MoGua

韩剧TV 1.4.5.APK 分析报告

APP名称:	韩剧TV
包名:	com.xyhj.hanju
域名线索:	63条
URL线索:	5条

邮箱线索:	0条
分析日期:	2025年8月20日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: com.xyhj.hanju_1.4.5.apk
文件大小: 61.91MB
MD5值: 6a83efb67ab8604d49b15484dcae6698
SHA1值: ab017f3f0f0e0786c58d0e3e772db28f14316568
SHA256值: 0f702dcd7fdc3eefed57537406773d727ebd622bbf55d15f4c05924100ed2bdb

APP 信息

App名称: 韩剧TV
包名: com.xyhj.hanju
主活动Activity: com.xyhj.hanju.ui.activity.WelcomeActivity
安卓版本名称: 1.4.5
安卓版本: 20500

域名线索

域名	服务器信息
adsmind.ugdtimg.com	**IP**: 14.205.93.185 **所属国家**: China **地区**: Yunnan **城市**: Yuxi **纬度**: 24.354839 **经度**: 102.541969
ugo.xiawan8.com	**IP**: 47.94.92.251 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
win.gdt.qq.com	**IP**: 220.194.116.80 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
ichannel.snssdk.com	**IP**: 116.136.186.207 **所属国家**: China **地区**: Nei Mongol **城市**: Hohhot **纬度**: 40.810650 **经度**: 111.650665
www.pangle.cn	**IP**: 116.196.135.205 **所属国家**: China **地区**: Zhejiang **城市**: Jinhua **纬度**: 30.013470 **经度**: 120.288658
100000189777.retail.n.weimob.com	**IP**: 212.64.63.139 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
cpro.baidustatic.com	**IP**: 101.72.203.38 **所属国家**: China **地区**: Hebei **城市**: Langfang **纬度**: 39.509720 **经度**: 116.694717
	IP: 60.28.203.192

toblog.ctobsnssdk.com	IP: 60.28.205.192 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
cdn-tos-cn.bytedance.net	IP: 10.8.6.203 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
mobads-pre-config.cdn.bcebos.com	IP: 123.117.132.38 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
connectivitycheck.gstatic.com	IP: 203.208.43.98 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
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
qzs.qq.com	IP: 116.196.150.247 **所属国家**: China **地区**: Zhejiang **城市**: Jinhua **纬度**: 30.013470 **经度**: 120.288658
tdid.m.qq.com	IP: 60.29.240.40 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
conf.qyb.qcloud.com	IP: 153.37.101.52 **所属国家**: China **地区**: Jiangsu

conf.qvb.qcloud.com	**城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
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
api-access.pangolin-sdk-toutiao.com	IP: 124.95.161.37 **所属国家**: China **地区**: Liaoning **城市**: Shenyang **纬度**: 41.792221 **经度**: 123.432877
dht.qvb.qcloud.com	IP: 220.194.117.142 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
playable.oceanengine.com	IP: 116.196.135.202 **所属国家**: China **地区**: Zhejiang **城市**: Jinhua **纬度**: 30.013470 **经度**: 120.288658
log.qvb.qcloud.com	IP: 220.196.132.69 **所属国家**: China **地区**: Jiangsu **城市**: Zhenjiang **纬度**: 32.209366 **经度**: 119.434372
opensource.org	IP: 172.67.26.198 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
g.fancyapi.com	IP: 123.126.109.215 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102

meta.qvb.qcloud.com	IP: 60.29.254.109 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
applog.snssdk.com	IP: 42.56.93.208 **所属国家**: China **地区**: Liaoning **城市**: Shenyang **纬度**: 41.792221 **经度**: 123.432877
lupic.cdn.bcebos.com	IP: 221.204.49.35 **所属国家**: China **地区**: Shanxi **城市**: Taiyuan **纬度**: 37.869438 **经度**: 112.561508
i.gtimg.cn	IP: 42.236.6.230 **所属国家**: China **地区**: Henan **城市**: Zhengzhou **纬度**: 34.757778 **经度**: 113.648613
cpucdn.baidu.com	IP: 101.72.203.38 **所属国家**: China **地区**: Hebei **城市**: Langfang **纬度**: 39.509720 **经度**: 116.694717
android.googlesource.com	IP: 74.125.142.82 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
rtapplog.snssdk.com	IP: 42.56.93.207 **所属国家**: China **地区**: Liaoning **城市**: Shenyang **纬度**: 41.792221 **经度**: 123.432877
	IP: 34.49.79.89

