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

**Spermatid（ 4.8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 | Spermatid |
| 版本 | 4.8 |
| 包名 | com.sjm.dtsecond.amh |
| 域名线索 | 71条 |
| URL线索 | 87条 |
| APP图标 |  |
| 分析日期 | 2025年5月10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 | Spermatid v4.8.apk |
| 文件大小 | 20.7MB |
| MD5值 | d730232baeb7bfe3e7d60cbe551b8332 |
| SHA1值 | 47249b58f15cb176c4116b1d4151ad6179d980a6 |
| SHA256值 | cfef524713e39a0b968d0545235a3436ba112a39ea655d3ba891b447088a01c5 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | Spermatid |
| 包名 | com.sjm.dtsecond.amh |
| 主活动Activity | com.sjm.dtsecond.amh.SplashActivity |
| 安卓版本名称 | 4.8 |
| 安卓版本 | 480 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| ads.oneway.mobi | IP: 118.178.152.152  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| changemaker.hzsanjiaomao.com | IP: 82.157.26.175  所属国家: China  地区: Beijing  城市: Beijing |
| whatwg.org | IP: 165.227.248.76  所属国家: United States of America  地区: New Jersey  城市: Clifton |
| 119.29.29.29 | IP: 119.29.29.29  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| httpbin.org | IP: 54.204.94.184  所属国家: United States of America  地区: Virginia  城市: Ashburn |
| dapi.sjmbdl.cn | 没有服务器地理信息. |
| tl.oneway.mobi | IP: 47.98.30.91  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| schemas.microsoft.com | IP: 13.107.246.74  所属国家: Netherlands  地区: Noord-Holland  城市: Amsterdam |
| i.snssdk.com | IP: 124.238.242.122  所属国家: China  地区: Hebei  城市: Langfang |
| java.oracle.com | IP: 23.223.211.24  所属国家: France  地区: Ile-de-France  城市: Aubervilliers |
| dc.sigmob.cn | IP: 112.126.7.24  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| xml.org | IP: 104.239.240.11  所属国家: United States of America  地区: Texas  城市: Windcrest |
| net.rayjump.com | IP: 39.107.225.241  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| test.api.yky.qq.com | IP: 183.47.102.215  所属国家: China  地区: Guangdong  城市: Huizhou |
| 118.178.152.152 | IP: 118.178.152.152  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| bugreport.java.com | IP: 23.59.209.203  所属国家: United States of America  地区: New York  城市: New York City |
| tl.oway.mobi | IP: 118.178.152.152  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| checkerframework.org | IP: 128.208.3.120  所属国家: United States of America  地区: Washington  城市: Seattle |
| jsoup.org | IP: 104.21.7.68  所属国家: United States of America  地区: California  城市: San Francisco |
| analytics.rayjump.com | IP: 182.92.120.219  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| github.com | IP: 20.205.243.166  所属国家: United States of America  地区: Washington  城市: Redmond |
| sdk.hzsanjiaomao.com | IP: 220.181.125.250  所属国家: China  地区: Beijing  城市: Beijing |
| m.sigmob.com | IP: 39.106.48.234  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| apps.oceanengine.com | IP: 111.225.210.139  所属国家: China  地区: Hebei  城市: Langfang |
| webcast-open.douyin.com | IP: 27.128.221.36  所属国家: China  地区: Hebei  城市: Langfang |
| javax.xml.transform.sax.saxsource | 没有服务器地理信息. |
| static.yky.qq.com | IP: 61.54.7.111  所属国家: China  地区: Henan  城市: Anyang |
| adservice.sigmob.cn | IP: 47.94.254.145  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| ads.oway.mobi | IP: 47.98.30.91  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| xml.apache.org | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| cloud.tgpa.qq.com | IP: 101.89.41.145  所属国家: China  地区: Shanghai  城市: Shanghai |
| apps.samsung.com | IP: 103.254.189.58  所属国家: China  地区: Beijing  城市: Beijing |
