 所属国家: United States of America 地区: Washington 城市: Redmond 纬度: 47.682899 经度: -122.120903
ulogs.umengcloud.com	IP: 223.109.148.130 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
sdk.e.qq.com	IP: 119.147.13.93 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298
gist.github.com	IP: 203.98.7.65 所属国家: New Zealand 地区: Auckland 城市: Auckland 纬度: -36.866669 经度: 174.766663
policy.rayjump.com	IP: 39.105.219.82 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
pms.mb.qq.com	IP: 175.27.12.246 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
apache.org	IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203

tbsrecovery.imtt.qq.com	IP: 109.244.244.237 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
irc.mprobrush.com	IP: 47.99.59.103 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
xml.org	IP: 104.239.240.11 所属国家: United States of America 地区: Texas 城市: Windcrest 纬度: 29.499678 经度: -98.399246
adservice.sigmob.cn	IP: 47.94.254.145 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
sf6-ttcdn-tos.pstatp.com	IP: 61.147.216.109 所属国家: China 地区: Jiangsu 城市: Nantong 纬度: 32.030281 经度: 120.874718
d1tru86qrby720.cloudfront.net	IP: 13.32.54.11 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689507 经度: 139.691696
ulogs.umeng.com	IP: 223.109.148.178 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
cdn-adn-https.rayjump.com	IP: 103.254.188.166 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
cfg.imtt.qq.com	IP: 175.27.12.246 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
	IP: 47.97.36.81

47.97.36.81	所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
irc.hpro1.com	IP: 112.124.5.225 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
alogsus.umeng.com	IP: 223.109.148.176 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
aaid.umeng.com	IP: 218.91.197.68 所属国家: China 地区: Jiangsu 城市: Nantong 纬度: 32.030281 经度: 120.874718
h5iad.sp-card.com	IP: 106.117.249.167 所属国家: China 地区: Hebei 城市: Tangshan 纬度: 39.633331 经度: 118.183327
www.samsungapps.com	IP: 52.18.136.34 所属国家: Ireland 地区: Dublin 城市: Dublin 纬度: 53.343990 经度: -6.267190
developer.umeng.com	IP: 59.82.31.160 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
static.yximgs.com	IP: 110.249.196.214 所属国家: China 地区: Hebei 城市: Shijiazhuang 纬度: 38.041389 经度: 114.478607
lazy.rayjump.com	IP: 39.105.219.82 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
	IP: 175.27.9.46

debugtbs.qq.com	所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
irc.wprosvi.com	IP: 118.31.168.72 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
apps.oceanengine.com	IP: 124.238.245.122 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
ouplog.umeng.com	IP: 47.246.110.93 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692

 URL线索

URL信息
http://www.sec.co.kr/dlna
http://schemas.xmlsoap.org/soap/envelope/
http://schemas.xmlsoap.org/soap/encoding/
https://developer.android.com/guide/topics/permissions/overview
http://adput.qubiankeji.com:7071
http://xml.org/sax/features/external-general-entities
http://xml.org/sax/features/external-parameter-entities
http://www.w3.org/2001/xml.xsd
http://xml.org/sax/features/external-general-entities
http://xml.org/sax/features/external-parameter-entities
http://apache.org/xml/features/disallow-doctype-decl
http://www.w3.org/2001/XMLSchema
https://sdk.e.qq.com/launch

https://sdk.e.qq.com/activate
http://purl.org/dc/elements/1.1/
https://adservice.sigmob.cn/sigmob/config
https://adservice.sigmob.cn/sigmob/config?
https://adservice.sigmob.cn/extconfig?
https://dc.sigmob.cn/log
https://adservice.sigmob.cn/ad/v4
https://adservice.sigmob.cn/hb/v2/ad
https://m.sigmob.com
http://%s:%d/%s
http://%s:%d/%s
https://github.com/danikula/AndroidVideoCache/issues/134 .
https://github.com/danikula/AndroidVideoCache/issues/43 .
https://github.com/danikula/AndroidVideoCache/issues .
https://github.com/danikula/AndroidVideoCache/issues/88 .
https://github.com/danikula/AndroidVideoCache/issues/43 .
https://github.com/danikula/AndroidVideoCache/issues .
https://github.com/danikula/AndroidVideoCache/issues
https://api.htp.ad-scope.com.cn/mb/sdk/event/v1? extInfo=wBLQeP8bmq6Auj5DaZyc5xQQU_92OWkSUdy_6V4n2RA3Mbgehw6j67ZfwcDQCmj3uTyhCkrT8nMAsQ&requestUuid=__REQUESTUID__&eventType=__EVENTTYPE__&appId=__APPID__&spaceID=__SPACEID__&channelID=__CHANNELID__&channelAppID=__CHANNELAPPID__&ch
https://v.behe.com/dsp20/ad/2017/5/5/28d147ed3e96a3ba8ac90703e4d66de2.jpg \
https://v.behe.com/dsp20/ad/2017/5/5/28d147ed3e96a3ba8ac90703e4d66de2.jpg
https://api.twitter.com/oauth/access_token
https://api.twitter.com/oauth/authorize
https://api.twitter.com/oauth/request_token
https://graph.facebook.com/oauth/authorize
https://www.facebook.com/connect/login_success.html
https://graph.facebook.com/oauth/authorize?
https://graph.facebook.com/me