www.openssl.org	**所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
sf3-fe-tos.pglstatp-toutiao.com	IP: 125.38.11.60 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
haokan.baidu.com	IP: 111.206.209.29 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
mobads.baidu.com	IP: 111.206.208.180 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
127.0.0.1	IP: 127.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
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
sf1-amtos-cdn.bytesmanager.com	IP: 123.126.74.239 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
t2.fancyapi.com	IP: 47.94.92.251 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou

	城市: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
sdk.e.qq.com	IP: 220.194.116.72 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
119.29.29.98	IP: 119.29.29.98 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
mi.gdt.qq.com	IP: 220.194.116.121 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
m.baidu.com	IP: 110.242.71.103 **所属国家**: China **地区**: Hebei **城市**: Baoding **纬度**: 38.851109 **经度**: 115.490280
imgcache.qq.com	IP: 119.188.44.140 **所属国家**: China **地区**: Shandong **城市**: Jinan **纬度**: 36.668331 **经度**: 116.997223
aden.baidu.com	IP: 110.242.68.230 **所属国家**: China **地区**: Hebei **城市**: Baoding **纬度**: 38.851109 **经度**: 115.490280
e.qq.com	IP: 220.194.116.85 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102

union.eff.qq.com	**IP**: 157.255.219.214 **所属国家**: China **地区**: Guangdong **城市**: Shenzhen **纬度**: 22.545673 **经度**: 114.068108
log.snssdk.com	**IP**: 116.136.186.207 **所属国家**: China **地区**: Nei Mongol **城市**: Hohhot **纬度**: 40.810650 **经度**: 111.650665
cpu-openapi.baidu.com	**IP**: 153.3.238.225 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
qzs.gdtimg.com	**IP**: 61.49.23.102 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
xx.xx.xx.xx	没有服务器地理信息.
hanjutv-406be.firebaseio.com	**IP**: 34.120.160.131 **所属国家**: United States of America **地区**: Missouri **城市**: Kansas City **纬度**: 39.099731 **经度**: -94.578568
apmlog.snssdk.com	**IP**: 27.221.120.205 **所属国家**: China **地区**: Shandong **城市**: Jinan **纬度**: 36.668331 **经度**: 116.997223
phoniex.toutiao.com	**IP**: 60.222.12.201 **所属国家**: China **地区**: Shanxi **城市**: Taiyuan **纬度**: 37.869438 **经度**: 112.561508

rtlog.snssdk.com	IP: 116.196.135.203 **所属国家**: China **地区**: Zhejiang **城市**: Jinhua **纬度**: 30.013470 **经度**: 120.288658
mi-eo.gdt.qq.com	IP: 60.28.220.193 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
render-server.cdn.bcebos.com	IP: 123.117.132.38 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
cpu.baidu.com	IP: 153.3.238.55 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
tobapplog.ctobsnssdk.com	IP: 42.56.93.212 **所属国家**: China **地区**: Liaoning **城市**: Shenyang **纬度**: 41.792221 **经度**: 123.432877
success.ctobsnssdk.com	IP: 139.215.162.49 **所属国家**: China **地区**: Jilin **城市**: Changchun **纬度**: 43.880001 **经度**: 125.322777
cdn.com	IP: 54.214.22.23 **所属国家**: United States of America **地区**: Oregon **城市**: Boardman **纬度**: 45.839859 **经度**: -119.700577
	IP: 42.56.93.210 **所属国家**: China

apps.bytesfield.com	**地区**: Liaoning **城市**: Shenyang **纬度**: 41.792221 **经度**: 123.432877
qzonestyle.gtimg.cn	IP: 221.204.15.113 **所属国家**: China **地区**: Shanxi **城市**: Taiyuan **纬度**: 37.869438 **经度**: 112.561508
bes-mtj.baidu.com	IP: 103.211.221.124 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
img.alicdn.com	IP: 119.167.193.6 **所属国家**: China **地区**: Shandong **城市**: Qingdao **纬度**: 36.098610 **经度**: 120.371941

