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

**电视家（ 9099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 | 电视家 |
| 版本 | 9099 |
| 包名 | com.television.enthusiasts |
| 域名线索 | 95条 |
| URL线索 | 42条 |
| APP图标 |  |
| 分析日期 | 2025年10月2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 | 电视家\_v9.0.99【聚玩盒子】.apk |
| 文件大小 | 17.86MB |
| MD5值 | 57d7d91c59aeb4d8d196f8910e2071d8 |
| SHA1值 | ff36d7155aa651af0feb0474f5e43524962c5ac3 |
| SHA256值 | dcf6b952e4acd7ccb976f59c87a4f567732e5a525a8e38f2dde8e20358ffcb52 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 电视家 |
| 包名 | com.television.enthusiasts |
| 主活动Activity | com.qy.kktv.miaokan.equity.SwitchActivity |
| 安卓版本名称 | 9099 |
| 安卓版本 | 9099 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| programs.nextaifun.com | IP: 125.38.11.152  所属国家: China  地区: Tianjin  城市: Tianjin |
| pslog.umeng.com | IP: 59.82.60.43  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| cdn.nextaifun.com | IP: 122.156.133.107  所属国家: China  地区: Heilongjiang  城市: Heihe |
| audid.umeng.com | IP: 123.183.232.13  所属国家: China  地区: Hebei  城市: Shijiazhuang |
| worldtimeapi.org | IP: 213.188.196.246  所属国家: Netherlands  地区: Noord-Holland  城市: Amsterdam |
| sss.umeng.com | IP: 59.82.31.92  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| as2.binstream.live | IP: 132.232.111.139  所属国家: China  地区: Beijing  城市: Beijing |
| javax.xml.xmlconstants | 没有服务器地理信息. |
| astat.bugly.cros.wr.pvp.net | IP: 170.106.118.26  所属国家: United States of America  地区: California  城市: San Francisco |
| tm2.binstream.live | IP: 132.232.111.139  所属国家: China  地区: Beijing  城市: Beijing |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| 4403-hs.otvstream.otvcloud.com | IP: 60.221.21.150  所属国家: China  地区: Shanxi  城市: Taiyuan |
| g3.letv.com | IP: 125.36.181.26  所属国家: China  地区: Tianjin  城市: Tianjin |
| www.walle-web.io | IP: 23.248.162.194  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| yd.cdn.nextaifun.com | IP: 122.156.133.106  所属国家: China  地区: Heilongjiang  城市: Heihe |
| tm3.binstream.live | IP: 188.131.178.178  所属国家: China  地区: Beijing  城市: Beijing |
| dtrace.ysp.cctv.cn | IP: 120.53.131.248  所属国家: China  地区: Beijing  城市: Beijing |
| android.bugly.qq.com | IP: 124.95.225.146  所属国家: China  地区: Liaoning  城市: Shenyang |
| live.cgtn.com | IP: 125.38.5.12  所属国家: China  地区: Tianjin  城市: Tianjin |
| kxmapp.mapi1.kxm.xmtv.cn | IP: 123.60.238.167  所属国家: China  地区: Guangdong  城市: Guangzhou |
| amdcopen.m.umeng.com | 没有服务器地理信息. |
| www.hljtv.com | IP: 221.212.177.42  所属国家: China  地区: Heilongjiang  城市: Harbin |
| cctvalih5ca.v.myalicdn.com | IP: 169.254.254.254  所属国家: -  地区: -  城市: - |
| gcc.gnu.org | IP: 8.43.85.97  所属国家: United States of America  地区: North Carolina  城市: Raleigh |
| ikukan.cn | IP: 119.23.247.140  所属国家: China  地区: Guangdong  城市: Shenzhen |
