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

**电影猎手⁡​（ 3.1.0.9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 | 电影猎手⁡​ |
| 版本 | 3.1.0.9 |
| 包名 | lfnuwg.toucqx.jfmzei |
| 域名线索 | 66条 |
| URL线索 | 64条 |
| APP图标 |  |
| 分析日期 | 2025年10月11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 | DYLS-632.apk |
| 文件大小 | 58.77MB |
| MD5值 | 0c9ff1200a2ff78d8578f239d312de04 |
| SHA1值 | 27a12f0e6335f04aff5ff95aa66447818d9793f4 |
| SHA256值 | ff800a760b5368ceb2f0dfc9a20875372ad94ba22ce0300071c52556962d3e43 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 电影猎手⁡​ |
| 包名 | lfnuwg.toucqx.jfmzei |
| 主活动Activity | com.moviehunter.app.ui.SplashActivity2 |
| 安卓版本名称 | 3.1.0.9 |
| 安卓版本 | 3109 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| t1.szrtcpa.com | IP: 8.218.223.207  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| conf.hpplay.cn | IP: 1.14.243.140  所属国家: China  地区: Beijing  城市: Beijing |
| hpplay.cdn.cibn.cc | IP: 61.163.51.35  所属国家: China  地区: Henan  城市: Xinxiang |
| www.w3.org | IP: 104.18.23.19  所属国家: United States of America  地区: California  城市: San Francisco |
| a.weilai555.com | IP: 103.216.152.183  所属国家: China  地区: Jiangsu  城市: Yangzhou |
| log.umsns.com | IP: 59.82.31.92  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| wiki.eclipse.org | IP: 198.41.30.195  所属国家: Canada  地区: Ontario  城市: Brampton |
| purl.org | IP: 207.241.225.157  所属国家: United States of America  地区: California  城市: San Francisco |
| vipauth.hpplay.cn | IP: 124.95.190.104  所属国家: China  地区: Liaoning  城市: Shenyang |
| 107.148.47.94 | IP: 107.148.47.94  所属国家: United States of America  地区: California  城市: San Jose |
| at.umeng.com | IP: 59.82.29.163  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| www.eclipse.org | IP: 198.41.30.198  所属国家: Canada  地区: Ontario  城市: Brampton |
| pin.hpplay.cn | IP: 1.14.243.163  所属国家: China  地区: Beijing  城市: Beijing |
| 111.173.119.203 | IP: 111.173.119.203  所属国家: China  地区: Hubei  城市: Wuhan |
| www.sec.co.kr | IP: 112.106.187.200  所属国家: Korea (Republic of)  地区: Seoul-teukbyeolsi  城市: Seoul |
| www.umeng.com | IP: 59.82.29.248  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| devicemgr.hpplay.cn | IP: 1.14.243.171  所属国家: China  地区: Beijing  城市: Beijing |
| vipimdns.hpplay.cn | IP: 1.14.243.37  所属国家: China  地区: Beijing  城市: Beijing |
| vodreport.qcloud.com | IP: 115.56.90.192  所属国家: China  地区: Henan  城市: Jiaozuo |
| logu.hpplay.cn | IP: 47.106.59.179  所属国家: China  地区: Guangdong  城市: Shenzhen |
| t.me | IP: 149.154.167.99  所属国家: United Kingdom of Great Britain and Northern Ireland  地区: England  城市: Warrington |
| gslb.hpplay.cn | IP: 1.14.243.105  所属国家: China  地区: Beijing  城市: Beijing |
| xmlpull.org | IP: 185.199.111.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| stats.umsns.com | 没有服务器地理信息. |
| www.openssl.org | IP: 34.49.79.89  所属国家: United States of America  地区: California  城市: Mountain View |
| doh.360.cn | IP: 112.65.69.15  所属国家: China  地区: Shanghai  城市: Shanghai |
| netty.io | IP: 172.67.130.186  所属国家: United States of America  地区: California  城市: San Francisco |
| wq3wr3r.qiaozhixuexiao.com | IP: 23.225.136.82  所属国家: United States of America  地区: California  城市: Los Angeles |
| playvideo.qcloud.com | IP: 119.188.180.230  所属国家: China  地区: Shandong  城市: Jinan |
| uat.hpplay.cn | IP: 47.112.158.161  所属国家: China  地区: Guangdong  城市: Shenzhen |
| www.4thline.org | IP: 51.15.52.165  所属国家: Netherlands  地区: Noord-Holland  城市: Haarlem |