URL线索

URL**信息**	Url**所在文件**
https://hanjutv-406be.firebaseio.com	摸瓜V1引擎
https://img.alicdn.com/imgextra/i3/O1CN01yaPRML1GyyqsOZP7R_!!6000000000692-1-tps-1200-432.gif	摸瓜V2引擎

http://ugo.xiawan8.com/public/whereami	摸瓜V2引擎
http://g.fancyapi.com/s2s?	摸瓜V2引擎
http://t2.fancyapi.com/NTAwMDAwMDAwMg68af/NTAwMDAwMDAwMg68af/b? ad=__ADID__&dt=__DATA__&ex=__EXT__&l=__LBS__&m1a=__ANDROIDID__&m2=__IMEI__&m5=__IDFA__&m6a=__MAC__&mo=__OS__&nn=__APP__&ns=__IP__&oa=__OAID__&pr=__PRICE__&tr=__REQUESTID__&ts=__TS__&o=	摸瓜V2引擎
http://t2.fancyapi.com/NTAwMDAwMDAwMg68af/NTAwMDAwMDAwMg68af/e? ad=__ADID__&dt=__DATA__&ex=__EXT__&l=__LBS__&m1a=__ANDROIDID__&m2=__IMEI__&m5=__IDFA__&m6a=__MAC__&mo=__OS__&nn=__APP__&ns=__IP__&oa=__OAID__&pr=__PRICE__&tr=__REQUESTID__&ts=__TS__&o=	摸瓜V2引擎
http://t2.fancyapi.com/NTAwMDAwMDAwMg68af/NTAwMDAwMDAwMg68af/i? ad=__ADID__&dt=__DATA__&ex=__EXT__&l=__LBS__&m1a=__ANDROIDID__&m2=__IMEI__&m5=__IDFA__&m6a=__MAC__&mo=__OS__&nn=__APP__&ns=__IP__&oa=__OAID__&pr=__PRICE__&tr=__REQUESTID__&ts=__TS__&o=	摸瓜V2引擎
http://t2.fancyapi.com/NTAwMDAwMDAwMg68af/NTAwMDAwMDAwMg68af/c? ad=__ADID__&dt=__DATA__&ex=__EXT__&l=__LBS__&m1a=__ANDROIDID__&m2=__IMEI__&m5=__IDFA__&m6a=__MAC__&mo=__OS__&nn=__APP__&ns=__IP__&oa=__OAID__&pr=__PRICE__&tr=__REQUESTID__&ts=__TS__&o=	摸瓜V2引擎
http://t2.fancyapi.com/NTAwMDAwMDAwMg68af/NTAwMDAwMDAwMg68af/s? ad=__ADID__&dt=__DATA__&ex=__EXT__&l=__LBS__&m1a=__ANDROIDID__&m2=__IMEI__&m5=__IDFA__&m6a=__MAC__&mo=__OS__&nn=__APP__&ns=__IP__&oa=__OAID__&pr=__PRICE__&tr=__REQUESTID__&ts=__TS__&o=	摸瓜V2引擎
https://github.com/Tencent/vConsole)	摸瓜V2引擎
http://opensource.org/licenses/MIT	摸瓜V2