| errnewlog.umeng.com | IP: 223.109.148.143  所属国家: China  地区: Jiangsu  城市: Nanjing |
| as4.binstream.live | IP: 212.129.136.254  所属国家: China  地区: Beijing  城市: Beijing |
| msg.umengcloud.com | IP: 124.239.14.132  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| o18657i542.iask.in | IP: 124.230.180.130  所属国家: China  地区: Hunan  城市: Shaoyang |
| m.lasatv.cn | IP: 123.125.216.218  所属国家: China  地区: Beijing  城市: Beijing |
| hls.nextaifun.com | IP: 125.38.11.151  所属国家: China  地区: Tianjin  城市: Tianjin |
| live.fjtv.net | IP: 116.172.75.13  所属国家: China  地区: Gansu  城市: Lanzhou |
| api.cdn.nextaifun.com | IP: 125.38.11.150  所属国家: China  地区: Tianjin  城市: Tianjin |
| www.openssl.org | IP: 34.49.79.89  所属国家: United States of America  地区: California  城市: Mountain View |
| iptv.deeptop.com.cn | IP: 124.222.131.122  所属国家: China  地区: Beijing  城市: Beijing |
| privacy.qq.com | IP: 119.188.86.134  所属国家: China  地区: Shandong  城市: Jinan |
| errnewlogos.umeng.com | IP: 47.246.110.96  所属国家: Singapore  地区: Singapore  城市: Singapore |
| cctvtxyh5ca.liveplay.myqcloud.com | IP: 115.56.90.122  所属国家: China  地区: Henan  城市: Jiaozuo |
| scgctvshow.sctv.com | IP: 116.196.148.70  所属国家: China  地区: Zhejiang  城市: Jinhua |
| kiqk.bdy.lnyun.com.cn | IP: 39.98.192.152  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| 154.19.70.157 | IP: 154.19.70.157  所属国家: United States of America  地区: District of Columbia  城市: Washington |
| 127.0.0.1 | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| mozilla.org | IP: 35.190.14.201  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| arm.zcj1.hiajfxo.cn | IP: 61.164.109.18  所属国家: China  地区: Zhejiang  城市: Wenzhou |
| keep.nextaifun.com | IP: 8.152.154.235  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| alogus.umeng.com | IP: 223.109.148.130  所属国家: China  地区: Jiangsu  城市: Nanjing |
| h5access.yangshipin.cn | IP: 81.70.60.180  所属国家: China  地区: Beijing  城市: Beijing |
| as3.binstream.live | IP: 188.131.178.178  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 |
| live.miguvideo.com | IP: 218.98.20.126  所属国家: China  地区: Shandong  城市: Jinan |
| www.baidu.com | IP: 110.242.68.4  所属国家: China  地区: Hebei  城市: Baoding |
| app.api.ulivetv.net | IP: 163.181.35.231  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| www.yangshipin.c | 没有服务器地理信息. |
| ulogs.umengcloud.com | IP: 223.109.148.130  所属国家: China  地区: Jiangsu  城市: Nanjing |
| player.hoge.cn | IP: 123.125.16.232  所属国家: China  地区: Beijing  城市: Beijing |
| player-api.yangshipin.cn | IP: 101.42.114.129  所属国家: China  地区: Beijing  城市: Beijing |
| ccs.umeng.com | IP: 110.253.189.200  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| tm1.binstream.live | IP: 134.175.7.236  所属国家: China  地区: Beijing  城市: Beijing |
| live3.hrtn.net | 没有服务器地理信息. |
| www.ahtv.cn | IP: 121.22.239.35  所属国家: China  地区: Hebei  城市: Qinhuangdao |