| sdk.frp.hpplay.com.cn | IP: 120.79.212.106  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| www.dbunit.org | IP: 74.220.199.51  所属国家: United States of America  地区: Utah  城市: Provo |
| 47.112.113.131 | IP: 47.112.113.131  所属国家: China  地区: Guangdong  城市: Shenzhen |
| sl.hpplay.cn | IP: 1.14.243.133  所属国家: China  地区: Beijing  城市: Beijing |
| test.hpplay.cn | IP: 122.152.230.114  所属国家: China  地区: Beijing  城市: Beijing |
| h5.hpplay.com.cn | IP: 222.161.53.222  所属国家: China  地区: Jilin  城市: Changchun |
| apptest.lscsfw.com | 没有服务器地理信息. |
| adisk-123.oss-cn-hangzhou.aliyuncs.com | IP: 101.67.62.1  所属国家: China  地区: Zhejiang  城市: Huzhou |
| adeng.hpplay.cn | IP: 1.14.243.52  所属国家: China  地区: Beijing  城市: Beijing |
| rps.hpplay.cn | IP: 175.22.9.231  所属国家: China  地区: Jilin  城市: Changchun |
| app-site.ecoliving168.com | IP: 125.39.113.1  所属国家: China  地区: Tianjin  城市: Tianjin |
| www.oracle.com | IP: 104.118.102.90  所属国家: Japan  地区: Osaka  城市: Osaka |
| android.asset | 没有服务器地理信息. |
| 192.168.8.230 | IP: 192.168.8.230  所属国家: -  地区: -  城市: - |
| vipgslb.hpplay.cn | IP: 1.14.243.65  所属国家: China  地区: Beijing  城市: Beijing |
| cdnauth2.hpplay.cn | IP: 218.60.172.242  所属国家: China  地区: Liaoning  城市: Dalian |
| 140.210.18.221 | IP: 140.210.18.221  所属国家: China  地区: Jiangsu  城市: Yangzhou |
| doh.pub | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| xml.apache.org | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| misdkauth.hpplay.cn | IP: 1.14.243.54  所属国家: China  地区: Beijing  城市: Beijing |
| run.json.qyfxgd.cn | 没有服务器地理信息. |
| cc3e497d.qdhgtch.com | IP: 104.233.167.194  所属国家: United States of America  地区: California  城市: San Jose |
| apache.org | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| schemas.xmlsoap.org | IP: 13.107.246.74  所属国家: United States of America  地区: Washington  城市: Redmond |
| cdnauth1.hpplay.cn | IP: 124.95.157.116  所属国家: China  地区: Liaoning  城市: Shenyang |
| 1255566655.vod2.myqcloud.com | IP: 221.204.15.52  所属国家: China  地区: Shanxi  城市: Taiyuan |
| points-mall.weilai555.com | IP: 103.216.152.183  所属国家: China  地区: Jiangsu  城市: Yangzhou |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| www.lebo.cn | IP: 125.39.113.1  所属国家: China  地区: Tianjin  城市: Tianjin |
| cloud.tencent.com | IP: 60.28.220.199  所属国家: China  地区: Tianjin  城市: Tianjin |
| dns.alidns.com | IP: 223.5.5.5  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| ssdkauth.hpplay.cn | IP: 1.14.243.123  所属国家: China  地区: Beijing  城市: Beijing |
| xml.org | IP: 104.239.240.11  所属国家: United States of America  地区: Texas  城市: Windcrest |
| vosdkauth.hpplay.cn | IP: 1.14.243.54  所属国家: China  地区: Beijing  城市: Beijing |
| ilivelog.qcloud.com | IP: 153.3.150.19  所属国家: China  地区: Jiangsu  城市: Nanjing |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://xml.apache.org/xslt | com/blankj/utilcode/util/LogUtils.java |
| https://github.com/danikula/AndroidVideoCache/issues/88. | com/danikula/videocache/HttpUrlSource.java |
| https://github.com/danikula/AndroidVideoCache/issues/43. | com/danikula/videocache/HttpUrlSource.java |
| https://github.com/danikula/AndroidVideoCache/issues. | com/danikula/videocache/HttpUrlSource.java |
| http://%s:%d/%s | com/danikula/videocache/Pinger.java |
| https://github.com/danikula/AndroidVideoCache/issues/134. | com/danikula/videocache/Pinger.java |
| http://%s:%d/%s | com/danikula/videocache/HttpProxyCacheServer.java |
| http://purl.org/dc/elements/1.1/\ | com/hpplay/component/protocol/ProtocolBuilder.java |