	引擎
https://github.com/Tencent/vConsole	摸瓜V2引擎
https://github.com/Tencent/vConsole.git	摸瓜V2引擎
https://dht.qvb.qcloud.com/api/v2/kad/locate?xresid=invalid	摸瓜V3引擎
https://sdk.e.qq.com/mediation?version=2	摸瓜V3引擎
http://119.29.29.98/d?id=3743&ttl=1&dn=Error	摸瓜V3引擎
https://log.snssdk.com/service/2/log_settings/	摸瓜V3引擎
https://toblog.ctobsnssdk.com/service/2/log_settings/	摸瓜V3引擎
connectivitycheck.gstatic.com	摸瓜V3引擎

https://adsmind.ugdtimg.com	摸瓜V3引擎
http://m.baidu.com	摸瓜V3引擎
https://100000189777.retail.n.weimob.com/saas/retail/100000189777/21036777/goods/detail	摸瓜V3引擎
https://mobads.baidu.com/ads/preload.php	摸瓜V3引擎
https://api-access.pangolin-sdk-toutiao.com	摸瓜V3引擎
https://mobads-pre-config.cdn.bcebos.com/sdk/feed/slide_finger.png	摸瓜V3引擎
https://sf3-fe-tos.pglstatp-toutiao.com/obj/ad-pattern/renderer/package.json	摸瓜V3引擎
https://qzs.gdtimg.com/union/res/union_cdn/page/ams_icon/ams_logo_light.png	摸瓜V3引擎
https://conf.qvb.qcloud.com/api/v4/xnet/mobilexnetrcvbufurgent_cdnp2p_costsconc_complete_costspunch_	摸瓜V3

	引擎
http://m.baidu.com/baidu.php?sc	摸瓜V3引擎
https://rtlog.snssdk.com/service/2/app_log/	摸瓜V3引擎
https://dht.qvb.qcloud.com/gen_id?ip=	摸瓜V3引擎
http://mobads.baidu.com/cpro/ui/mads.php	摸瓜V3引擎
https://cpu-openapi.baidu.com/api/v2/data/playlet/detail/ads	摸瓜V3引擎
https://log.qvb.qcloud.com/reporter/multiplep2p_download_bytesconc_interrupt_timesupload_overloadcop	摸瓜V3引擎
https://xx.xx.xx.xx	摸瓜V3引擎
https://log.snssdk.com/service/2/device_register_only/	摸瓜V3引擎

https://sf1-amtos-cdn.bytesmanager.com/obj/ad-app-package/personal-privacy-page.html	摸瓜V3引擎
https://qzs.gdtimg.com/union/res/union_cdn/page/ams_icon/ams_logo_dark.png	摸瓜V3引擎
https://conf.qvb.qcloud.com/api/v4/xnet/mobile	摸瓜V3引擎
https://tdid.m.qq.com?mc=2	摸瓜V3引擎
https://log.qvb.qcloud.com/reporter/multiple	摸瓜V3引擎
https://qzs.qq.com/union/res/union_cdn/page/images/loading_2x.gif	摸瓜V3引擎
http://hmma.baidu.com/app.gif	摸瓜V3引擎
https://phoniex.toutiao.com	摸瓜V3引擎
https://mi-eo.gdt.qq.com/	摸瓜V3

	引擎
http://aden.baidu.com/	摸瓜V3引擎
https://render-server.cdn.bcebos.com/static/images/20201231/zhongcao.png	摸瓜V3引擎
https://toblog.ctobsnssdk.com/service/2/app_alert_check/	摸瓜V3引擎
https://cdn-tos-cn.bytedance.net/obj/archi/ad/play-comp/playable-component-sdk/dev/index.ecommerce.h	摸瓜V3引擎
https://qzs.gdtimg.com/union/res/union_cdn/page/ams_icon/ams_logo_transparent.png	摸瓜V3引擎
http://127.0.0.1	摸瓜V3引擎
http://schemas.android.com/apk/res-auto	摸瓜V3引擎
https://m.baidu.com/baidu.php?sc	摸瓜V3引擎