| sn.nextaifun.com | IP: 123.56.14.42  所属国家: China  地区: Beijing  城市: Beijing |
| umengacs.m.taobao.com | IP: 110.253.189.208  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| www.a.shifen.com | IP: 110.242.68.4  所属国家: China  地区: Hebei  城市: Baoding |
| offmsg.umeng.com | IP: 59.82.31.95  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| www.olympicchannelchina.cn | IP: 123.125.46.43  所属国家: China  地区: Beijing  城市: Beijing |
| alogsus.umeng.com | IP: 223.109.148.176  所属国家: China  地区: Jiangsu  城市: Nanjing |
| live2.wisetv.com.cn | IP: 123.125.46.7  所属国家: China  地区: Beijing  城市: Beijing |
| www.w3.org | IP: 104.18.23.19  所属国家: United States of America  地区: California  城市: San Francisco |
| msgacs.m.umeng.com.gds.alibabadns.com | IP: 110.253.189.208  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| cdn.nextaifun.com.w.kunlunaq.com | IP: 122.156.133.107  所属国家: China  地区: Heilongjiang  城市: Heihe |
| www.live.com | IP: 204.79.197.212  所属国家: United States of America  地区: Washington  城市: Redmond |
| test.api.nextaifun.com | IP: 123.56.239.160  所属国家: China  地区: Beijing  城市: Beijing |
| infoaibos.oss-cn-beijing.aliyuncs.com | IP: 39.97.203.46  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| poll.nextaifun.com | IP: 47.94.173.41  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| vjpi.bdy.lnyun.com.cn | IP: 39.98.85.183  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| www.wshifen.com | IP: 103.235.46.96  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| plbslog.umeng.com | IP: 36.156.202.68  所属国家: China  地区: Jiangsu  城市: Yangzhou |
| 42e83a32dc4e03efd8bbca6906228db9.h2.smtcdns.net | IP: 118.183.33.49  所属国家: China  地区: Gansu  城市: Tianshui |
| h.trace.qq.com | IP: 113.56.189.162  所属国家: China  地区: Hubei  城市: Huangshi |
| 123.57.155.33 | IP: 123.57.155.33  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| cctvcnch5ca.v.wscdns.com | 没有服务器地理信息. |
| errlog.umeng.com | IP: 223.109.148.129  所属国家: China  地区: Jiangsu  城市: Nanjing |
| ulogs.umeng.com | IP: 223.109.148.179  所属国家: China  地区: Jiangsu  城市: Nanjing |
| astat.bugly.qcloud.com | IP: 119.28.121.133  所属国家: Singapore  地区: Singapore  城市: Singapore |
| play.miguvideo.com | IP: 218.98.20.43  所属国家: China  地区: Shandong  城市: Jinan |
| developer.umeng.com | IP: 59.82.29.163  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| cdn.media.ulivetv.net | IP: 104.18.5.68  所属国家: United States of America  地区: California  城市: San Francisco |
| 47.94.13.7 | IP: 47.94.13.7  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| utoken.umeng.com | IP: 223.109.148.139  所属国家: China  地区: Jiangsu  城市: Nanjing |
| tm4.binstream.live | IP: 212.129.136.254  所属国家: China  地区: Beijing  城市: Beijing |
| msgacs.m.umeng.com | IP: 110.253.189.208  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| weblive.olympicchannelchina.cn | IP: 125.38.11.164  所属国家: China  地区: Tianjin  城市: Tianjin |