| http://www.sec.co.kr/\ | com/hpplay/component/protocol/ProtocolBuilder.java |
| https://www.lebo.cn/DTDs/PropertyList-1.0.dtd\ | com/hpplay/component/protocol/plist/NSObject.java |
| http://apache.org/xml/features/nonvalidating/load-external-dtd | com/hpplay/component/protocol/plist/XMLPropertyListParser.java |
| http://xml.org/sax/features/external-general-entities | com/hpplay/component/protocol/plist/XMLPropertyListParser.java |
| http://xml.org/sax/features/external-parameter-entities | com/hpplay/component/protocol/plist/XMLPropertyListParser.java |
| http://schemas.xmlsoap.org/soap/encoding/ | com/hpplay/cybergarage/soap/SOAP.java |
| http://schemas.xmlsoap.org/soap/envelope/ | com/hpplay/cybergarage/soap/SOAP.java |
| https://pin.hpplay.cn | com/hpplay/sdk/source/x.java |
| https://rps.hpplay.cn | com/hpplay/sdk/source/x.java |
| http://sl.hpplay.cn | com/hpplay/sdk/source/x.java |
| http://sdk.frp.hpplay.com.cn/user-device-link | com/hpplay/sdk/source/x.java |
| https://vipauth.hpplay.cn | com/hpplay/sdk/source/x.java |
| https://uat.hpplay.cn:90/Author/PhoneAuthor/? | com/hpplay/sdk/source/x.java |
| https://uat.hpplay.cn:1001/Author/PhoneAuthor/? | com/hpplay/sdk/source/x.java |
| https://uat.hpplay.cn:1002/Author/PhoneAuthor/? | com/hpplay/sdk/source/x.java |
| http://47.112.113.131:90/Author/PhoneAuthor/? | com/hpplay/sdk/source/x.java |
| https://misdkauth.hpplay.cn/Author/PhoneAuthor/? | com/hpplay/sdk/source/x.java |
| https://vosdkauth.hpplay.cn/Author/PhoneAuthor/? | com/hpplay/sdk/source/x.java |
| https://ssdkauth.hpplay.cn/Author/PhoneAuthor/? | com/hpplay/sdk/source/x.java |
| https://cdnauth1.hpplay.cn/Author/PhoneAuthor/? | com/hpplay/sdk/source/x.java |
| https://cdnauth2.hpplay.cn/Author/PhoneAuthor/? | com/hpplay/sdk/source/x.java |
| http://hpplay.cdn.cibn.cc/release/out/weixin.html | com/hpplay/sdk/source/x.java |
| https://adeng.hpplay.cn | com/hpplay/sdk/source/x.java |
| http://192.168.8.230:8000 | com/hpplay/sdk/source/x.java |
| https://conf.hpplay.cn:90 | com/hpplay/sdk/source/x.java |
| https://devicemgr.hpplay.cn | com/hpplay/sdk/source/x.java |
| https://vipgslb.hpplay.cn | com/hpplay/sdk/source/x.java |
| https://vipimdns.hpplay.cn | com/hpplay/sdk/source/x.java |
| https://logu.hpplay.cn:8856 | com/hpplay/sdk/source/x.java |
| http://test.hpplay.cn:8855 | com/hpplay/sdk/source/x.java |
| https://logu.hpplay.cn:8868 | com/hpplay/sdk/source/x.java |
| http://test.hpplay.cn:8865 | com/hpplay/sdk/source/x.java |
| https://h5.hpplay.com.cn/webapps/h5/help/ | com/hpplay/sdk/source/browser/b/a.java |
| https://uat.hpplay.cn:90/Author/PhoneAuthor/? | com/hpplay/sdk/source/business/cloud/CloudAPI.java |
| https://uat.hpplay.cn:1001/Author/PhoneAuthor/? | com/hpplay/sdk/source/business/cloud/CloudAPI.java |
| https://uat.hpplay.cn:1002/Author/PhoneAuthor/? | com/hpplay/sdk/source/business/cloud/CloudAPI.java |
| http://47.112.113.131:90/Author/PhoneAuthor/? | com/hpplay/sdk/source/business/cloud/CloudAPI.java |
| https://misdkauth.hpplay.cn/Author/PhoneAuthor/? | com/hpplay/sdk/source/business/cloud/CloudAPI.java |
| https://vosdkauth.hpplay.cn/Author/PhoneAuthor/? | com/hpplay/sdk/source/business/cloud/CloudAPI.java |
| https://ssdkauth.hpplay.cn/Author/PhoneAuthor/? | com/hpplay/sdk/source/business/cloud/CloudAPI.java |
| https://cdnauth1.hpplay.cn/Author/PhoneAuthor/? | com/hpplay/sdk/source/business/cloud/CloudAPI.java |
| https://cdnauth2.hpplay.cn/Author/PhoneAuthor/? | com/hpplay/sdk/source/business/cloud/CloudAPI.java |
