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

**Spermatid Pro（ 6.3.2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 Pro |
| 版本 | 6.3.2 |
| 包名 | com.csjcbs |
| 域名线索 | 45条 |
| URL线索 | 67条 |
| APP图标 |  |
| 分析日期 | 2025年9月23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 | SpermatidPro\_6.3.2.apk |
| 文件大小 | 43.45MB |
| MD5值 | 7bc35a673c36836d260d64bf515ad91d |
| SHA1值 | d172984365b14dac2d41e1cb55efdf5ec0770dfb |
| SHA256值 | a40cda615b2d88d84d6f886a91f9badedc0fa9e79d08bdfb6997c2ec72cb0456 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | Spermatid Pro |
| 包名 | com.csjcbs |
| 主活动Activity | com.csjcbs.SplashActivity |
| 安卓版本名称 | 6.3.2 |
| 安卓版本 | 632 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| xml.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| open.weixin.qq.com | IP: 220.196.139.154 所属国家: China 地区: Jiangsu 城市: Yangzhou  |
| i.snssdk.com | IP: 123.125.216.193 所属国家: China 地区: Beijing 城市: Beijing  |
| long.open.weixin.qq.com | IP: 112.65.193.150 所属国家: China 地区: Shanghai 城市: Shanghai  |
| logrcv.qquanquan.com | IP: 60.29.233.213 所属国家: China 地区: Tianjin 城市: Tianjin  |
| fy.1sapp.com | IP: 123.56.87.63 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  |
| www.adintl.cn | IP: 39.106.82.180 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| sdk-config.tanx.com | IP: 203.119.169.238 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| dsp.shenshiads.com | 没有服务器地理信息.  |
| crbug.com | IP: 216.239.32.29 所属国家: United States of America 地区: California 城市: Mountain View  |
| tracelog-debug.qquanquan.com | IP: 60.29.233.213 所属国家: China 地区: Tianjin 城市: Tianjin  |
| style-browse-openapi.test.gifshow.com | IP: 103.102.202.41 所属国家: China 地区: Beijing 城市: Beijing  |
| static01.kuaichuanad.com | IP: 1.56.96.144 所属国家: China 地区: Heilongjiang 城市: Harbin  |
| pre-sdk-config.alibaba-inc.com | IP: 203.119.204.173 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| plus.google.com | IP: 199.193.116.105 所属国家: United States of America 地区: Florida 城市: Tampa  |
| apps.bytesfield-b.com | IP: 116.136.187.89 所属国家: China 地区: Nei Mongol 城市: Hohhot  |
| dc.sigmob.cn | IP: 47.94.5.41 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| p1-lm.adkwai.com | IP: 119.188.131.16 所属国家: China 地区: Shandong 城市: Jinan  |
| static.yximgs.com | IP: 101.73.102.242 所属国家: China 地区: Hebei 城市: Shijiazhuang  |
| mp.weixin.qq.com | IP: 220.196.139.154 所属国家: China 地区: Jiangsu 城市: Yangzhou  |
| open.e.kuaishou.com | IP: 101.73.106.220 所属国家: China 地区: Hebei 城市: Shijiazhuang  |
| engine.tuifish.com | IP: 47.110.6.71 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| task.tanx.com | IP: 59.82.31.200 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| union.baidu.com | IP: 111.206.208.169 所属国家: China 地区: Beijing 城市: Beijing  |
| apps.bytesfield.com | IP: 60.222.11.205 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| passport.kuaishou.com | IP: 103.107.217.66 所属国家: China 地区: Beijing 城市: Beijing  |
| usr-api.1sapp.com | IP: 123.56.87.63 所属国家: China 地区: Beijing 城市: Beijing  |
| et.tanx.com | IP: 59.82.31.200 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| update0.qquanquan.com | IP: 125.36.181.16 所属国家: China 地区: Tianjin 城市: Tianjin  |
| js-ad.a.yximgs.com | IP: 116.136.186.68 所属国家: China 地区: Nei Mongol 城市: Hohhot  |
| oc-adpict.oss-cn-shanghai.aliyuncs.com | IP: 140.206.110.94 所属国家: China 地区: Shanghai 城市: Shanghai  |
| opehs.tanx.com | IP: 59.82.31.200 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| schemas.android.com | 没有服务器地理信息.  |