| www.yangshipin.cn | IP: 116.196.152.179  所属国家: China  地区: Zhejiang  城市: Jinhua |
| errlogos.umeng.com | IP: 47.246.110.18  所属国家: Singapore  地区: Singapore  城市: Singapore |
| as1.binstream.live | IP: 134.175.7.236  所属国家: China  地区: Beijing  城市: Beijing |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://errnewlogos.umeng.com/api/crashsdk/logcollect | com/efs/sdk/base/core/controller/ControllerCenter.java |
| https://errnewlog.umeng.com/api/crashsdk/logcollect | com/efs/sdk/base/core/controller/ControllerCenter.java |
| https://errnewlog.umeng.com/api/crashsdk/logcollect | com/efs/sdk/base/core/f/c.java |
| https://android.bugly.qq.com/rqd/async | com/tencent/bugly/crashreport/common/strategy/StrategyBean.java |
| https://h.trace.qq.com/kv | com/tencent/bugly/proguard/ad.java |
| https://astat.bugly.qcloud.com/rqd/async | com/tencent/bugly/proguard/ac.java |
| https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async | com/tencent/bugly/proguard/ac.java |
| http://developer.umeng.com/docs/66650/cate/66650 | com/umeng/analytics/pro/j.java |
| https://plbslog.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://ulogs.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://alogus.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://developer.umeng.com/docs/66632/detail/ | com/umeng/commonsdk/debug/UMLogUtils.java |
| https://developer.umeng.com/docs/119267/detail/182050 | com/umeng/commonsdk/debug/UMLogCommon.java |
| https://pslog.umeng.com | com/umeng/commonsdk/vchannel/a.java |
| https://pslog.umeng.com/ | com/umeng/commonsdk/vchannel/a.java |
| https://offmsg.umeng.com/log/upload | com/umeng/message/common/UPLog.java |
| https://ccs.umeng.com/aa | com/umeng/message/proguard/m.java |
| https://sss.umeng.com/api/v2/al | com/umeng/message/proguard/m.java |
| https://offmsg.umeng.com/v2/offmsg/switch | com/umeng/message/proguard/ak.java |
| https://offmsg.umeng.com/v2/offmsg/req | com/umeng/message/proguard/t.java |
| https://msg.umengcloud.com/v3/tag/add | com/umeng/message/proguard/ar.java |
| https://msg.umengcloud.com/v3/tag/delete | com/umeng/message/proguard/ar.java |
| https://msg.umengcloud.com/v3/tag/get | com/umeng/message/proguard/ar.java |
| https://msg.umengcloud.com/admsg/v3/stats | com/umeng/message/proguard/ai.java |
| https://msg.umengcloud.com/admsg/v3/launch | com/umeng/message/proguard/ai.java |
| https://msg.umengcloud.com/admsg/v3/getmsg | com/umeng/message/proguard/ai.java |
| https://offmsg.umeng.com/log/switch | com/umeng/message/proguard/p.java |
| https://msg.umengcloud.com/v3/alias/set | com/umeng/message/proguard/z.java |
| https://msg.umengcloud.com/v3/alias/delete | com/umeng/message/proguard/z.java |
| https://msg.umengcloud.com/v3/alias | com/umeng/message/proguard/z.java |