https://cpu-openapi.baidu.com/api/v2/data/list	摸瓜V3引擎
https://mi.gdt.qq.com/	摸瓜V3引擎
https://i.gtimg.cn/ams-web/page-performance/page-performance.min.js?v=1	摸瓜V3引擎
https://cpro.baidustatic.com/cpro/logo/sdk/new-bg-logo.png	摸瓜V3引擎
https://apps.bytesfield.com/app_package_ce/appIntro	摸瓜V3引擎
https://qzonestyle.gtimg.cn/qzone/biz/gdt/mob/sdk/v2/android01/download.html	摸瓜V3引擎
https://sdk.e.qq.com/launch	摸瓜V3引擎
http://119.29.29.98/d?id=3743&ttl=1&dn=	摸瓜V3引擎
https://meta.qvb.qcloud.com/api/v3/info?xresid=next_	摸瓜V3

	引擎
https://www.pangle.cn/privacy/partner	摸瓜V3引擎
http://127.0.0.1:	摸瓜V3引擎
https://union.baidu.com	摸瓜V3引擎
https://e.qq.com/dev/index.html	摸瓜V3引擎
android.googleapis.com	摸瓜V3引擎
http://%s:%d/%s?timestamp=%s&cachefactor=%.2f&sign=%s	摸瓜V3引擎
http://www.openssl.org/support/faq.htmldual	摸瓜V3引擎
http://union.baidu.com/	摸瓜V3引擎

https://sdk.e.qq.com/activate	摸瓜V3引擎
https://applog.snssdk.com/service/2/app_log/	摸瓜V3引擎
https://toblog.ctobsnssdk.com/service/2/app_log/	摸瓜V3引擎
https://haokan.baidu.com/activity/h5/chaihongbao?productid=2&inviteCode=736CCC5X010&pd=lu&tab=guide&	摸瓜V3引擎
www.googleapis.com	摸瓜V3引擎
https://lupic.cdn.bcebos.com/static/aden_sdk_cache_larkplayer.1ed5e92.js	摸瓜V3引擎
https://playable.oceanengine.com/web-api/v1/coldstart	摸瓜V3引擎
clientservices.googleapis.com	摸瓜V3引擎
https://android.googlesource.com/toolchain/llvm-project	摸瓜V3

	引擎
https://aden.baidu.com/	摸瓜V3引擎
https://mobads-pre-config.cdn.bcebos.com/sdk/cpu/cpu_drama_playing.json	摸瓜V3引擎
https://dht.qvb.qcloud.com/gen_id?ip=xnet/xdfs/block_cdn_ttfb	摸瓜V3引擎
http://mobads-pre-config.cdn.bcebos.com/sdk/iadex/full_iadex.php	摸瓜V3引擎
http://cpu-openapi.baidu.com/api/v2/data/playlet/detail/ads	摸瓜V3引擎
http://cdn.com/precache?blkid=	摸瓜V3引擎
https://toblog.ctobsnssdk.com/service/2/device_register_only/	摸瓜V3引擎
https://cpu.baidu.com/block/app/	摸瓜V3引擎

https://success.ctobsnssdk.com/service/2/app_log/	摸瓜V3引擎
https://win.gdt.qq.com/win_notice.fcg?viewid=1	摸瓜V3引擎
https://android.googlesource.com/toolchain/clang	摸瓜V3引擎
https://cpu-openapi.baidu.com/api/v2/aggregation/channels	摸瓜V3引擎
gmscompliance-pa.googleapis.com	摸瓜V3引擎
https://tobapplog.ctobsnssdk.com/service/2/app_log/	摸瓜V3引擎
https://sdk.e.qq.com/mediation?version=1	摸瓜V3引擎
https://union.eff.qq.com/v2/query/gdtmview	摸瓜V3引擎
https://api-access.pangolin-sdk-toutiao.com/v2/inspect/aegis/client/page/	摸瓜V3