| gw.alicdn.com | IP: 60.9.1.110 所属国家: China 地区: Hebei 城市: Hengshui  |
| img.alicdn.com | IP: 27.221.79.107 所属国家: China 地区: Shandong 城市: Qingdao  |
| apps.oceanengine.com | IP: 116.136.187.90 所属国家: China 地区: Nei Mongol 城市: Hohhot  |
| sf6-ttcdn-tos.pstatp.com | IP: 101.71.175.236 所属国家: China 地区: Zhejiang 城市: Ningbo  |
| www.samsungapps.com | IP: 54.229.93.185 所属国家: Ireland 地区: Dublin 城市: Dublin  |
| videoproxy.tanx.com | IP: 59.82.31.141 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| cpro.baidustatic.com | IP: 101.72.203.38 所属国家: China 地区: Hebei 城市: Langfang  |
| content-api.shenshiads.com | IP: 203.107.86.92 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| opensource.org | IP: 104.21.84.214 所属国家: United States of America 地区: California 城市: San Francisco  |
| qfc.innotechx.com | IP: 123.56.87.63 所属国家: China 地区: Beijing 城市: Beijing  |
| apps.samsung.com | IP: 139.215.225.97 所属国家: China 地区: Jilin 城市: Changchun  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://crbug.com/581399  | aegon/chrome/net/impl/UrlRequestBuilderImpl.java  |
| https://github.com/javaparser/javaparser/issues  | a9/j.java  |
| https://gw.alicdn.com/imgextra/i3/O1CN01yRRocx28JI2PSwyrX\_!!6000000007911-0-tps-1080-1320.jpg\_q90.jpg  | com/alimm/tanx/core/ad/ad/template/rendering/feed/dialog/ExitRetentionDialog.java  |
| https://img.alicdn.com/imgextra/i3/O1CN01yaPRML1GyyqsOZP7R\_!!6000000000692-1-tps-1200-432.gif  | com/alimm/tanx/core/orange/OrangeManager.java  |
| https://sdk-config.tanx.com  | com/alimm/tanx/core/request/C.java  |
| https://pre-sdk-config.alibaba-inc.com  | com/alimm/tanx/core/request/C.java  |
| http://pre-sdk-config.alibaba-inc.com  | com/alimm/tanx/core/request/C.java  |
| https://videoproxy.tanx.com  | com/alimm/tanx/core/request/C.java  |
| http://videoproxy.tanx.com  | com/alimm/tanx/core/request/C.java  |
| https://et.tanx.com  | com/alimm/tanx/core/request/C.java  |
| http://sdk-config.tanx.com  | com/alimm/tanx/core/request/C.java  |
| https://task.tanx.com  | com/alimm/tanx/core/request/C.java  |
| http://task.tanx.com  | com/alimm/tanx/core/request/C.java  |
| https://opehs.tanx.com  | com/alimm/tanx/core/request/C.java  |
| http://opehs.tanx.com  | com/alimm/tanx/core/request/C.java  |
| http://et.tanx.com  | com/alimm/tanx/core/request/C.java  |
| https://videoproxy.tanx.com/tanx\_task  | com/alimm/tanx/core/request/C.java  |
| http://videoproxy.tanx.com/tanx\_task  | com/alimm/tanx/core/request/C.java  |
| https://github.com/danikula/AndroidVideoCache/issues/88.  | com/alimm/tanx/core/view/player/cache/videocache/HttpUrlSource.java  |
| https://github.com/danikula/AndroidVideoCache/issues/43.  | com/alimm/tanx/core/view/player/cache/videocache/HttpUrlSource.java  |
| https://github.com/danikula/AndroidVideoCache/issues.  | com/alimm/tanx/core/view/player/cache/videocache/HttpUrlSource.java  |
| http://%s:%d/%s  | com/alimm/tanx/core/view/player/cache/videocache/Pinger.java  |
| https://github.com/danikula/AndroidVideoCache/issues/134.  | com/alimm/tanx/core/view/player/cache/videocache/Pinger.java  |
| http://%s:%d/%s  | com/alimm/tanx/core/view/player/cache/videocache/HttpProxyCacheServer.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  |
| 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  |
| http://union.baidu.com  | com/baidu/mobads/sdk/internal/ao.java  |
| https://i.snssdk.com/  | com/bytedance/sdk/openadsdk/downloadnew/core/AdBaseConstants.java  |