| https://errnewlog.umeng.com | com/umeng/umcrash/UMCrashContent.java |
| https://errnewlogos.umeng.com | com/umeng/umcrash/UMCrashContent.java |
| https://developer.umeng.com/docs/193624/detail/194590 | com/umeng/umcrash/UMCrash.java |
| https://errnewlogos.umeng.com/upload | com/umeng/umcrash/UMCrash.java |
| https://errnewlogos.umeng.com | com/umeng/umcrash/UMCrash.java |
| https://errnewlog.umeng.com/upload | com/umeng/umcrash/UMCrash.java |
| https://errnewlog.umeng.com | com/umeng/umcrash/UMCrash.java |
| https://audid.umeng.com/v3/a/audid/req | com/umeng/ut/a/b/g.java |
| https://utoken.umeng.com | com/umeng/umzid/ZIDManager.java |
| https://errlogos.umeng.com | com/uc/crashsdk/a/d.java |
| https://errlog.umeng.com | com/uc/crashsdk/a/d.java |
| http://127.0.0.1 | org/mozilla/javascript/tools/debugger/Dim.java |
| http://javax.xml.XMLConstants/feature/secure-processing | org/mozilla/javascript/xmlimpl/XmlProcessor.java |
| http://apache.org/xml/features/disallow-doctype-decl | org/mozilla/javascript/xmlimpl/XmlProcessor.java |
| http://apache.org/xml/features/nonvalidating/load-external-dtd | org/mozilla/javascript/xmlimpl/XmlProcessor.java |
| http://javax.xml.XMLConstants/property/accessExternalDTD | org/mozilla/javascript/xmlimpl/XmlProcessor.java |
| http://javax.xml.XMLConstants/property/accessExternalStylesheet | org/mozilla/javascript/xmlimpl/XmlProcessor.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | p003O00ooO00oo/p004oOooOoOooO/O000oO000o.java |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0 | p003O00ooO00oo/p004oOooOoOooO/p009O0oo0O0oo0/O00ooO00oo.java |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling | p003O00ooO00oo/p004oOooOoOooO/p009O0oo0O0oo0/oOOoooOOoo.java |
| http://127.0.0.1: | p072oOOoooOOoo/p139O0o0oO0o0o/p141oOoOoOoO/O000oO000o.java |
| http://%s/api/app/v1/player\_upgrade?module=splayer | p072oOOoooOOoo/p139O0o0oO0o0o/p141oOoOoOoO/oOoOoOoO.java |
| http://%s/act?tag=plugin&ver=1 | p072oOOoooOOoo/p139O0o0oO0o0o/p141oOoOoOoO/oOoOoOoO.java |
| http://127.0.0.1: | p072oOOoooOOoo/p139O0o0oO0o0o/p141oOoOoOoO/O0Oo0O0Oo0.java |
| http://127.0.0.1 | p072oOOoooOOoo/p139O0o0oO0o0o/p141oOoOoOoO/p143O0o00O0o00/oOooOoOooO.java |
| https://www.baidu.com | p072oOOoooOOoo/p139O0o0oO0o0o/p144oOooOoOooO/p170OoOoOoOo/C1818o0OO0o0OO0.java |
| http://47.94.13.7 | p072oOOoooOOoo/p139O0o0oO0o0o/p144oOooOoOooO/p159OOo0OOo0/O00ooO00oo.java |
| http://123.57.155.33 | p072oOOoooOOoo/p139O0o0oO0o0o/p144oOooOoOooO/p159OOo0OOo0/O00ooO00oo.java |
| http://%s: | p072oOOoooOOoo/p139O0o0oO0o0o/p144oOooOoOooO/p165OoO0oOoO0o/oOOoooOOoo.java |
| https://developer.umeng.com/docs/147377/detail/209997\n\n | p072oOOoooOOoo/p107O0Oo0O0Oo0/p108oOooOoOooO/p109oOooOoOooO/p111O00ooO00oo/O00ooO00oo.java |
| http://www.walle-web.io/\n\n | p072oOOoooOOoo/p107O0Oo0O0Oo0/p108oOooOoOooO/p109oOooOoOooO/p111O00ooO00oo/O00ooO00oo.java |