| http://hpplay.cdn.cibn.cc/release/out/weixin.html | com/hpplay/sdk/source/business/cloud/CloudAPI.java |
| https://pin.hpplay.cn | com/hpplay/sdk/source/business/cloud/CloudAPI.java |
| http://gslb.hpplay.cn | com/hpplay/sdk/source/business/cloud/CloudAPI.java |
| https://adeng.hpplay.cn | com/hpplay/sdk/source/business/cloud/CloudAPI.java |
| http://%s:%s/www.hpplay.com.cn/tv/app/DnsTxtInfo | com/hpplay/sdk/source/business/cloud/CloudAPI.java |
| https://misdkauth.hpplay.cn/Author/PhoneAuthor/? | com/hpplay/sdk/source/business/cloud/AuthSDK.java |
| https://vosdkauth.hpplay.cn/Author/PhoneAuthor/? | com/hpplay/sdk/source/business/cloud/AuthSDK.java |
| https://uat.hpplay.cn:90/Author/PhoneAuthor/? | com/hpplay/sdk/source/business/cloud/AuthSDK.java |
| https://uat.hpplay.cn:1001/Author/PhoneAuthor/? | com/hpplay/sdk/source/business/cloud/AuthSDK.java |
| https://uat.hpplay.cn:1002/Author/PhoneAuthor/? | com/hpplay/sdk/source/business/cloud/AuthSDK.java |
| https://ssdkauth.hpplay.cn/Author/PhoneAuthor/? | com/hpplay/sdk/source/business/cloud/AuthSDK.java |
| https://cdnauth1.hpplay.cn/Author/PhoneAuthor/? | com/hpplay/sdk/source/business/cloud/AuthSDK.java |
| https://cdnauth2.hpplay.cn/Author/PhoneAuthor/? | com/hpplay/sdk/source/business/cloud/AuthSDK.java |
| http://hpplay.cdn.cibn.cc/release/out/weixin.html? | com/hpplay/sdk/source/device/qr/QRCodeController.java |
| http://xml.apache.org/xslt | com/jsj/library/util/CharacterHandler.java |
| https://111.173.119.203:45443/chat/mobile?noCanClose=1&token=67aa98823a51c1f53818982058417121&uid= | com/moviehunter/app/ui/integralgoods/IntegralGoodsWebViewActivity$setListener$2.java |
| https://111.173.119.203:45443/chat/mobile?noCanClose=1&token=67aa98823a51c1f53818982058417121&uid= | com/moviehunter/app/ui/mine/MineFragment2.java |
| https://t1.szrtcpa.com/2023/02/06/cbc39b5f9c4f8.jpg | com/moviehunter/app/ui/theme/ThemeDetailActivity.java |
| https://cc3e497d.qdhgtch.com:2345/api/ | com/moviehunter/app/network/BaseUrlAndHeaderInterceptor.java |
| http://107.148.47.94:8787/ | com/moviehunter/app/network/BaseUrlAndHeaderInterceptor.java |
| https://dns.alidns.com/dns-query | com/moviehunter/app/utils/MultiDnsOverHttpsWithCache.java |
| https://doh.pub/dns-query | com/moviehunter/app/utils/MultiDnsOverHttpsWithCache.java |
| https://doh.360.cn/dns-query | com/moviehunter/app/utils/MultiDnsOverHttpsWithCache.java |
| https://apptest.lscsfw.com:2345/uk.php?type=qq | com/moviehunter/app/utils/config/ConstantKt.java |
| https://t.me/+fHuxCUYgtCZjYzU1 | com/moviehunter/app/utils/config/ConstantKt.java |
| https://wq3wr3r.qiaozhixuexiao.com | com/moviehunter/app/utils/config/ConstantKt.java |
| https://apptest.lscsfw.com:2345/uk.php?type=weibo | com/moviehunter/app/utils/config/ConstantKt.java |
| https://apptest.lscsfw.com:2345/uk.php?type=wx | com/moviehunter/app/utils/config/ConstantKt.java |
| https://app-site.ecoliving168.com/domain\_v5.json | com/moviehunter/app/utils/config/ConstantKt.java |
| https://a.weilai555.com:9800/domain\_v5.json | com/moviehunter/app/utils/config/ConstantKt.java |
| https://adisk-123.oss-cn-hangzhou.aliyuncs.com/domain\_v5.json | com/moviehunter/app/utils/config/ConstantKt.java |
| https://run.json.qyfxgd.cn:9312/captcha\_black.html | com/moviehunter/app/utils/config/ConstantKt.java |
| http://140.210.18.221:9319/ | com/moviehunter/app/utils/config/ConstantKt.java |
| https://points-mall.weilai555.com:1008/ | com/moviehunter/app/utils/config/ConstantKt.java |