| api.hzsanjiaomao.com | IP: 121.199.61.218  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| owads.audioadx.com | IP: 8.136.116.120  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| v.behe.com | 没有服务器地理信息. |
| passport.kuaishou.com | IP: 103.102.200.8  所属国家: China  地区: Beijing  城市: Beijing |
| api.ipify.org | IP: 104.237.62.211  所属国家: United States of America  地区: Utah  城市: Ogden |
| api.yky.qq.com | IP: 109.244.172.228  所属国家: China  地区: Beijing  城市: Beijing |
| owtk.audioadx.com | IP: 8.136.116.120  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| test.com | 没有服务器地理信息. |
| open.e.kuaishou.com | IP: 103.102.200.30  所属国家: China  地区: Beijing  城市: Beijing |
| www.samsungapps.com | IP: 52.18.136.34  所属国家: Ireland  地区: Dublin  城市: Dublin |
| hybird.rayjump.com | IP: 42.81.147.71  所属国家: China  地区: Tianjin  城市: Tianjin |
| webcast.amemv.com | IP: 220.181.127.237  所属国家: China  地区: Beijing  城市: Beijing |
| htmlpreview.github.io | IP: 185.199.108.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| track.oway.mobi | IP: 47.98.30.91  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| policy.rayjump.com | IP: 59.110.124.183  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| play.google.com | IP: 142.251.42.238  所属国家: United States of America  地区: California  城市: Mountain View |
| www.w3.org | IP: 104.18.23.19  所属国家: United States of America  地区: California  城市: San Francisco |
| www.google.com | IP: 96.44.137.28  所属国家: United States of America  地区: California  城市: Los Angeles |
| configure.rayjump.com | IP: 59.110.124.183  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| lazy.rayjump.com | IP: 59.110.124.183  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| d1tru86qrby720.cloudfront.net | IP: 99.86.195.163  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| check.rayjump.com | IP: 59.110.124.183  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| 211.151.146.65 | IP: 211.151.146.65  所属国家: China  地区: Beijing  城市: Beijing |
| javax.xml.transform.sax.saxresult | 没有服务器地理信息. |
| static.yximgs.com | IP: 221.204.165.242  所属国家: China  地区: Shanxi  城市: Taiyuan |
| crbug.com | IP: 216.239.32.29  所属国家: United States of America  地区: California  城市: Mountain View |
| sf6-ttcdn-tos.pstatp.com | IP: 61.147.216.109  所属国家: China  地区: Jiangsu  城市: Nantong |
| detect.rayjump.com | IP: 52.44.33.71  所属国家: United States of America  地区: Virginia  城市: Ashburn |
| apache.org | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| js-ad.a.yximgs.com | IP: 1.71.163.1  所属国家: China  地区: Shanxi  城市: Taiyuan |
| testcloud.tgpa.qq.com | IP: 101.91.22.88  所属国家: China  地区: Shanghai  城市: Shanghai |
| d.alipay.com | IP: 203.209.245.74  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| bugs.java.com | IP: 23.59.209.203  所属国家: United States of America  地区: New York  城市: New York City |
| cdn-adn-https.rayjump.com | IP: 42.81.147.71  所属国家: China  地区: Tianjin  城市: Tianjin |
| gist.github.com | IP: 37.61.54.158  所属国家: Azerbaijan  地区: Baki  城市: Baku |
| api.htp.ad-scope.com.cn | IP: 47.94.43.167  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| cpro.baidustatic.com | IP: 101.72.203.35  所属国家: China  地区: Hebei  城市: Tangshan |
| union.baidu.com | IP: 220.181.111.40  所属国家: China  地区: Beijing  城市: Beijing |
| android.asset | 没有服务器地理信息. |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://' | org/jsoup/helper/HttpConnection.java |
| https://'. | org/jsoup/helper/HttpConnection.java |
| https://jsoup.org/cookbook/extracting-data/working-with-urls | org/jsoup/helper/HttpConnection.java |
