



MoGua

星河影视 4.2.0.APK 分析报告



APP名称:	星河影视
包名:	com.ganfantv.xx
域名线索:	86条
URL线索:	95条
邮箱线索:	5条
分析日期:	2025年7月22日
分析平台:	摸瓜APK反编译平台

📁 文件信息

文件名: 星河影视.apk
文件大小: 51.15MB
MD5值: ec682c3222a1238069d27d8bfc10eeec
SHA1值: 4fa46f9968029196e27ab778f6a6d41685b46769
SHA256值: f695522454ab91a59de939dff47f9699b6e8ffee5d43662b022fbb2f530ce285

i APP 信息

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

🔍 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 纬度: 35.689499 经度: 139.692322
webcast.amemv.com	IP: 123.125.216.223 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
dc.sigmob.cn	IP: 112.126.7.24 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102

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: 120.161583
aomedia.org	IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
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: 120.161583
pslog.umeng.com	IP: 59.82.29.162 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
developer.apple.com	IP: 17.253.85.205 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
configure.rayjump.com	IP: 59.110.124.183 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
changemaker.hzsanjiaomao.com	IP: 82.157.26.175 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
ads.oway.mobi	IP: 47.98.30.91 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
static.yximgs.com	IP: 39.91.183.221 所属国家: China 地区: Shandong 城市: Linyi 纬度: 35.063061 经度: 118.342781
	IP: 61.48.83.235

webcast-open.douyin.com	所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
api.yky.qq.com	IP: 116.130.223.28 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
alogsus.umeng.com	IP: 223.109.148.177 所属国家: China 地区: jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
policy.rayjump.com	IP: 59.110.124.183 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
whatwg.org	IP: 165.227.248.76 所属国家: United States of America 地区: New Jersey 城市: Clifton 纬度: 40.858585 经度: -74.163605
dns.qq.com	IP: 119.29.29.229 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
hmma.baidu.com	IP: 110.242.68.196 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
i.snssdk.com	IP: 123.125.216.198 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
exoplayer.dev	IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
	IP: 121.199.61.218 所属国家: China

api.hzsanjiaomao.com	地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
grs.dbankcloud.com	IP: 113.201.107.54 所属国家: China 地区: Shaanxi 城市: Baoji 纬度: 34.353611 经度: 107.375275
hybird.rayjump.com	IP: 111.161.121.2 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
open.e.kuaishou.com	IP: 116.136.162.35 所属国家: China 地区: Nei Mongol 城市: Hohhot 纬度: 40.810650 经度: 111.650665
119.29.29.29	IP: 119.29.29.29 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
www.w3.org	IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
test.com	IP: 67.225.146.248 所属国家: United States of America 地区: Michigan 城市: Lansing 纬度: 42.733280 经度: -84.637764
211.151.146.65	IP: 211.151.146.65 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
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 纬度: 37.775700 经度: -122.395203

analytics.rayjump.com	IP: 123.56.168.170 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
dashif.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
cpro.baidustatic.com	IP: 101.72.203.35 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
check.rayjump.com	IP: 59.110.124.183 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
tl.oway.mobi	IP: 118.178.152.152 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
tdsdk.cpatrk.net	IP: 116.198.16.229 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
sdk.hzsanjiaomao.com	IP: 221.195.216.36 所属国家: China 地区: Hebei 城市: Cangzhou 纬度: 38.316669 经度: 116.866669
cloud.tgpa.qq.com	IP: 153.3.50.50 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
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 纬度: 36.098610 经度: 120.371941

dxp.baidu.com	IP: 110.242.68.94 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
118.178.152.152	IP: 118.178.152.152 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
test.api.yky.qq.com	IP: 123.125.0.201 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
sf6-ttcdn-tos.pstatp.com	IP: 103.3.115.129 所属国家: China 地区: Zhejiang 城市: Taizhou 纬度: 28.666668 经度: 121.349998
apps.samsung.com	IP: 221.193.246.123 所属国家: China 地区: Hebei 城市: Handan 纬度: 36.600559 经度: 114.467781
api.htp.ad-scope.com.cn	IP: 47.94.43.167 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
tl.oneway.mobi	IP: 47.98.30.91 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
utoken.umeng.com	IP: 112.85.139.76 所属国家: China 地区: jiangsu 城市: Nantong 纬度: 32.030296 经度: 120.874779
lazy.rayjump.com	IP: 59.110.124.183 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102

detect.rayjump.com	IP: 52.21.161.152 所属国家: United States of America 地区: Virginia 城市: Ashburn 纬度: 39.039474 经度: -77.491806
me.cpatrk.net	IP: 116.198.14.142 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
developer.android.com	IP: 142.251.42.142 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
static.yky.qq.com	IP: 221.204.209.156 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
gist.github.com	IP: 159.24.3.173 所属国家: United States of America 地区: North Carolina 城市: Cary 纬度: 35.805500 经度: -78.794998
testcloud.tgpa.qq.com	IP: 114.222.114.87 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
ulogs.umengcloud.com	IP: 223.109.148.141 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
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
api.ipify.org	IP: 173.231.16.77 所属国家: United States of America 地区: Utah 城市: Ogden 纬度: 41.276379 经度: -111.987442