| https://points-mall.weilai555.com:1008/game | com/moviehunter/app/utils/config/ConstantKt.java |
| https://wq3wr3r.qiaozhixuexiao.com/chat/index?noCanClose=1&token=c5f6b16c0a60510cb828fe875e7d40b0&uid= | com/moviehunter/app/utils/config/ConstantKt.java |
| https://cc3e497d.qdhgtch.com/debug\_v5.json | com/moviehunter/app/utils/config/ConstantKt.java |
| https://cloud.tencent.com/act/event/License | com/tencent/liteav/a.java |
| https://cloud.tencent.com/document/product/454/18872 | com/tencent/liteav/demo/superplayer/SuperPlayerView.java |
| https://ilivelog.qcloud.com | com/tencent/liteav/demo/superplayer/model/net/LogReport.java |
| https://playvideo.qcloud.com/getplayinfo/v2 | com/tencent/liteav/demo/superplayer/model/protocol/PlayInfoProtocolV2.java |
| https://playvideo.qcloud.com/getplayinfo/v4 | com/tencent/liteav/demo/superplayer/model/protocol/PlayInfoProtocolV4.java |
| http://playvideo.qcloud.com/getplayinfo/v2 | com/tencent/liteav/txcvodplayer/b/d.java |
| https://playvideo.qcloud.com/getplayinfo/v2 | com/tencent/liteav/txcvodplayer/b/d.java |
| http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff14564972818519602447/coverBySnapshot/1513156403\_1311093072.100\_0.jpg?t=5c08d9fa&us=someus&sign=95f34beb353fe32cfe7f8b5e79cc28b1\ | com/tencent/liteav/txcvodplayer/b/d.java |
| http://1255566655.vod2.myqcloud.com/ca754badvodgzp1255566655/8f5fbff14564972818519602447/imageSprite/1513156058\_533711271\_00001.jpg?t=5c08d9fa&us=someus&sign=79449db4e1fb05a3becfa096613659c3\ | com/tencent/liteav/txcvodplayer/b/d.java |
| http://1255566655.vod2.myqcloud.com/ca754badvodgzp1255566655/8f5fbff14564972818519602447/imageSprite/1513156058\_533711271.vtt?t=5c08d9fa&us=someus&sign=79449db4e1fb05a3becfa096613659c3\ | com/tencent/liteav/txcvodplayer/b/d.java |
| http://1255566655.vod2.myqcloud.com/ca754badvodgzp1255566655/8f5fbff14564972818519602447/uAnXX0OMLSAA.wmv?t=5c08d9fa&us=someus&sign=659af5dd3f27eb92dc4ed74eb561daa4\ | com/tencent/liteav/txcvodplayer/b/d.java |
| http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff14564972818519602447/master\_playlist.m3u8?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d\ | com/tencent/liteav/txcvodplayer/b/d.java |
| http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff14564972818519602447/v.f220.m3u8?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d\ | com/tencent/liteav/txcvodplayer/b/d.java |
| http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff14564972818519602447/v.f230.m3u8?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d\ | com/tencent/liteav/txcvodplayer/b/d.java |
| http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff14564972818519602447/v.f240.m3u8?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d\ | com/tencent/liteav/txcvodplayer/b/d.java |
| http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff14564972818519602447/v.f210.m3u8?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d\ | com/tencent/liteav/txcvodplayer/b/d.java |
| http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff14564972818519602447/v.f10.mp4?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d\ | com/tencent/liteav/txcvodplayer/b/d.java |
| http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff14564972818519602447/v.f20.mp4?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d\ | com/tencent/liteav/txcvodplayer/b/d.java |
| https://playvideo.qcloud.com/getplayinfo/v4 | com/tencent/liteav/txcvodplayer/b/c.java |