| https://privacy.qq.com/document/preview/fc748b3d96224fdb825ea79e132c1a56\n\n | p072oOOoooOOoo/p107O0Oo0O0Oo0/p108oOooOoOooO/p109oOooOoOooO/p111O00ooO00oo/O00ooO00oo.java |
| http://ikukan.cn/advert\n\n\n | p072oOOoooOOoo/p107O0Oo0O0Oo0/p108oOooOoOooO/p109oOooOoOooO/p111O00ooO00oo/O00ooO00oo.java |
| http://yd.cdn.nextaifun.com/app/apk/ppcontent\_hdlive.txt | p072oOOoooOOoo/p107O0Oo0O0Oo0/p108oOooOoOooO/p109oOooOoOooO/p111O00ooO00oo/oOoOoOoO.java |
| https://www.live.com/cctv1.m3u8) | 摸瓜V1引擎 |
| http://poll.nextaifun.com | 摸瓜V3引擎 |
| https://msg.umengcloud.com/admsg/v3/getmsg | 摸瓜V3引擎 |
| programs.nextaifun.com | 摸瓜V3引擎 |
| cdn.nextaifun.com | 摸瓜V3引擎 |
| audid.umeng.com | 摸瓜V3引擎 |
| worldtimeapi.org | 摸瓜V3引擎 |
| https://developer.umeng.com/docs/193624/detail/194590#h2-n5n-d0l-fmj | 摸瓜V3引擎 |
| https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async | 摸瓜V3引擎 |
| as2.binstream.live | 摸瓜V3引擎 |
| tm2.binstream.live | 摸瓜V3引擎 |
| g3.letv.com | 摸瓜V3引擎 |
| http://4403-hs.otvstream.otvcloud.com/otv/skcc/review/channel%s/2300/%s/ | 摸瓜V3引擎 |
| https://errnewlog.umeng.com/upload | 摸瓜V3引擎 |
| https://www.ahtv.cn/ | 摸瓜V3引擎 |
| tm3.binstream.live | 摸瓜V3引擎 |
| https://msg.umengcloud.com/v3/tag/delete | 摸瓜V3引擎 |
| http://test.api.nextaifun.com | 摸瓜V3引擎 |
| dtrace.ysp.cctv.cn | 摸瓜V3引擎 |
| android.bugly.qq.com | 摸瓜V3引擎 |
| https://weblive.olympicchannelchina.cn/aoyun/%s\_%s.m3u8 | 摸瓜V3引擎 |
| https://offmsg.umeng.com/log/upload | 摸瓜V3引擎 |
| amdcopen.m.umeng.com | 摸瓜V3引擎 |
| https://offmsg.umeng.com/log/switch | 摸瓜V3引擎 |
| https://errnewlogos.umeng.com/upload | 摸瓜V3引擎 |
| https://errlog.umeng.com | 摸瓜V3引擎 |
| https://h.trace.qq.com/kv | 摸瓜V3引擎 |
| errnewlog.umeng.com | 摸瓜V3引擎 |
| https://www.olympicchannelchina.cn | 摸瓜V3引擎 |
| https://msg.umengcloud.com/v3/tag/add | 摸瓜V3引擎 |
| as4.binstream.live | 摸瓜V3引擎 |
| http://schemas.android.com/aapt | 摸瓜V3引擎 |
| http://javax.xml.XMLConstants/property/accessExternalStylesheet | 摸瓜V3引擎 |
| msg.umengcloud.com | 摸瓜V3引擎 |
| o18657i542.iask.in | 摸瓜V3引擎 |
| https://audid.umeng.com/v3/a/audid/req | 摸瓜V3引擎 |
| hls.nextaifun.com | 摸瓜V3引擎 |
| https://msg.umengcloud.com/v3/alias | 摸瓜V3引擎 |
| https://www.yangshipin.cn/#/tv/home?pid= | 摸瓜V3引擎 |
| http://live.cgtn.com/1000/prog\_index.m3u8 | 摸瓜V3引擎 |
| https://ccs.umeng.com/aa | 摸瓜V3引擎 |
| https://github.com/ReactiveX/RxJava/wiki/What | 摸瓜V3引擎 |
| https://kxmapp.mapi1.kxm.xmtv.cn/ | 摸瓜V3引擎 |
| http://47.94.13.7 | 摸瓜V3引擎 |
| https://developer.umeng.com/docs/119267/detail/182050 | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android$$layout/fragment\_maincontent\_audiov\_0 | 摸瓜V3引擎 |
| https://offmsg.umeng.com/v2/offmsg/req | 摸瓜V3引擎 |
| https://sss.umeng.com/api/v2/al | 摸瓜V3引擎 |
| https://msg.umengcloud.com/admsg/v3/launch | 摸瓜V3引擎 |
| http://gcc.gnu.org/bugs.html): | 摸瓜V3引擎 |