| http://undefined/ | org/jsoup/helper/HttpConnection.java |
| http://javax.xml.transform.sax.SAXSource/feature | org/checkerframework/org/objectweb/asmx/xml/Processor.java |
| http://javax.xml.transform.sax.SAXResult/feature | org/checkerframework/org/objectweb/asmx/xml/Processor.java |
| https://github.com/javaparser/javaparser/issues | org/checkerframework/com/github/javaparser/GeneratedJavaParserBase.java |
| http://java.oracle.com/ | org/checkerframework/com/github/javaparser/JavaParserBuild.java |
| https://github.com/L-JINBIN/ApkSignatureKillerEx | bin/mt/signature/KillerApplication.java |
| https://github.com/typetools/annotation-tools/issues | scenelib/annotations/io/classfile/ClassFileReader.java |
| https://github.com/typetools/annotation-tools/issues | scenelib/annotations/io/classfile/ClassFileWriter.java |
| https://checkerframework.org/annotation-file-utilities/)\nusage: | scenelib/annotations/tools/Anncat.java |
| http://xml.apache.org/xslt | cn/hutool/core/util/XmlUtil.java |
| http://apache.org/xml/features/disallow-doctype-decl | cn/hutool/core/util/XmlUtil.java |
| http://xml.org/sax/features/external-general-entities | cn/hutool/core/util/XmlUtil.java |
| http://xml.org/sax/features/external-parameter-entities | cn/hutool/core/util/XmlUtil.java |
| http://apache.org/xml/features/nonvalidating/load-external-dtd | cn/hutool/core/util/XmlUtil.java |
| http://www.w3.org/2000/xmlns/ | cn/hutool/core/util/XmlUtil.java |
| http://android.asset/ | mobi/oneway/sd/core/runtime/ShadowWebView.java |
| https://tl.oneway.mobi | mobi/oneway/export/a/a.java |
| http://track.oway.mobi | mobi/oneway/export/a/a.java |
| http://tl.oway.mobi | mobi/oneway/export/a/a.java |
| http://owtk.audioadx.com | mobi/oneway/export/a/a.java |
| http://118.178.152.152 | mobi/oneway/export/a/a.java |
| https://ads.oneway.mobi | mobi/oneway/export/a/a.java |
| http://ads.oway.mobi | mobi/oneway/export/a/a.java |
| http://owads.audioadx.com | mobi/oneway/export/a/a.java |
| https://adservice.sigmob.cn/strategy/v5 | com/windmill/sdk/c/c.java |
| https://dc.sigmob.cn/log | com/windmill/sdk/c/c.java |
| https://adservice.sigmob.cn/windmill/config? | com/windmill/sdk/c/c.java |
| https://adservice.sigmob.cn/extconfig? | com/windmill/sdk/c/c.java |
| https://cpro.baidustatic.com/cpro/logo/sdk/mob-adIcon\_2x.png | com/baidu/mobads/sdk/api/XAdEntryResponse.java |
| https://cpro.baidustatic.com/cpro/logo/sdk/new-bg-logo.png | com/baidu/mobads/sdk/api/XAdEntryResponse.java |
| http://union.baidu.com/ | com/baidu/mobads/sdk/api/XAdEntryResponse.java |
| https://cpro.baidustatic.com/cpro/logo/sdk/mob-adIcon\_2x.png | com/baidu/mobads/sdk/api/XAdNativeResponse.java |
| https://cpro.baidustatic.com/cpro/logo/sdk/new-bg-logo.png | com/baidu/mobads/sdk/api/XAdNativeResponse.java |
| http://union.baidu.com/ | com/baidu/mobads/sdk/api/XAdNativeResponse.java |
| http://211.151.146.65:8080/wlantest/shanghai\_sun/mock\_ad\_server\_intersitial\_video.json | com/baidu/mobads/sdk/internal/dj.java |
| https://github.com/danikula/AndroidVideoCache/issues/43. | com/danikula/videocache/HttpUrlSource.java |
| https://github.com/danikula/AndroidVideoCache/issues. | com/danikula/videocache/HttpUrlSource.java |
| https://github.com/danikula/AndroidVideoCache/issues/88. | com/danikula/videocache/HttpUrlSource.java |
| https://github.com/danikula/AndroidVideoCache/issues/134. | com/danikula/videocache/Pinger.java |
| http://%s:%d/%s | com/danikula/videocache/Pinger.java |
| http://%s:%d/%s | com/danikula/videocache/HttpProxyCacheServer.java |