https://androidquery.appspot.com
http://irc.wprosvi.com
http://irc.wprosvii.com
http://irc.mprobrush.com
http://irc.mprobrushh.com
http://irc.avgnati.com
http://irc.avgnatii.com
http://irc.native-ave1.com
http://irc.native-ave2.com
http://irc.hpro1.com
http://irc.hpro2.com
http://irc.drapro1.com
http://irc.drapro2.com
http://irc.magictop1.com
http://irc.magictop2.com
http://saas.qubiankeji.com:18013
http://47.97.36.81:8090/PrivacyLink
https://h5iad.sp-card.com/games/launch/?appSecret=
https://hybird.rayjump.com/rv/authoriztion.html
https://play.google.com/
http://www.w3.org/ns/ttml
http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense
https://cdn-adn-https.rayjump.com/cdn-adn/v2/portal/19/08/20/11/06/5d5b63cb457e2.js
https://analytics.rayjump.com
https://net.rayjump.com
https://configure.rayjump.com
https://detect.rayjump.com/mapi/find
https://detect.rayjump.com/mapi/result

https://d1tru86qrby720.cloudfront.net/hostsetting
https://policy.rayjump.com
https://lazy.rayjump.com
https://check.rayjump.com
https://play.google.com/store/apps/details?id=
https://play.google.com/
https://play.google.com
https://cdn-adn-https.rayjump.com/cdn-adn/v2/portal/19/08/20/11/06/5d5b63cb457e2.js
http://whatwg.org/html/common-microsyntaxes.html
http://whatwg.org/html/webappapis.html
https://gist.github.com/atk/1020396\n
http://whatwg.org/C
https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDK/ks_so-appStatusArm64v8aRelease-3.3.14.apk
https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDK/ks_so-appStatusArmeabiv7aRelease-3.3.14.apk
http://apps.samsung.com/appquery/appDetail.as?appId=
https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDK/so/ks_so-kwaiPlayerArm64v8aRelease-3.3.20.apk
https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDK/so/ks_so-kwaiPlayerArmeabiv7aRelease-3.3.20.apk
https://github.com/danikula/AndroidVideoCache/issues/43 .
https://github.com/danikula/AndroidVideoCache/issues .
https://github.com/danikula/AndroidVideoCache/issues/88 .
http://%s:%d/%s
https://open.e.kuaishou.com/rest/e/v3/open/sdk2
https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDK/ks_so-exceptionArm64v8aRelease-3.3.23.apk
https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDK/ks_so-exceptionArmeabiv7aRelease-3.3.23.apk
https://static.yximgs.com/udata/pkg/KSAdSDK/ksad_page_loading_data_limit_error.png
https://static.yximgs.com/udata/pkg/KSAdSDK/ksad_no_video_img.png
https://static.yximgs.com/udata/pkg/KSAdSDK/ksad_page_loading_data_error.png
https://static.yximgs.com/udata/pkg/KSAdSDK/ksad_no_data_img.png