| as1.binstream.live | 摸瓜V3引擎 |
| http://live2.wisetv.com.cn/%s/%s/ | 摸瓜V3引擎 |
| http://154.19.70.157:5556/abcdddd123?chan= | 摸瓜V3引擎 |
| api.cdn.nextaifun.com | 摸瓜V3引擎 |
| https://developer.umeng.com/docs/66632/detail/ | 摸瓜V3引擎 |
| https://www.ahtv.cn | 摸瓜V3引擎 |
| https://cctvalih5ca.v.myalicdn.com/live/%s\_2/index.m3u8 | 摸瓜V3引擎 |
| http://123.57.155.33 | 摸瓜V3引擎 |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling | 摸瓜V3引擎 |
| http://player.hoge.cn/player.swf | 摸瓜V3引擎 |
| arm.zcj1.hiajfxo.cn | 摸瓜V3引擎 |
| https://cctvtxyh5ca.liveplay.myqcloud.com/live/%s\_2/index.m3u8 | 摸瓜V3引擎 |
| keep.nextaifun.com | 摸瓜V3引擎 |
| h5access.yangshipin.cn | 摸瓜V3引擎 |
| as3.binstream.live | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android | 摸瓜V3引擎 |
| live.miguvideo.com | 摸瓜V3引擎 |
| https://offmsg.umeng.com/v2/offmsg/switch | 摸瓜V3引擎 |
| https://astat.bugly.qcloud.com/rqd/async | 摸瓜V3引擎 |
| www.baidu.com | 摸瓜V3引擎 |
| http://127.0.0.1: | 摸瓜V3引擎 |
| https://errnewlogos.umeng.com | 摸瓜V3引擎 |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | 摸瓜V3引擎 |
| https://scgctvshow.sctv.com/hdlive/%s8f9fb5888dedbe0c6a1b/1- | 摸瓜V3引擎 |
| app.api.ulivetv.net | 摸瓜V3引擎 |
| http://vjpi.bdy.lnyun.com.cn | 摸瓜V3引擎 |
| player-api.yangshipin.cn | 摸瓜V3引擎 |
| http://live.fjtv.net/ | 摸瓜V3引擎 |
| ccs.umeng.com | 摸瓜V3引擎 |
| tm1.binstream.live | 摸瓜V3引擎 |
| https://errnewlog.umeng.com/api/crashsdk/logcollect | 摸瓜V3引擎 |
| sn.nextaifun.com | 摸瓜V3引擎 |
| umengacs.m.taobao.com | 摸瓜V3引擎 |
| https://msg.umengcloud.com/v3/alias/set | 摸瓜V3引擎 |
| www.a.shifen.com | 摸瓜V3引擎 |
| offmsg.umeng.com | 摸瓜V3引擎 |
| https://msg.umengcloud.com/v3/tag/get | 摸瓜V3引擎 |
| http://javax.xml.XMLConstants/property/accessExternalDTD | 摸瓜V3引擎 |
| http://iptv.deeptop.com.cn/api/iptv/getiptvlist?mac=%s&wifi\_mac=%s | 摸瓜V3引擎 |
| http://mozilla.org/MPL/2.0/. | 摸瓜V3引擎 |
| https://worldtimeapi.org/api/ip | 摸瓜V3引擎 |
| msgacs.m.umeng.com.gds.alibabadns.com | 摸瓜V3引擎 |
| cdn.nextaifun.com.w.kunlunaq.com | 摸瓜V3引擎 |
| https://errnewlogos.umeng.com/api/crashsdk/logcollect | 摸瓜V3引擎 |
| http://live3.hrtn.net/live/%s/%s\_ | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android##layout/fragment\_product\_dialog\_lx\_0 | 摸瓜V3引擎 |
| infoaibos.oss-cn-beijing.aliyuncs.com | 摸瓜V3引擎 |
| http://apache.org/xml/features/disallow-doctype-decl | 摸瓜V3引擎 |
| https://www.yangshipin.cn | 摸瓜V3引擎 |
| https://www.yangshipin.cn/ | 摸瓜V3引擎 |
| http://kiqk.bdy.lnyun.com.cn | 摸瓜V3引擎 |
| www.wshifen.com | 摸瓜V3引擎 |
| http://developer.umeng.com/docs/66650/cate/66650 | 摸瓜V3引擎 |
| https://errlogos.umeng.com | 摸瓜V3引擎 |
| https://m.lasatv.cn/ | 摸瓜V3引擎 |
| https://msg.umengcloud.com/admsg/v3/stats | 摸瓜V3引擎 |
| http://apache.org/xml/features/nonvalidating/load-external-dtd | 摸瓜V3引擎 |
| https://www.yangshipin.c | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res-auto | 摸瓜V3引擎 |