| https://adservice.sigmob.cn/sigmob/config | com/sigmob/sdk/base/h.java |
| https://adservice.sigmob.cn/sigmob/config? | com/sigmob/sdk/base/i.java |
| https://adservice.sigmob.cn/extconfig? | com/sigmob/sdk/base/i.java |
| https://dc.sigmob.cn/log | com/sigmob/sdk/base/i.java |
| https://adservice.sigmob.cn/ad/v4 | com/sigmob/sdk/base/i.java |
| https://adservice.sigmob.cn/hb/v2/ad | com/sigmob/sdk/base/i.java |
| https://m.sigmob.com | com/sigmob/sdk/mraid/b.java |
| http://%s:%d/%s | com/sigmob/sdk/videocache/h.java |
| http://%s:%d/%s | com/sigmob/sdk/videocache/m.java |
| https://github.com/danikula/AndroidVideoCache/issues/134. | com/sigmob/sdk/videocache/m.java |
| https://github.com/danikula/AndroidVideoCache/issues/43. | com/sigmob/sdk/videocache/j.java |
| https://github.com/danikula/AndroidVideoCache/issues. | com/sigmob/sdk/videocache/j.java |
| https://github.com/danikula/AndroidVideoCache/issues/88. | com/sigmob/sdk/videocache/j.java |
| https://github.com/danikula/AndroidVideoCache/issues/43. | com/beizi/ad/internal/c/h.java |
| https://github.com/danikula/AndroidVideoCache/issues. | com/beizi/ad/internal/c/h.java |
| https://github.com/danikula/AndroidVideoCache/issues | com/beizi/ad/internal/c/j.java |
| https://api.htp.ad-scope.com.cn/mb/sdk/event/v1?extInfo=wBLQeP8bmq6AuJ5DaZyc5xQQU\_92OWkSUdy\_6V4n2RA3Mbgehw6J67ZfwcDQCmj3uTyhCkrT8nMAsQ&requestUuid=\_\_REQUESTUUID\_\_&eventType=\_\_EVENTTYPE\_\_&appID=\_\_APPID\_\_&spaceID=\_\_SPACEID\_\_&channelID=\_\_CHANNELID\_\_&channelAppID=\_\_CHANNELAPPID\_\_&channelSpaceID=\_\_CHANNELSPACEID\_\_&ts=\_\_TS\_\_&ip=\_\_IP\_\_&netType=\_\_NETTYPE\_\_&carrier=\_\_CARRIER\_\_&errInfo=\_\_ERRINFO\_\_&sdkExtInfo=\_\_SDKEXTINFO\_\_&imei=\_\_IMEI\_\_&androidID=\_\_ANDROIDID\_\_&idfa=\_\_IDFA\_\_&idfv=\_\_IDFV\_\_&mac=\_\_MAC\_\_&uid=\_\_UID\_\_&sdkVersion=\_\_SDKVERSION\_\_&appVerison=\_\_APPVERSION\_\_ | com/beizi/ad/internal/view/AdViewImpl.java |
| https://v.behe.com/dsp20/ad/2017/5/5/28d147ed3e96a3ba8ac90703e4d66de2.jpg\ | com/beizi/ad/internal/network/ServerResponse.java |
| https://v.behe.com/dsp20/ad/2017/5/5/28d147ed3e96a3ba8ac90703e4d66de2.jpg | com/beizi/ad/internal/network/ServerResponse.java |
| https://api.ipify.org | com/sjm/sjmdsp/core/utils/NetworkTypeUtil.java |
| https://httpbin.org/ip | com/sjm/sjmdsp/core/utils/NetworkTypeUtil.java |
| http://www.google.com | com/sjm/sjmdsp/net/security/ParamSec.java |
| http://www.google.com? | com/sjm/sjmdsp/net/security/ParamSec.java |
| http://dapi.sjmbdl.cn | com/sjm/sjmdsp/net/task/NetConfig.java |
| http://dapi.sjmbdl.cn/api/android/v1/events | com/sjm/sjmdsp/net/task/NetConfig.java |
| http://sdk.hzsanjiaomao.com/sspconfig/%s.txt | com/sjm/sjmdsp/net/task/NetConfig.java |
| http://dapi.sjmbdl.cn/api/app/statistics | com/sjm/sjmdsp/net/task/NetConfig.java |
| http://dapi.sjmbdl.cn/api/app/v2/log | com/sjm/sjmdsp/net/task/NetConfig.java |
| http://dapi.sjmbdl.cn/api/android/v1/init | com/sjm/sjmdsp/net/task/NetConfig.java |
| https://d.alipay.com | com/sjm/sjmdsp/web/SjmAdPageWebViewSetting.java |
| http://changemaker.hzsanjiaomao.com:6688/105009 | com/sjm/sjmdsp/adCore/SjmDspAd.java |
| http://api.hzsanjiaomao.com/api/adEvent | com/sjm/sjmsdk/adSdk/f/d.java |
| http://sdk.hzsanjiaomao.com/sjmconfig/%s.json | com/sjm/sjmsdk/core/c/c.java |
| https://d.alipay.com | com/sjm/sjmsdk/js/b.java |
| https://hybird.rayjump.com/rv/authoriztion.html | com/mbridge/msdk/a.java |
| https://play.google.com/ | com/mbridge/msdk/click/b.java |
