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

**韩剧TV（ 1.4.5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 | 韩剧TV |
| 版本 | 1.4.5 |
| 包名 | com.xyhj.hanju |
| 域名线索 | 63条 |
| URL线索 | 5条 |
| APP图标 |  |
| 分析日期 | 2025年8月20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.xyhj.hanju\_1.4.5.apk |
| 文件大小 | 61.91MB |
| MD5值 | 6a83efb67ab8604d49b15484dcae6698 |
| SHA1值 | ab017f3f0f0e0786c58d0e3e772db28f14316568 |
| SHA256值 | 0f702dcd7fdc3eefed57537406773d727ebd622bbf55d15f4c05924100ed2bdb |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| 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 |

## **4. 线索情况**

### **4.1 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  |
| ugo.xiawan8.com | IP: 47.94.92.251 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| win.gdt.qq.com | IP: 220.194.116.80 所属国家: China 地区: Tianjin 城市: Tianjin  |
| ichannel.snssdk.com | IP: 116.136.186.207 所属国家: China 地区: Nei Mongol 城市: Hohhot  |
| www.pangle.cn | IP: 116.196.135.205 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| 100000189777.retail.n.weimob.com | IP: 212.64.63.139 所属国家: China 地区: Beijing 城市: Beijing  |
| cpro.baidustatic.com | IP: 101.72.203.38 所属国家: China 地区: Hebei 城市: Langfang  |
| toblog.ctobsnssdk.com | IP: 60.28.203.192 所属国家: China 地区: Tianjin 城市: Tianjin  |
| cdn-tos-cn.bytedance.net | IP: 10.8.6.203 所属国家: - 地区: - 城市: -  |
| mobads-pre-config.cdn.bcebos.com | IP: 123.117.132.38 所属国家: China 地区: Beijing 城市: Beijing  |
| connectivitycheck.gstatic.com | IP: 203.208.43.98 所属国家: China 地区: Beijing 城市: Beijing  |
| hmma.baidu.com | IP: 110.242.68.196 所属国家: China 地区: Hebei 城市: Baoding  |
| qzs.qq.com | IP: 116.196.150.247 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| tdid.m.qq.com | IP: 60.29.240.40 所属国家: China 地区: Tianjin 城市: Tianjin  |
| conf.qvb.qcloud.com | IP: 153.37.101.52 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| union.baidu.com | IP: 111.206.208.169 所属国家: China 地区: Beijing 城市: Beijing  |
| api-access.pangolin-sdk-toutiao.com | IP: 124.95.161.37 所属国家: China 地区: Liaoning 城市: Shenyang  |
| dht.qvb.qcloud.com | IP: 220.194.117.142 所属国家: China 地区: Tianjin 城市: Tianjin  |
| playable.oceanengine.com | IP: 116.196.135.202 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| log.qvb.qcloud.com | IP: 220.196.132.69 所属国家: China 地区: Jiangsu 城市: Zhenjiang  |
| opensource.org | IP: 172.67.26.198 所属国家: United States of America 地区: California 城市: San Francisco  |
| g.fancyapi.com | IP: 123.126.109.215 所属国家: China 地区: Beijing 城市: Beijing  |
| meta.qvb.qcloud.com | IP: 60.29.254.109 所属国家: China 地区: Tianjin 城市: Tianjin  |
| applog.snssdk.com | IP: 42.56.93.208 所属国家: China 地区: Liaoning 城市: Shenyang  |
| lupic.cdn.bcebos.com | IP: 221.204.49.35 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| i.gtimg.cn | IP: 42.236.6.230 所属国家: China 地区: Henan 城市: Zhengzhou  |
| cpucdn.baidu.com | IP: 101.72.203.38 所属国家: China 地区: Hebei 城市: Langfang  |
| android.googlesource.com | IP: 74.125.142.82 所属国家: United States of America 地区: California 城市: Mountain View  |
| rtapplog.snssdk.com | IP: 42.56.93.207 所属国家: China 地区: Liaoning 城市: Shenyang  |
| www.openssl.org | IP: 34.49.79.89 所属国家: United States of America 地区: California 城市: Mountain View  |
| sf3-fe-tos.pglstatp-toutiao.com | IP: 125.38.11.60 所属国家: China 地区: Tianjin 城市: Tianjin  |
| haokan.baidu.com | IP: 111.206.209.29 所属国家: China 地区: Beijing 城市: Beijing  |
| mobads.baidu.com | IP: 111.206.208.180 所属国家: China 地区: Beijing 城市: Beijing  |
| 127.0.0.1 | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| sf1-amtos-cdn.bytesmanager.com | IP: 123.126.74.239 所属国家: China 地区: Beijing 城市: Beijing  |
| t2.fancyapi.com | IP: 47.94.92.251 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| sdk.e.qq.com | IP: 220.194.116.72 所属国家: China 地区: Tianjin 城市: Tianjin  |
| 119.29.29.98 | IP: 119.29.29.98 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| mi.gdt.qq.com | IP: 220.194.116.121 所属国家: China 地区: Tianjin 城市: Tianjin  |
| m.baidu.com | IP: 110.242.71.103 所属国家: China 地区: Hebei 城市: Baoding  |
| imgcache.qq.com | IP: 119.188.44.140 所属国家: China 地区: Shandong 城市: Jinan  |
| aden.baidu.com | IP: 110.242.68.230 所属国家: China 地区: Hebei 城市: Baoding  |
| e.qq.com | IP: 220.194.116.85 所属国家: China 地区: Tianjin 城市: Tianjin  |
| union.eff.qq.com | IP: 157.255.219.214 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| log.snssdk.com | IP: 116.136.186.207 所属国家: China 地区: Nei Mongol 城市: Hohhot  |
| cpu-openapi.baidu.com | IP: 153.3.238.225 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| qzs.gdtimg.com | IP: 61.49.23.102 所属国家: China 地区: Beijing 城市: Beijing  |
| 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  |
| apmlog.snssdk.com | IP: 27.221.120.205 所属国家: China 地区: Shandong 城市: Jinan  |
| phoniex.toutiao.com | IP: 60.222.12.201 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| rtlog.snssdk.com | IP: 116.196.135.203 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| mi-eo.gdt.qq.com | IP: 60.28.220.193 所属国家: China 地区: Tianjin 城市: Tianjin  |
| render-server.cdn.bcebos.com | IP: 123.117.132.38 所属国家: China 地区: Beijing 城市: Beijing  |
| cpu.baidu.com | IP: 153.3.238.55 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| tobapplog.ctobsnssdk.com | IP: 42.56.93.212 所属国家: China 地区: Liaoning 城市: Shenyang  |
| success.ctobsnssdk.com | IP: 139.215.162.49 所属国家: China 地区: Jilin 城市: Changchun  |
| cdn.com | IP: 54.214.22.23 所属国家: United States of America 地区: Oregon 城市: Boardman  |
| apps.bytesfield.com | IP: 42.56.93.210 所属国家: China 地区: Liaoning 城市: Shenyang  |
| qzonestyle.gtimg.cn | IP: 221.204.15.113 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| bes-mtj.baidu.com | IP: 103.211.221.124 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| img.alicdn.com | IP: 119.167.193.6 所属国家: China 地区: Shandong 城市: Qingdao  |

### **4.2 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  |

### **4.3 邮箱线索**

### **4.4 手机号线索**

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: True 找到 1 个唯一证书 主题: C=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**

## **6. 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"  |

## **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\_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。 |
| 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 |

## **10. 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**](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。**