| https://vodreport.qcloud.com/describeControlInfos/v1/ | com/tencent/liteav/txcvodplayer/a/b.java |
| http://log.umsns.com/link/qq/download/ | com/umeng/socialize/common/SocializeConstants.java |
| http://log.umsns.com/link/weixin/download/ | com/umeng/socialize/common/SocializeConstants.java |
| http://www.umeng.com/social | com/umeng/socialize/common/SocializeConstants.java |
| https://stats.umsns.com/ | com/umeng/socialize/net/stats/StatsRequest.java |
| https://log.umsns.com/ | com/umeng/socialize/net/base/SocializeRequest.java |
| https://at.umeng.com/bObWzC?cid=476 | com/umeng/socialize/net/base/SocializeRequest.java |
| https://at.umeng.com/ya4Dmy?cid=476 | com/umeng/socialize/net/base/SocializeRequest.java |
| https://at.umeng.com/0fqeCy?cid=476 | com/umeng/socialize/utils/UrlUtil.java |
| https://at.umeng.com/CuKXbi?cid=476 | com/umeng/socialize/utils/UrlUtil.java |
| https://at.umeng.com/1HTzyC?cid=476 | com/umeng/socialize/utils/UrlUtil.java |
| https://at.umeng.com/i8Dy8n?cid=476 | com/umeng/socialize/utils/UrlUtil.java |
| https://at.umeng.com/ya4Dmy?cid=476 | com/umeng/socialize/utils/UrlUtil.java |
| https://at.umeng.com/aOzmWf?cid=476 | com/umeng/socialize/utils/UrlUtil.java |
| https://at.umeng.com/5P9baC?cid=476 | com/umeng/socialize/utils/UrlUtil.java |
| https://at.umeng.com/ve4Pbm?cid=476 | com/umeng/socialize/utils/UrlUtil.java |
| https://at.umeng.com/bObWzC?cid=476 | com/umeng/socialize/utils/UrlUtil.java |
| https://at.umeng.com/8Tfmei?cid=476 | com/umeng/socialize/utils/UrlUtil.java |
| https://at.umeng.com/9T595j?cid=476 | com/umeng/socialize/utils/UrlUtil.java |
| https://at.umeng.com/CCiOHv?cid=476 | com/umeng/socialize/utils/UrlUtil.java |
| https://at.umeng.com/KzKfWz?cid=476 | com/umeng/socialize/utils/UrlUtil.java |
| https://at.umeng.com/LXzm8D?cid=476 | com/umeng/socialize/utils/UrlUtil.java |
| https://at.umeng.com/Pn0TTr?cid=476 | com/umeng/socialize/utils/UrlUtil.java |
| https://at.umeng.com/KD4zOf?cid=476 | com/umeng/socialize/utils/UrlUtil.java |
| https://at.umeng.com/OTnqea?cid=476 | com/umeng/socialize/utils/UrlUtil.java |
| https://at.umeng.com/jiia8D?cid=476 | com/umeng/socialize/utils/UrlUtil.java |
| https://at.umeng.com/WT95za?cid=476 | com/umeng/socialize/utils/UrlUtil.java |
| https://at.umeng.com/iWvmGD?cid=476 | com/umeng/socialize/utils/UrlUtil.java |
| https://at.umeng.com/19HTvC?cid=476 | com/umeng/socialize/utils/UrlUtil.java |
| https://at.umeng.com/iqmK1D?cid=476 | com/umeng/socialize/utils/UrlUtil.java |
| https://at.umeng.com/CC0LLz?cid=476 | com/umeng/socialize/utils/UrlUtil.java |
| https://at.umeng.com/9XX5ry?cid=476 | com/umeng/socialize/utils/UrlUtil.java |
| https://at.umeng.com/4v4XPn?cid=476 | com/umeng/socialize/utils/UrlUtil.java |
| https://at.umeng.com/GPruqi?cid=476 | com/umeng/socialize/utils/UrlUtil.java |
| https://at.umeng.com/9XXbCm?cid=476 | com/umeng/socialize/utils/UrlUtil.java |
| https://at.umeng.com/KHDGXb?cid=476 | com/umeng/socialize/utils/UrlUtil.java |
| https://at.umeng.com/HL1T9j?cid=476 | com/umeng/socialize/utils/UrlUtil.java |
| https://at.umeng.com/iiuOHz?cid=476 | com/umeng/socialize/utils/UrlUtil.java |
| https://at.umeng.com/SLDG5z?cid=476 | com/umeng/socialize/utils/UrlUtil.java |
| https://at.umeng.com/f8HHDi?cid=476 | com/umeng/socialize/utils/UrlUtil.java |
| https://at.umeng.com/H5vGLj?cid=476 | com/umeng/socialize/utils/UrlUtil.java |
| https://at.umeng.com/uOjyCu?cid=476 | com/umeng/socialize/utils/UrlUtil.java |