| http://www.w3.org/ns/ttml | com/mbridge/msdk/playercommon/exoplayer2/text/ttml/TtmlDecoder.java |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense | com/mbridge/msdk/playercommon/exoplayer2/drm/HttpMediaDrmCallback.java |
| https://cdn-adn-https.rayjump.com/cdn-adn/v2/portal/19/08/20/11/06/5d5b63cb457e2.js | com/mbridge/msdk/foundation/controller/b.java |
| https://analytics.rayjump.com | com/mbridge/msdk/foundation/same/net/g/d.java |
| https://net.rayjump.com | com/mbridge/msdk/foundation/same/net/g/d.java |
| https://configure.rayjump.com | com/mbridge/msdk/foundation/same/net/g/d.java |
| https://detect.rayjump.com/mapi/find | com/mbridge/msdk/foundation/same/net/g/d.java |
| https://detect.rayjump.com/mapi/result | com/mbridge/msdk/foundation/same/net/g/d.java |
| https://d1tru86qrby720.cloudfront.net/hostsetting | com/mbridge/msdk/foundation/same/net/g/d.java |
| https://policy.rayjump.com | com/mbridge/msdk/foundation/same/net/g/d.java |
| https://lazy.rayjump.com | com/mbridge/msdk/foundation/same/net/g/d.java |
| https://check.rayjump.com | com/mbridge/msdk/foundation/same/net/g/d.java |
| https://play.google.com/store/apps/details?id= | com/mbridge/msdk/foundation/tools/v.java |
| https://play.google.com/ | com/mbridge/msdk/foundation/tools/v.java |
| https://play.google.com | com/mbridge/msdk/mbjscommon/windvane/WindVaneWebView.java |
| https://cdn-adn-https.rayjump.com/cdn-adn/v2/portal/19/08/20/11/06/5d5b63cb457e2.js | com/mbridge/msdk/b/b.java |
| http://whatwg.org/html/common-microsyntaxes.html | com/mbridge/msdk/b/b/c.java |
| http://whatwg.org/html/webappapis.html | com/mbridge/msdk/b/b/c.java |
| https://gist.github.com/atk/1020396\n | com/mbridge/msdk/b/b/c.java |
| http://whatwg.org/C | com/mbridge/msdk/b/b/c.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/ks\_so-appStatusArm64v8aRelease-3.3.14.apk | com/kwad/sdk/collector/d.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/ks\_so-appStatusArmeabiv7aRelease-3.3.14.apk | com/kwad/sdk/collector/d.java |
| http://apps.samsung.com/appquery/appDetail.as?appId= | com/kwad/sdk/utils/d.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/so/ks\_so-kwaiPlayerArm64v8aRelease-3.3.20.apk | com/kwad/sdk/core/video/kwai/e.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/so/ks\_so-kwaiPlayerArmeabiv7aRelease-3.3.20.apk | com/kwad/sdk/core/video/kwai/e.java |
| https://github.com/danikula/AndroidVideoCache/issues/43. | com/kwad/sdk/core/videocache/h.java |
| https://github.com/danikula/AndroidVideoCache/issues. | com/kwad/sdk/core/videocache/h.java |
| https://github.com/danikula/AndroidVideoCache/issues/88. | com/kwad/sdk/core/videocache/h.java |
| http://%s:%d/%s | com/kwad/sdk/core/videocache/f.java |
| https://open.e.kuaishou.com/rest/e/v3/open/sdk2 | com/kwad/sdk/api/loader/v.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/ks\_so-exceptionArm64v8aRelease-3.3.23.apk | com/kwad/sdk/crash/f.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/ks\_so-exceptionArmeabiv7aRelease-3.3.23.apk | com/kwad/sdk/crash/f.java |
| https://static.yximgs.com/udata/pkg/KSAdSDK/ksad\_page\_loading\_data\_limit\_error.png | com/kwad/components/ct/tube/view/EpisodeChooseLoadingView.java |
| https://static.yximgs.com/udata/pkg/KSAdSDK/ksad\_no\_video\_img.png | com/kwad/components/ct/tube/view/EpisodeChooseLoadingView.java |
| https://static.yximgs.com/udata/pkg/KSAdSDK/ksad\_page\_loading\_data\_error.png | com/kwad/components/ct/tube/view/EpisodeChooseLoadingView.java |
| https://static.yximgs.com/udata/pkg/KSAdSDK/ksad\_no\_data\_img.png | com/kwad/components/ct/tube/view/EpisodeChooseLoadingView.java |