union.baidu.com	IP: 111.206.208.169 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
apps.oceanengine.com	IP: 123.125.216.203 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
ads.oneway.mobi	IP: 118.178.152.152 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
cdn-adn-https.rayjump.com	IP: 121.18.168.32 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
js-ad.a.yximgs.com	IP: 112.83.167.2 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
alogus.umeng.com	IP: 223.109.148.141 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
developer.umeng.com	IP: 59.82.31.210 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
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 纬度: 1.289987 经度: 103.850281
ulogs.umeng.com	IP: 223.109.148.177 所属国家: China 地区: Jiangsu 城市: Nanjing

	纬度: 32.061668 经度: 118.777992
schemas.microsoft.com	IP: 13.107.213.74 所属国家: United States of America 地区: Washington 城市: Redmond 纬度: 47.682899 经度: -122.120903
play.google.com	IP: 46.82.174.69 所属国家: Germany 地区: Niedersachsen 城市: Braunschweig 纬度: 52.266121 经度: 10.526730
adservice.sigmob.cn	IP: 101.200.125.221 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
owtk.audioadx.com	IP: 8.136.116.120 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
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 纬度: 39.907501 经度: 116.397102
plbslog.umeng.com	IP: 36.156.202.78 所属国家: China 地区: Jiangsu 城市: Yangzhou 纬度: 32.397221 经度: 119.435600
cloud.cpatrk.net	IP: 116.198.14.42 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
grs.dbankcloud.cn	IP: 121.36.116.8 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
	IP: 47.98.30.91 所属国家: China

track.oway.mobi	地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
developer.mozilla.org	IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568
grs.dbankcloud.asia	IP: 119.8.176.236 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
journeyapps.com	IP: 18.65.168.3 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
openrcv.baidu.com	IP: 111.206.209.112 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
owads.audioadx.com	IP: 8.136.116.120 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
www.samsungapps.com	IP: 52.31.24.56 所属国家: Ireland 地区: Dublin 城市: Dublin 纬度: 53.344151 经度: -6.267249

 URL线索

URL信息
https://crbug.com/581399
https://d.alipay.com
https://cpro.baidustatic.com/cpro/logo/sdk/mob-adlcon_2x.png
https://cpro.baidustatic.com/cpro/logo/sdk/new-bg-logo.png

http://union.baidu.com/
https://cpro.baidustatic.com/cpro/logo/sdk/mob-adlcon_2x.png
https://cpro.baidustatic.com/cpro/logo/sdk/new-bg-logo.png
http://union.baidu.com/
http://211.151.146.65:8080/wlantest/shanghai_sun/mock_ad_server_interstitial_video.json
http://hmma.baidu.com/app.gif
https://hmma.baidu.com/app.gif
https://dxp.baidu.com/vizParser
https://dxp.baidu.com/autoTracker
https://dxp.baidu.com/circleConfig?
http://openrcv.baidu.com/1010/bplus.gif
https://openrcv.baidu.com/1010/bplus.gif
https://hmma.baidu.com/auto.gif
http://datax.baidu.com/xs.gif
https://datax.baidu.com/xs.gif
http://dyp.baidu.com/upgrade
https://dyp.baidu.com/upgrade
https://github.com/danikula/AndroidVideoCache/issues/43 .
https://github.com/danikula/AndroidVideoCache/issues .
https://github.com/danikula/AndroidVideoCache/issues
https://v.behe.com/dsp20/ad/2017/5/5/28d147ed3e96a3ba8ac90703e4d66de2.jpg \
https://v.behe.com/dsp20/ad/2017/5/5/28d147ed3e96a3ba8ac90703e4d66de2.jpg
https://api.hp.ad-scope.com.cn/mb/sdk/event/v1? extInfo=wBLQeP8bmq6AuJ5DaZyc5xQQU_92OWkSUdy_6V4n2RA3Mbgehw6j67ZfwcDQCmj3uTyhCkrT8nMasQ&requestUuid=__REQUESTUUID__&eventType=__EVENTTYPE__&applID=__APPID__&spaceID=__SPACEID__&channelID=__CHANNELID__&channelApplID=__CHANNELAPPID__&ch
https://webcast.amemv.com/falcon/webcast_douyin/page/anchor_task_v2/panel/index.html?web_bg_color=%23ff161823
https://webcast.amemv.com/falcon/webcast_douyin/page/recharge_v1/index.html
https://webcast-open.douyin.com
https://webcast-open.douyin.com/webcast/openapi/pangle/setting?app_id=
https://dc.sigmob.cn/log