| https://at.umeng.com/9D49bu?cid=476 | com/umeng/socialize/utils/UrlUtil.java |
| https://at.umeng.com/KfWLzu?cid=476 | com/umeng/socialize/utils/UrlUtil.java |
| https://log.umsns.com/ | com/umeng/socialize/view/OauthDialog.java |
| https://wiki.eclipse.org/Jetty/Feature/NPN | io/netty/handler/ssl/JdkNpnApplicationProtocolNegotiator.java |
| http://netty.io/wiki/forked-tomcat-native.html | io/netty/handler/ssl/OpenSsl.java |
| https://www.openssl.org/docs/man1.0.2/apps/verify.html. | io/netty/handler/ssl/OpenSslCertificateException.java |
| http://netty.io/wiki/sslcontextbuilder-and-private-key.html | io/netty/handler/ssl/PemReader.java |
| http://www.eclipse.org/jetty/documentation/current/alpn-chapter.html | io/netty/handler/ssl/JdkAlpnApplicationProtocolNegotiator.java |
| http://netty.io/wiki/reference-counted-objects.html | io/netty/util/ResourceLeakDetector.java |
| https://android.asset/ | io/noties/markwon/image/destination/ImageDestinationProcessorAssets.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/Completable.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/Maybe.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/Single.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/Observable.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/Flowable.java |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling | io/reactivex/rxjava3/exceptions/OnErrorNotImplementedException.java |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0 | io/reactivex/rxjava3/exceptions/UndeliverableException.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/rxjava3/core/Completable.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/rxjava3/core/Single.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/rxjava3/core/Maybe.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/rxjava3/core/Observable.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/rxjava3/core/Flowable.java |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling | io/reactivex/exceptions/OnErrorNotImplementedException.java |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0 | io/reactivex/exceptions/UndeliverableException.java |
| http://purl.org/dc/elements/1.1/ | org/fourthline/cling/support/model/DIDLObject.java |
| http://www.sec.co.kr/ | org/fourthline/cling/support/model/DIDLObject.java |
| http://www.4thline.org/projects/mailinglists-cling.html\n\n | org/fourthline/cling/support/shared/Main.java |
| http://schemas.xmlsoap.org/soap/envelope/ | org/fourthline/cling/model/Constants.java |
| http://schemas.xmlsoap.org/soap/encoding/ | org/fourthline/cling/model/Constants.java |
| http://www.sec.co.kr/dlna | org/fourthline/cling/binding/xml/Descriptor.java |
| http://schemas.xmlsoap.org/soap/envelope/ | org/fourthline/cling/transport/impl/SOAPActionProcessorImpl.java |
| http://schemas.xmlsoap.org/soap/encoding/ | org/fourthline/cling/transport/impl/SOAPActionProcessorImpl.java |
| http://[ | org/seamless/util/URIUtil.java |
| http://www.dbunit.org/properties/datatypeFactory | org/seamless/util/dbunit/H2DBUnitOperations.java |
| http://xmlpull.org/v1/doc/features.html | org/seamless/xml/XmlPullParserUtils.java |
| http://apache.org/xml/features/xinclude/fixup-base-uris | org/seamless/xml/DOMParser.java |
| http://apache.org/xml/features/xinclude/fixup-language | org/seamless/xml/DOMParser.java |
| http://apache.org/xml/features/validation/dynamic | org/seamless/xml/DOMParser.java |