| https://static.yximgs.com/udata/pkg/KSAdSDK/ksad\_page\_loading\_data\_limit\_error.png | com/kwad/components/ct/widget/KSPageLoadingView.java |
| https://static.yximgs.com/udata/pkg/KSAdSDK/ksad\_no\_video\_img.png | com/kwad/components/ct/widget/KSPageLoadingView.java |
| https://static.yximgs.com/udata/pkg/KSAdSDK/ksad\_page\_loading\_data\_error.png | com/kwad/components/ct/widget/KSPageLoadingView.java |
| https://static.yximgs.com/udata/pkg/KSAdSDK/ksad\_no\_data\_img.png | com/kwad/components/ct/widget/KSPageLoadingView.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/wallpaper/kwai\_wallpaper\_plugin\_1.4.apk | com/kwad/components/ct/wallpaper/c/b.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/wallpaper/kwai\_wallpaper\_plugin\_1.5.apk | com/kwad/components/ct/wallpaper/c/b.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/ks\_so-webpArm64v8aRelease-3.3.9.apk | com/kwad/components/ct/a/c.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/ks\_so-webpArmeabiv7aRelease-3.3.9.apk | com/kwad/components/ct/a/c.java |
| https://static.yximgs.com/udata/pkg/KSAdSDK/coupon/ksad\_coupon\_entry\_status\_3.webp | com/kwad/components/ct/coupon/entry/CouponEntryContainer.java |
| https://static.yximgs.com/udata/pkg/KSAdSDK/coupon/ksad\_coupon\_entry\_status\_2.webp | com/kwad/components/ct/coupon/entry/CouponEntryContainer.java |
| https://static.yximgs.com/udata/pkg/KSAdSDK/coupon/ksad\_coupon\_entry\_status\_1.webp | com/kwad/components/ct/coupon/entry/CouponEntryContainer.java |
| https://static.yximgs.com/udata/pkg/KSAdSDK/coupon/ksad\_coupon\_entry\_status\_4.webp | com/kwad/components/ct/coupon/entry/CouponEntryContainer.java |
| https://static.yximgs.com/udata/pkg/KSAdSDK/coupon/ksad\_coupon\_entry\_status\_0.webp | com/kwad/components/ct/coupon/entry/CouponEntryContainer.java |
| https://js-ad.a.yximgs.com/kos/nlav10933/ksad\_profile\_header\_bg.png | com/kwad/components/ct/profile/home/b/c.java |
| https://passport.kuaishou.com/account-h5/login?smallWebview=true&sid=kuaishou.unioncontent.wallpaper | com/kwad/components/ct/b/a.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/offline\_components/tk/ks\_so-tachikomaNoSoRelease-3.3.32.1-c07a870c9-58.zip | com/kwad/components/offline/tk/b.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/tachikoma/3.3.24.2/ks\_so-tachikomaLiteArm64v8aRelease-3.3.24.2.apk | com/kwad/components/offline/tk/a/a.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/tachikoma/3.3.24.2/ks\_so-tachikomaArm64v8aRelease-3.3.24.2.apk | com/kwad/components/offline/tk/a/a.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/tachikoma/3.3.24.2/ks\_so-tachikomaLiteArmeabiv7aRelease-3.3.24.2.apk | com/kwad/components/offline/tk/a/a.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/tachikoma/3.3.24.2/ks\_so-tachikomaArmeabiv7aRelease-3.3.24.2.apk | com/kwad/components/offline/tk/a/a.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/offline\_components/obiwan/ks\_so-obiwanNoSoRelease-3.3.31.1-261163b35a-47.zip | com/kwad/components/offline/obiwan/a.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/offline\_components/adLive/ks\_so-adLiveNoSoRelease-3.3.32.1-f1f921211-59.zip | com/kwad/components/offline/adLive/a.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/adLive/3.3.26.1/ks\_so-adLiveArm64v8aRelease-3.3.26.1.apk | com/kwad/components/offline/adLive/kwai/a.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/adLive/3.3.26.1/ks\_so-adLiveArmeabiv7aRelease-3.3.26.1.apk | com/kwad/components/offline/adLive/kwai/a.java |