https://([\s\\S]*)
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://passport.kuaishou.com/account-h5/login?smallWebview=true&sid=kuaishou.unioncontent.wallpaper
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://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/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/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://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/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://open.e.kuaishou.com/rest/e/v3/open/sdk2
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
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
http://%s:%d/%s
https://github.com/danikula/AndroidVideoCache/issues/43 .
https://github.com/danikula/AndroidVideoCache/issues .
https://github.com/danikula/AndroidVideoCache/issues/88 .
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
http://apps.samsung.com/appquery/appDetail.as?appId=
https://github.com/lingochamp/FileDownloader/wiki/filedownloader.properties
https://hybird.rayjump.com/rv/authoriztion.html
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://play.google.com/
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
http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense
http://www.w3.org/ns/ttml
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.
http://changemaker.hzsanjiaomao.com:6688/105009
http://sdk.hzsanjiaomao.com/sspconfig/%s.txt
https://i.snssdk.com/
https://sf6-ttcdn-tos.pstatp.com/obj/ad-tetris-site/personal-privacy-page.html
https://apps.oceanengine.com/customer/api/app/pkg_info?
https://www.samsungapps.com/appquery/appDetail.as?appid=
https://test.api.yky.qq.com/

https://api.yky.qq.com/
https://static.yky.qq.com/bridge-h5/latest/dist/js-bridge-h5.umd.js
https://test.api.yky.qq.com/
https://api.yky.qq.com/
http://119.29.29.29/d?dn=
https://test.com
https://test.api.yky.qq.com/
https://api.yky.qq.com/
https://github.com/danikula/AndroidVideoCache/issues/43 .
https://github.com/danikula/AndroidVideoCache/issues .
https://github.com/danikula/AndroidVideoCache/issues/88 .
https://cloud.tgpa.qq.com
https://cloud.tgpa.qq.com
https://testcloud.tgpa.qq.com
https://cloud.cpatrk.net/configcloud/rest/sdk/gdprCheck
https://tdsdk.cpatrk.net/n/a/v1
https://cloud.cpatrk.net/configcloud/rest/sdk/match
https://me.cpatrk.net
https://dns.qq.com
http://developer.umeng.com/docs/66650/cate/66650
https://developer.umeng.com/docs/119267/detail/182050
https://developer.umeng.com/docs/66632/detail/
https://plbslog.umeng.com
https://ulogs.umeng.com
https://alogus.umeng.com
https://ulogs.umeng.com
https://alogus.umeng.com
https://alogus.umeng.com
https://alogus.umeng.com

https://ulogs.umengcloud.com
https://pslog.umeng.com
https://pslog.umeng.com/
https://utoken.umeng.com/apl/postZdata/v4
https://utoken.umeng.com/api/updateZdata/v4
https://adservice.sigmob.cn/strategy/v5
https://dc.sigmob.cn/log
https://adservice.sigmob.cn/extconfig?
https://adservice.sigmob.cn/windmill/config?
https://aomedia.org/emsg/ID3
https://developer.apple.com/streaming/emsg-id3
https://exoplayer.dev/issues/cleartext-not-permitted
https://developer.android.com/guide/topics/permissions/overview
http://sdk.hzsanjiaomao.com/sjmconfig/%s.json
https://d.alipay.com
http://api.hzsanjiaomao.com/api/adEvent
https://tl.oneway.mobi
http://track.oway.mobi
http://tl.oway.mobi
http://owtk.audioadx.com
http://118.178.152.152
https://ads.oneway.mobi
http://ads.oway.mobi
http://owads.audioadx.com
http://android.asset/
http://dashif.org/guidelines/last-segment-number
http://dashif.org/guidelines/trickmode
http://dashif.org/thumbnail_tile

http://dashif.org/guidelines/thumbnail_tile
http://ns.adobe.com/xap/1.0/
https://api.ipify.org
https://journeyapps.com/
https://github.com/journeyapps/zxing-android-embedded
https://grs.dbankcloud.com
https://grs.dbankcloud.cn
https://grs.dbankcloud.eu
https://grs.dbankcloud.asia
https://www.jsdelivr.com/using-sri-with-dynamic-files
https://github.com/apvarun/toastify-js
https://github.com/richttr/NoSleep.js/issues/15
https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released)

 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/video/cache/h.java
danikula@gmail.com	com/sigmob/sdk/video/cache/j.java
danikula@gmail.com	com/tencent/klewin/e/j/d.java

 手机线索

手机号	所在文件
17179869184	com/kwai/video/player/KsMediaMeta.java
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: 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: 64b0c245140528c4fceb1c506950906d9e15b60
sha256值: 4c7eb1318a4ac726f98423622a2a4bbc23c72bd8446f389af3b62781642764c4
sha512值: a45d982ce60a1c6d832886a4244d925f026611a3c053325b71bab2326ae1287a0878d02817b6c699b56e1652d24d17d215a820a4b0972c2aed6feab56dd42059
公钥算法: rsa
密钥长度: 2048
指纹: 20faa2414e1cab0b876adce1a53bdea7c80323eebcb85cf0e29dffabd5399093

🔑 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/"

🛡️ 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.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

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](#) 自动生成，并非包含所有检测结果，有疑问请联系管理员。