| http://www.oracle.com/xml/is-standalone | org/seamless/xml/DOMParser.java |
| http://xml.apache.org/xslt | org/seamless/xml/DOMParser.java |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| danikula@gmail.com | com/danikula/videocache/HttpUrlSource.java |
| this@movieactivity.window | com/moviehunter/app/ui/MovieActivity.java |
| xxx@email.elided | com/tencent/liteav/base/PiiElider.java |

### **4.4 手机号线索**

## **5. 签名证书**

**APK已签名 v1 签名: False v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: C=cnlxxsqtnzvwl, ST=bncyrgklnqoib, L=wnjphvubnwrlr, O=bdw1734835929522, OU=zol1734835929522, CN=TG@apkfangdujiagu 签名算法: rsassa\_pkcs1v15 有效期自: 2024-12-22 02:52:09+00:00 有效期至: 2074-12-10 02:52:09+00:00 发行人: C=cnlxxsqtnzvwl, ST=bncyrgklnqoib, L=wnjphvubnwrlr, O=bdw1734835929522, OU=zol1734835929522, CN=TG@apkfangdujiagu 序列号: 0x44bb172d 哈希算法: sha1 md5值: 47b47a0479fba9491433aa82f9981f96 sha1值: c041be767297cb9afb905956816e200290d6f35e sha256值: 4df5cadbfa54697cf65425800469ff259a4a74d69fa2ae9348e710957301ca18 sha512值: e3517d5de626d79448c1838f67c7387236c4ea4b739bd9e7916029a759647ca3970d20ef4a52189cb31c2023288f0d054b6eda494d2d3945ae5a2823d18b4f3c 公钥算法: rsa 密钥长度: 1024 指纹: 1ce408cb691030dc8dcb995460d3463434d4d38d12995a59af0c768f124248eb**

## **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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.NEARBY\_WIFI\_DEVICES | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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.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.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.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.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.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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.FOREGROUND\_SERVICE\_LOCATION | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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.MANAGE\_EXTERNAL\_STORAGE | 危险 | 允许应用程序广泛访问范围存储中的外部存储 | 允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用 |
| 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.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FOREGROUND\_SERVICE\_MEDIA\_PLAYBACK | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FOREGROUND\_SERVICE\_DATA\_SYNC | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_IMAGES | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_AUDIO | 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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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 |
| android.permission.WRITE\_SETTINGS | 危险 | 修改全局系统设置 | 允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。 |
| android.permission.READ\_MEDIA\_VISUAL\_USER\_SELECTED | 未知 | Unknown permission | Unknown permission from android reference |
| lfnuwg.toucqx.jfmzei.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.USE\_FINGERPRINT | 正常 | allow use of指纹 | 该常量在 API 级别 28 中已被弃用。应用程序应改为请求 USE\_BIOMETRIC |
| android.permission.USE\_BIOMETRIC | 正常 |  | 允许应用使用设备支持的生物识别模式。 |
| lfnuwg.toucqx.jfmzei\_com.google.android.providers.gsf.permission.READ\_GSERVICES | 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。 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.moviehunter.app.ui.mine.AccountConnectActivity | **Schemes**: dylsapp://,  **Hosts:** bind, |
| com.moviehunter.app.ui.newlogin.SocialBindActivity | **Schemes**: dylsapp://,  **Hosts:** login, |

**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。**