| ulogs.umeng.com | 摸瓜V3引擎 |
| play.miguvideo.com | 摸瓜V3引擎 |
| https://utoken.umeng.com | 摸瓜V3引擎 |
| http://javax.xml.XMLConstants/feature/secure-processing | 摸瓜V3引擎 |
| cdn.media.ulivetv.net | 摸瓜V3引擎 |
| http://42e83a32dc4e03efd8bbca6906228db9.h2.smtcdns.net/t-fjnetv51.live.bestvcdn.com.cn/live/program/ | 摸瓜V3引擎 |
| https://www.hljtv.com | 摸瓜V3引擎 |
| utoken.umeng.com | 摸瓜V3引擎 |
| tm4.binstream.live | 摸瓜V3引擎 |
| msgacs.m.umeng.com | 摸瓜V3引擎 |
| https://www.baidu.com | 摸瓜V3引擎 |
| https://msg.umengcloud.com/v3/alias/delete | 摸瓜V3引擎 |
| http://127.0.0.1 | 摸瓜V3引擎 |
| https://cctvcnch5ca.v.wscdns.com/live/%s\_2/index.m3u8 | 摸瓜V3引擎 |
| https://www.hljtv.com/ | 摸瓜V3引擎 |
| http://cdn.nextaifun.com/app/apk/desk\_silent.apk | 摸瓜V3引擎 |
| http://127.0.0.1:%s/%s?enc=base64&url=%s&mediatype=m3u8 | 摸瓜V3引擎 |
| https://errnewlog.umeng.com | 摸瓜V3引擎 |
| www.yangshipin.cn | 摸瓜V3引擎 |
| http://yd.cdn.nextaifun.com/app/apk/ppcontent\_hdlive.txt | 摸瓜V3引擎 |
| http://www.openssl.org/support/faq.html | lib/armeabi-v7a/libijkffmpeg.so |
| http://www.openssl.org/support/faq.html | lib/armeabi-v7a/libplayer.so |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| 问也可发送邮件至qingyuntv168@gmail.com联系我们  您可以发送邮件至qingyuntv168@gmail.com申请注销  qingyuntv168@gmail.com | p072oOOoooOOoo/p107O0Oo0O0Oo0/p108oOooOoOooO/p109oOooOoOooO/p111O00ooO00oo/O00ooO00oo.java |
| ffmpeg-devel@ffmpeg.org | lib/armeabi-v7a/libijkplayer.so |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869184 | tv/danmaku/ijk/media/player/IjkMediaMeta.java |

## **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=CN 签名算法: rsassa\_pkcs1v15 有效期自: 2024-06-05 10:36:41+00:00 有效期至: 2049-05-30 10:36:41+00:00 发行人: C=CN 序列号: 0x579fc4ff 哈希算法: sha256 md5值: 5be9f20ff358e0620c8b63481a9514bc sha1值: 68a0f950ce0c77cb7389d9e0161874ccb0c6225a sha256值: e5886822c17699b22f0a15d3752d0d0e71a98a6bdcbce78d95e0c04ecbb6a6f4 sha512值: 188d5e26e8e77e17647444140c059b41fef0e8737929915c273624131d08af8c217cc8fb271621e84b4a43b6994a4325968de9d3c1f741406e475961c4e160f4 公钥算法: rsa 密钥长度: 2048 指纹: 0a6c649cf2c95ec0db76da695a2688a122b7b00b25979f6d146534216efb71b0**

## **6. 硬编码敏感信息**

## **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.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.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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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.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.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.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.BLUETOOTH\_ADMIN | 正常 | 蓝牙管理 | 允许应用程序发现和配对蓝牙设备。 |
| 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 |
| 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 |
| android.permission.POST\_NOTIFICATIONS | 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。**