https://static.yximgs.com/udata/pkg/KSAdSDK/ksad_page_loading_data_limit_error.png
https://static.yximgs.com/udata/pkg/KSAdSDK/ksad_no_video_img.png
https://static.yximgs.com/udata/pkg/KSAdSDK/ksad_page_loading_data_error.png
https://static.yximgs.com/udata/pkg/KSAdSDK/ksad_no_data_img.png
https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/wallpaper/kwai_wallpaper_plugin_1.4.apk
https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/wallpaper/kwai_wallpaper_plugin_1.5.apk
https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/ks_so-webpArm64v8aRelease-3.3.9.apk
https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/ks_so-webpArmeabiv7aRelease-3.3.9.apk
https://static.yximgs.com/udata/pkg/KSAdSDK/coupon/ksad_coupon_entry_status_3.webp
https://static.yximgs.com/udata/pkg/KSAdSDK/coupon/ksad_coupon_entry_status_2.webp
https://static.yximgs.com/udata/pkg/KSAdSDK/coupon/ksad_coupon_entry_status_1.webp
https://static.yximgs.com/udata/pkg/KSAdSDK/coupon/ksad_coupon_entry_status_4.webp
https://static.yximgs.com/udata/pkg/KSAdSDK/coupon/ksad_coupon_entry_status_0.webp
https://js-ad.a.yximgs.com/kos/nlav10933/ksad_profile_header_bg.png
https://passport.kuaishou.com/account-h5/login?smallWebView=true&sid=kuaishou.uniononcontent.wallpaper
https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDK/offline_components/tk/ks_so-tachikomaNoSoRelease-3.3.32.1-c07a870c9-58.zip
https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDK/tachikoma/3.3.24.2/ks_so-tachikomaLiteArm64v8aRelease-3.3.24.2.apk
https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/tachikoma/3.3.24.2/ks_so-tachikomaArm64v8aRelease-3.3.24.2.apk
https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/tachikoma/3.3.24.2/ks_so-tachikomaLiteArmeabiv7aRelease-3.3.24.2.apk
https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/tachikoma/3.3.24.2/ks_so-tachikomaArmeabiv7aRelease-3.3.24.2.apk
https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDK/offline_components/obiwan/ks_so-obiwanNoSoRelease-3.3.31.1-261163b35a-47.zip
https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDK/offline_components/adLive/ks_so-adLiveNoSoRelease-3.3.32.1-f1f921211-59.zip
https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDK/adLive/3.3.26.1/ks_so-adLiveArm64v8aRelease-3.3.26.1.apk
https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/adLive/3.3.26.1/ks_so-adLiveArmeabiv7aRelease-3.3.26.1.apk
https://github.com/lingochamp/FileDownloader/wiki/filedownloader.properties
https://webcast-open.douyin.com
https://webcast-open.douyin.com/webcast/openapi/pangle/setting?app_id=
https://webcast.amemv.com/falcon/webcast_douyin/page/anchor_v2/panel/index.html?web_bg_color=%23ff161823

https://webcast.amemv.com/falcon/webcast_douyin/page/recharge_v1/index.html
https://aaid.umeng.com/api/postZdata
https://aaid.umeng.com/api/updateZdata
https://plbslog.umeng.com
https://ulogs.umeng.com
https://ouplog.umeng.com
https://ulogs.umeng.com
https://alogus.umeng.com
https://alogsus.umeng.com
https://ulogs.umengcloud.com
https://pslog.umeng.com
https://pslog.umeng.com/
https://developer.umeng.com/docs/66632/detail/
http://developer.umeng.com/docs/66650/cate/66650
https://log.tbs.qq.com/ajax?c=pu&v=2&k=
https://log.tbs.qq.com/ajax?c=pu&tk=
https://log.tbs.qq.com/ajax?c=dl&k=
https://cfg.imtt.qq.com/tbs?v=2&mk=
https://log.tbs.qq.com/ajax?c=ul&v=2&k=
https://mqqad.html5.qq.com/adjs
https://log.tbs.qq.com/ajax?c=ucfu&k=
https://tbsrecovery.imtt.qq.com/getconfig
https://soft.tbs.imtt.qq.com/17421/tbs_res_imtt_tbs_DebugPlugin_DebugPlugin.tbs
https://pms.mb.qq.com/rsp204
https://debugtbs.qq.com
https://debugx5.qq.com
https://debugtbs.qq.com?10000\
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=50079

https://mdc.html5.qq.com/mh?channel_id=50079&u=
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=11041
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=11047
https://www.samsungapps.com/appquery/appDetail.as?appId=
https://apps.oceanengine.com/customer/api/app/pkg_info?
https://sf6-ttcdn-tos.pstatp.com/obj/ad-tetris-site/personal-privacy-page.html
https://i.snssdk.com/
https://dc.sigmob.cn/log
https://crbug.com/581399

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

手机线索

手机号	所在文件
17179869184	com/kwai/video/player/KsMediaMeta.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=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

🔑 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"

🔒 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.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

应用内通信