| https://dc.sigmob.cn/log  | com/czhj/sdk/common/models/Config.java  |
| https://usr-api.1sapp.com  | com/inno/innosdk/utils/m.java  |
| https://qfc.innotechx.com  | com/inno/innosdk/utils/m.java  |
| https://fy.1sapp.com  | com/inno/innosdk/utils/m.java  |
| http://qfc.innotechx.com/report/v1  | com/inno/innosdk/utils/m.java  |
| http://usr-api.1sapp.com/107635  | com/inno/innosdk/utils/m.java  |
| http://usr-api.1sapp.com  | com/inno/innosdk/utils/m.java  |
| http://qfc.innotechx.com  | com/inno/innosdk/utils/m.java  |
| http://fy.1sapp.com  | com/inno/innosdk/utils/m.java  |
| https://tracelog-debug.qquanquan.com  | com/hailiang/advlib/common/d.java  |
| https://logrcv.qquanquan.com/trace  | com/hailiang/advlib/common/d.java  |
| http://content-api.shenshiads.com/content/toutiao  | com/kc/openset/news/NewsTypeFragment.java  |
| http://dsp.shenshiads.com/event/show  | com/kc/openset/sdk/dsp/banner/ODBannerView.java  |
| http://dsp.shenshiads.com/event/show  | com/kc/openset/sdk/dsp/dialog/a.java  |
| http://dsp.shenshiads.com/event/show  | com/kc/openset/sdk/dsp/information/ODInformation.java  |
| http://static01.kuaichuanad.com/upload/20220221/1bd77fc5f982095ac4d96bb53f34f362.mp4  | com/kc/openset/sdk/mat/a.java  |
| https://engine.tuifish.com/index/activity?appKey=36cYig9mbhQdFcbYJQgdaKACmVnL\\u0026adslotId=376287\\u0026uk\_a1=\_\_IMEI\_\_\\u0026uk\_a2=\_\_IMEI2\_\_\\u0026uk\_a3=\_\_MUID\_\_\\u0026uk\_b1=\_\_IDFA\_\_\\u0026uk\_b2=\_\_IDFA2\_\_\\u0026uk\_c1=\_\_OAID\_\_\\u0026uk\_c2=\_\_OAID2\_\_  | com/kc/openset/sdk/mat/a.java  |
| http://content-api.shenshiads.com/weather  | com/kc/openset/activity/OSETWeatherDetailsActivity.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://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/wallpaper/kwai\_wallpaper\_plugin\_1.4.apk  | com/kwad/components/ct/wallpaper/d/b.java  |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/wallpaper/kwai\_wallpaper\_plugin\_1.5.apk  | com/kwad/components/ct/wallpaper/d/b.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://js-ad.a.yximgs.com/kos/nlav10933/ksad\_profile\_header\_bg.png  | com/kwad/components/ct/profile/home/c/c.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://passport.kuaishou.com/account-h5/login?smallWebview=true&sid=kuaishou.unioncontent.wallpaper  | com/kwad/components/ct/c/a.java  |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/ks\_so-webpArm64v8aRelease-3.3.9-e8fbb3a5f8-666.apk  | com/kwad/components/ct/b/c.java  |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/ks\_so-webpArmeabiv7aRelease-3.3.9-e8fbb3a5f8-666.apk  | com/kwad/components/ct/b/c.java  |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/offline\_components/tk/ks\_so-tachikomaNoSoRelease-3.3.71-2c1b8e2a82-567.zip  | com/kwad/components/offline/c/c.java  |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/tachikoma/3.3.58/ks\_tk\_so\_v8\_lite\_3358  | com/kwad/components/offline/c/b/a.java  |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/tachikoma/3.3.58/ks\_tk\_so\_v8\_3358  | com/kwad/components/offline/c/b/a.java  |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/tachikoma/3.3.58/ks\_tk\_so\_v7\_lite\_3358  | com/kwad/components/offline/c/b/a.java  |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/tachikoma/3.3.58/ks\_tk\_so\_v7\_3358  | com/kwad/components/offline/c/b/a.java  |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/offline\_components/obiwan/ks\_so-obiwanNoSoRelease-3.3.56-445ef4f109-409.zip  | com/kwad/components/offline/b/b.java  |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/offline\_components/adLive/ks\_so-adLiveNoSoRelease-3.3.68-9a2e5abfa5-559.zip  | com/kwad/components/offline/a/b.java  |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/adLive/ks\_so-adLiveArm64v8aRelease-3.3.44.2-e8fbb3a5f8-666.apk  | com/kwad/components/offline/a/a/a.java  |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/adLive/ks\_so-adLiveArmeabiv7aRelease-3.3.44.2-e8fbb3a5f8-666.apk  | com/kwad/components/offline/a/a/a.java  |
| https://github.com/lingochamp/FileDownloader/wiki/filedownloader.properties  | com/kwad/framework/filedownloader/services/a.java  |
| https://style-browse-openapi.test.gifshow.com//rest/e/internal/adBrowse  | com/kwad/sdk/h.java  |
| https://open.e.kuaishou.com/rest/e/v3/open/sdk2  | com/kwad/sdk/api/loader/v.java  |
| http://%s:%d/%s  | com/kwad/sdk/core/videocache/f.java  |
| https://github.com/danikula/AndroidVideoCache/issues/88.  | com/kwad/sdk/core/videocache/h.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://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/so/ks\_so-kwaiPlayerArm64v8aRelease-3.3.44-e8fbb3a5f8-666.apk  | com/kwad/sdk/core/video/a/e.java  |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/so/ks\_so-kwaiPlayerArmeabiv7aRelease-3.3.44-e8fbb3a5f8-666.apk  | com/kwad/sdk/core/video/a/e.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  |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/so/exception/202406211433/ks\_so-exceptionArm64v8aRelease-3.3.67-e8fbb3a5f8-666.apk  | com/kwad/sdk/crash/g.java  |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/so/exception/202406211433/ks\_so-exceptionArmeabiv7aRelease-3.3.67-e8fbb3a5f8-666.apk  | com/kwad/sdk/crash/g.java  |
| http://apps.samsung.com/appquery/appDetail.as?appId=  | com/kwad/sdk/utils/e.java  |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/kmac/ks\_kmac64  | com/kwad/sdk/kgeo/c.java  |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/kmac/ks\_kmac32  | com/kwad/sdk/kgeo/c.java  |
| https://github.com/danikula/AndroidVideoCache/issues/88.  | com/octopus/ad/internal/a/j.java  |
| http://%s:%d/%s  | com/octopus/ad/internal/a/m.java  |
| https://github.com/danikula/AndroidVideoCache/issues/134.  | com/octopus/ad/internal/a/m.java  |
| http://%s:%d/%s  | com/octopus/ad/internal/a/h.java  |
| https://www.adintl.cn/sdkFeedback.html?slotId=  | com/octopus/ad/internal/view/AdViewImpl.java  |
| https://oc-adpict.oss-cn-shanghai.aliyuncs.com/static/img/octlogo.png  | com/octopus/ad/internal/nativead/c.java  |
| https://oc-adpict.oss-cn-shanghai.aliyuncs.com/static/img/remdad.png  | com/octopus/ad/internal/nativead/c.java  |
| https://www.adintl.cn/sdkFeedback.html?slotId=  | com/octopus/ad/internal/nativead/c.java  |
| https://oc-adpict.oss-cn-shanghai.aliyuncs.com/static/img/remdad.png  | com/octopus/ad/internal/utilities/ViewUtil.java  |
| https://oc-adpict.oss-cn-shanghai.aliyuncs.com/static/img/octlogo.png  | com/octopus/ad/internal/utilities/ViewUtil.java  |
| https://dc.sigmob.cn/log  | com/sigmob/sdk/base/l.java  |
| http://%s:%d/%s  | com/sigmob/sdk/videocache/n.java  |
| http://%s:%d/%s  | com/sigmob/sdk/videocache/h.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/b.java  |
| https://apps.bytesfield.com  | com/ss/android/downloadlib/addownload/compliance/f.java  |
| https://apps.bytesfield-b.com  | com/ss/android/downloadlib/addownload/compliance/f.java  |