	引擎
http://mobads.baidu.com/ads/index.htm	摸瓜V3引擎
firebaseinstallations.googleapis.com	摸瓜V3引擎
http://cpu-openapi.baidu.com/api/v2/data/detailwithconfig	摸瓜V3引擎
http://127.0.0.1:user	摸瓜V3引擎
https://sf3-fe-tos.pglstatp-toutiao.com/obj/ad-pattern/static/images/	摸瓜V3引擎
https://mobads-pre-config.cdn.bcebos.com/sdk/splash/bd_splash_shake_lottie_red_package_common.json	摸瓜V3引擎
https://qzs.gdtimg.com/union/res/union_cdn/page/temp_v2/webview-cover.png	摸瓜V3引擎
http://mobads.baidu.com/	摸瓜V3引擎

https://lupic.cdn.bcebos.com/static/aden_sdk_cache_iconhand.74457e7.png	摸瓜V3引擎
https://ichannel.snssdk.com/service/2/app_alert_check/	摸瓜V3引擎
http://schemas.android.com/aapt	摸瓜V3引擎
https://hmma.baidu.com/app.gif	摸瓜V3引擎
https://mobads-pre-config.cdn.bcebos.com/sdk/splash/mix_interact_shake.json	摸瓜V3引擎
https://cpucdn.baidu.com/static/assets/sdk-cache.cache-packages.3d231ecb.chunk.js	摸瓜V3引擎
https://apmlog.snssdk.com/apm/collect/crash/	摸瓜V3引擎
https://bes-mtj.baidu.com/auto.gif	摸瓜V3引擎
https://toblog.ctobsnssdk.com/service/2/abtest_config/	摸瓜V3

	引擎
https://rtapplog.snssdk.com/service/2/app_log/	摸瓜V3引擎
https://imgcache.qq.com/qzone/biz/gdt/dev/sdk/cdn/resources/common/SdkRewardAdLogo.png	摸瓜V3引擎
https://cpucdn.baidu.com/static/assets/sdk-cache.cache-lottie.94178d47.chunk.js	摸瓜V3引擎
http://www.openssl.org/support/faq.html	摸瓜V3引擎
https://mobads-pre-config.cdn.bcebos.com/sdk/splash/mix_interact_slide.json	摸瓜V3引擎
http://cpu-openapi.baidu.com/api/v2/data/novel/detail/ads	摸瓜V3引擎

邮箱线索

手机线索

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=86, ST=hj, L=hj, O=xyhj, OU=xyhj, CN=han ju
签名算法: rsassa_pkcs1v15
有效期自: 2022-11-25 03:17:10+00:00
有效期至: 2122-11-01 03:17:10+00:00
发行人: C=86, ST=hj, L=hj, O=xyhj, OU=xyhj, CN=han ju
序列号: 0x4740b75f
哈希算法: sha256
md5值: 80691c79ac5ca386d8e4d588fd538131
sha1值: 6b0fa604fffa1d81cd019586cf481dd183674d1c
sha256值: bf841914287ee20bbfc26780d610df8c95e4cc9b2dd7746b19aad2090ee2fa96
sha512值: aea8e74040dcca11237600bb211ed1da580698a1e4ba1e7ba0b8d386b76f960f908f5c93691d4e783ae7b3aae204019ce6bab955d03c75d52c67ad3675918680
公钥算法: rsa
密钥长度: 2048
指纹: 1e7e6539623b2f075fe2d2e0a2001d504acc1903fa0147db340684112fe299a0

🔑 硬编码敏感信息

可能的敏感信息
"firebase_database_url" : "https://hanjutv-406be.firebaseio.com"
"google_api_key" : "AIzaSyCCzOWQ6MfYdqzrPe9SZJVVEStWVacYZss"
"google_crash_reporting_api_key" : "AIzaSyCCzOWQ6MfYdqzrPe9SZJVVEStWVacYZss"
"identification_and_authentication" : "用户网络标识和鉴权信息"
"mobad_compliance_author" : ""
"opos_mob_reward_install_key" : "安装完成"
"opos_mob_reward_key" : "领取奖励"
"opos_mob_reward_open_key" : "打开应用"
"opos_mob_reward_open_without_install_key" : "下载打开应用"
"opos_mob_reward_spilt_key" : "/"
"opos_mob_reward_video_complete_key" : "看%s"