| https://github.com/lingochamp/FileDownloader/wiki/filedownloader.properties | com/kwai/filedownloader/services/a.java |
| https://webcast-open.douyin.com | com/bytedance/android/openliveplugin/material/LiveInitMaterialManager.java |
| https://webcast-open.douyin.com/webcast/openapi/pangle/setting/?app\_id= | com/bytedance/android/openliveplugin/material/LiveInitMaterialManager.java |
| https://webcast.amemv.com/falcon/webcast\_douyin/page/anchor\_task\_v2/panel/index.html?web\_bg\_color=%23ff161823 | com/bytedance/android/live/base/api/BuildConfig.java |
| https://webcast.amemv.com/falcon/webcast\_douyin/page/recharge\_v1/index.html | com/bytedance/android/live/base/api/BuildConfig.java |
| http://bugs.java.com) | com/sun/tools/javac/resources/javac\_zh\_CN.java |
| http://bugreport.java.com) | com/sun/tools/javac/resources/javac\_zh\_CN.java |
| http://bugs.java.com) | com/sun/tools/javac/resources/javac\_ja.java |
| http://bugreport.java.com) | com/sun/tools/javac/resources/javac\_ja.java |
| https://htmlpreview.github.io/?https://bitbucket.org/typetools/jsr308-langtools/raw/tip/doc/README-jsr308.html | com/sun/tools/javac/resources/javac.java |
| https://test.com | com/tencent/klevin/download/b/w/e.java |
| http://119.29.29.29/d?dn= | com/tencent/klevin/download/b/s/a.java |
| https://test.api.yky.qq.com/ | com/tencent/klevin/c/e/a.java |
| https://api.yky.qq.com/ | com/tencent/klevin/c/e/a.java |
| https://static.yky.qq.com/bridge-h5/latest/dist/js-bridge-h5.umd.js | com/tencent/klevin/config/b/a.java |
| https://test.api.yky.qq.com/ | com/tencent/klevin/config/b/b.java |
| https://api.yky.qq.com/ | com/tencent/klevin/config/b/b.java |
| https://github.com/danikula/AndroidVideoCache/issues/43. | com/tencent/klevin/e/j/d.java |
| https://github.com/danikula/AndroidVideoCache/issues. | com/tencent/klevin/e/j/d.java |
| https://github.com/danikula/AndroidVideoCache/issues/88. | com/tencent/klevin/e/j/d.java |
| https://test.api.yky.qq.com/ | com/tencent/klevin/e/b/a.java |
| https://api.yky.qq.com/ | com/tencent/klevin/e/b/a.java |
| https://cloud.tgpa.qq.com | com/tencent/tgpa/lite/InitConfig.java |
| https://cloud.tgpa.qq.com | com/tencent/tgpa/lite/f/a.java |
| https://testcloud.tgpa.qq.com | com/tencent/tgpa/lite/f/a.java |
| https://www.samsungapps.com/appquery/appDetail.as?appId= | com/ss/android/downloadlib/utils/ko.java |
| https://sf6-ttcdn-tos.pstatp.com/obj/ad-tetris-site/personal-privacy-page.html | com/ss/android/downloadlib/addownload/compliance/AppPrivacyPolicyActivity.java |
| https://apps.oceanengine.com/customer/api/app/pkg\_info? | com/ss/android/downloadlib/addownload/compliance/ox.java |
| https://i.snssdk.com/ | com/ss/android/downloadad/api/constant/AdBaseConstants.java |
| https://dc.sigmob.cn/log | com/czhj/sdk/common/models/Config.java |
| https://crbug.com/581399 | aegon/chrome/net/impl/UrlRequestBuilderImpl.java |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| auth-agent@openssh.com | cn/hutool/extra/ssh/ChannelType.java |
| danikula@gmail.com | com/danikula/videocache/HttpUrlSource.java |
| danikula@gmail.com | com/sigmob/sdk/videocache/j.java |
| .apk@classes.dex | com/kuaishou/weapon/p0/ac.java |
| danikula@gmail.com | com/kwad/sdk/core/videocache/h.java |
| danikula@gmail.com | com/tencent/klevin/e/j/d.java |
| xxx@email.elided | aegon/chrome/base/PiiElider.java |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179879616 | org/checkerframework/com/github/javaparser/GeneratedJavaParserTokenManager.java |