| https://www.samsungapps.com/appquery/appDetail.as?appId=  | com/ss/android/downloadlib/g/h.java  |
| https://i.snssdk.com/  | com/ss/android/downloadad/api/constant/AdBaseConstants.java  |
| https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s  | com/tencent/mm/opensdk/diffdev/a/c.java  |
| https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s  | com/tencent/mm/opensdk/diffdev/a/b.java  |
| https://mp.weixin.qq.com/publicpoc/opensdkconf?action=GetShareConf&appid=%s&sdkVersion=%s&buffer=%s  | com/tencent/mm/opensdk/openapi/WXAPiSecurityHelper.java  |
| http://xml.apache.org/xslt  | e1/y.java  |
| https://plus.google.com/  | m5/m.java  |
| http://schemas.android.com/apk/res/android  | t6/b.java  |
| https://update0.qquanquan.com/qm/nsdk/cgi/  | r8/h.java  |
| https://img.alicdn.com/imgextra/i3/O1CN01yaPRML1GyyqsOZP7R\_!!6000000000692-1-tps-1200-432.gif  | 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  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| xxx@email.elided  | aegon/chrome/base/PiiElider.java  |
| auth-agent@openssh.com  | cn/hutool/extra/ssh/ChannelType.java  |
| danikula@gmail.com  | com/alimm/tanx/core/view/player/cache/videocache/HttpUrlSource.java  |
| .apk@classes.dex  | com/kuaishou/weapon/p0/ac.java  |
| danikula@gmail.com  | com/kwad/sdk/core/videocache/h.java  |
| u0013android@android.com0 u0013android@android.com  | j5/o.java  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179879616  | a9/l.java  |
| 17205037056  | a9/l.java  |
| 17205035008  | a9/l.java  |
| 17179878401  | a9/l.java  |
| 17179869188  | a9/l.java  |
| 17179869184  | a9/l.java  |
| 17512775099  | b6/a.java  |
| 17179869184  | com/kwai/video/player/KsMediaMeta.java  |
| 17179869184  | com/sun/tools/javac/code/Flags.java  |
| 17179869184  | com/sun/tools/javac/code/Symbol.java  |
| 17179869184  | com/sun/tools/javac/tree/Pretty.java  |
| 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: 2024-03-24 12:04:43+00:00 有效期至: 2049-03-18 12:04:43+00:00 发行人: C=CN 序列号: 0x79d2462f 哈希算法: sha256 md5值: fa41bc00503cf2db5578bd493b9a90dd sha1值: 59b315eef18a2ded0ebd02a32a7a4b7ef7aae450 sha256值: 6e40647e5bef2cfb141a3c9bddd9c1622a77e9d43f12e5533bf266251f45d531 sha512值: 095c68d67b0341b35e22cc1b61355342c0a98c3753b00ab1117fba992b8cc97decb0b862922c61251bb8ccb1e04c9808d5bad61a379617b975f65c30f91e519c 公钥算法: rsa 密钥长度: 2048 指纹: 3e6b2eac47df7f6832c4cac3583a0c7adccab87ab9273899564377d9f0185ac2**

## **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.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.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.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.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\_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.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.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.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.REQUEST\_DELETE\_PACKAGES | 正常 |  | 允许应用程序请求删除包 |
| com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| freemme.permission.msa | 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 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| com.csjcbs.openadsdk.permission.TT\_PANGOLIN | 未知 | Unknown permission | Unknown permission from android reference |
| 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.EXPAND\_STATUS\_BAR | 正常 | 展开/折叠状态栏 | 允许应用程序展开或折叠状态栏 |
| 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。**