"opos_mob_reward_without_video_complete_key" : "%s"
"phone_token_expired" : "token已失效"
"question_token_fail" : "登录token失效、请重试"
"ttdp_author_desc_more" : "更多"
"ttdp_author_loadmore_no" : "暂无更多内容"
"ttdp_author_loadmore_yes" : "加载更多..."
"ttdp_author_works_count" : "作品 %1$s"
"ttdp_block_author" : "拉黑"
"ttdp_block_author_failed" : "拉黑失败请重试"
"ttdp_block_author_success" : "已拉黑"
"ttdp_follow_when_author_blocked" : "请解除拉黑后再关注哦"
"ttdp_unblock_author" : "解除拉黑"
"ttdp_unblock_author_failed" : "解除失败请重试"
"ttdp_unblock_author_success" : "已解除拉黑"
"mobad_compliance_author" : "开发者： "
"opos_mob_reward_install_key" : "安装完成"
"opos_mob_reward_key" : "领取奖励"
"opos_mob_reward_open_key" : "打开应用"
"opos_mob_reward_open_without_install_key" : "下载打开应用"
"opos_mob_reward_spilt_key" : "/"
"opos_mob_reward_video_complete_key" : "看%s"
"opos_mob_reward_without_video_complete_key" : "%s"

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_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.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.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.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VIDEO	未知	Unknown permission	Unknown permission from android reference
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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。
[illegible]	[illegible]	[illegible]	[illegible]

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.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕
android.permission.BROADCAST_PACKAGE_ADDED	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_CHANGED	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_INSTALL	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_REPLACED	未知	Unknown permission	Unknown permission from android reference
android.permission.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
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。
com.android.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
android.permission.DISABLE_KEYGUARD	正常		如果键盘不安全,允许应用程序禁用它。
android.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
android.permission.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由
org.simalliance.openmobileapi.SMARTCARD	未知	Unknown permission	Unknown permission from android reference
android.permission.ACTIVITY_RECOGNITION	危险	允许应用程序识别身体活动	允许应用程序识别身体活动
android.permission.READ_CALENDAR	危险	读取日历事件	允许应用程序读取您手机上存储的所有日历事件。恶意应用程序可以借此将您的日历事件发送给其他人
android.permission.WRITE_CALENDAR	危险	添加或修改日历事件并向客人发送电子邮件	允许应用程序添加或更改日历上的事件,这可能会向客人发送电子邮件。恶意应用程序可以使用它来删除或修改您的日历活动或向客人发送电子邮件
miui.permission.READ_STEPS	未知	Unknown permission	Unknown permission from android reference
com.xyhj.hanju.andpermission.bridge	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
com.xyhj.hanju.heytap.msp.mobad.BROADCAST_PERMISSION	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_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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
freemme.permission.msa	未知	Unknown permission	Unknown permission from android reference
com.xyhj.hanju.openadsdk.permission.TT_PANGOLIN	未知	Unknown permission	Unknown permission from android reference
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.permissio.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
com.xyhj.hanju.permission.KW_SDK_BROADCAST	未知	Unknown permission	Unknown permission from android reference
com.google.android.gms.permission.AD_ID	未知	Unknown permission	Unknown permission from android reference
com.huawei.android.launcher.permission.CHANGE_BADGE	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.vivo.notification.permission.BADGE_ICON	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.xyhj.hanju.ui.activity.WelcomeActivity	Schemes: sa9c619904://,
com.xyhj.hanju.ui.activity.ZtvHomeActivity	Schemes: xyhanju://, Hosts: quickOpen,
com.xyhj.hanju.search.activity.SearchResultActivity	Schemes: xyhanju://, Hosts: search,
com.xyhj.hanju.vip.activity.VipPayActivity	Schemes: xyhanju://, Hosts: openvip,
com.tencent.tauth.AuthActivity	Schemes: tencent1105303990://,

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。