| 17205037056 | org/checkerframework/com/github/javaparser/GeneratedJavaParserTokenManager.java |
| 17205035008 | org/checkerframework/com/github/javaparser/GeneratedJavaParserTokenManager.java |
| 17179869184 | org/checkerframework/com/github/javaparser/GeneratedJavaParserTokenManager.java |
| 17179878401 | org/checkerframework/com/github/javaparser/GeneratedJavaParserTokenManager.java |
| 17179869188 | org/checkerframework/com/github/javaparser/GeneratedJavaParserTokenManager.java |
| 17179869184 | com/kwai/video/player/KsMediaMeta.java |
| 17179869184 | com/sun/tools/javac/comp/DeferredAttr.java |
| 17179869184 | com/sun/tools/javac/comp/Resolve.java |
| 17179869184 | com/sun/tools/javac/comp/Check.java |
| 17179869184 | com/sun/tools/javac/comp/MemberEnter.java |
| 17179869184 | com/sun/tools/javac/comp/LambdaToMethod.java |
| 17179869184 | com/sun/tools/javac/code/Printer.java |
| 17179869184 | com/sun/tools/javac/code/Symbol.java |
| 17179869184 | com/sun/tools/javac/code/Flags.java |
| 17179869184 | com/sun/tools/javac/util/RichDiagnosticFormatter.java |
| 17179869184 | com/sun/tools/javac/jvm/ClassReader.java |
| 17179869184 | com/sun/tools/javac/jvm/ClassWriter.java |
| 17179869184 | com/sun/tools/javac/tree/Pretty.java |
| 17179869184 | com/sun/tools/javac/parser/JavacParser.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=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com 签名算法: rsassa\_pkcs1v15 有效期自: 2008-02-29 01:33:46+00:00 有效期至: 2035-07-17 01:33:46+00:00 发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com 序列号: 0x936eacbe07f201df 哈希算法: sha1 md5值: e89b158e4bcf988ebd09eb83f5378e87 sha1值: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81 sha256值: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc sha512值: 5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea303977272d17958704d89b7711292a4569 公钥算法: rsa 密钥长度: 2048 指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "ksad\_ad\_default\_author" : "@可爱的广告君创造的原声" |
| "ksad\_ad\_default\_username" : "@可爱的广告君" |

## **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.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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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.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.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\_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.GET\_TASKS | 危险 | 检索正在运行的应用程序 | 允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息 |
| android.permission.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.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.MOUNT\_UNMOUNT\_FILESYSTEMS | 危险 | 装载和卸载文件系统 | 允许应用程序为可移动存储安装和卸载文件系统 |
| com.sjm.dtsecond.amh.openadsdk.permission.TT\_PANGOLIN | 未知 | Unknown permission | Unknown permission from android reference |
| com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.CHANGE\_NETWORK\_STATE | 正常 | 更改网络连接 | 允许应用程序更改网络连接状态。 |
| android.permission.QUERY\_ALL\_PACKAGES | 正常 |  | 允许查询设备上的任何普通应用程序,无论清单声明如何 |
| android.permission.REORDER\_TASKS | 正常 | 重新排序正在运行的应用程序 | 允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前 |
| freemme.permission.msa | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_PRIVILEGED\_PHONE\_STATE | 未知 | Unknown permission | Unknown permission from android reference |
| com.sjm.dtsecond.amh.permission.KW\_SDK\_BROADCAST | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.SET\_WALLPAPER | 正常 | 设置壁纸 | 允许应用程序设置系统壁纸 |
| 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 |

## **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。**