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

**直播管家（ 3.14.0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 | 直播管家 |
| 版本 | 3.14.0 |
| 包名 | com.dada.live.pusher |
| 域名线索 | 61条 |
| URL线索 | 58条 |
| APP图标 |  |
| 分析日期 | 2025年6月17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 | 3.14.0-2029.apk |
| 文件大小 | 213.6MB |
| MD5值 | b5f00673a5dd00a70df65a02265006b4 |
| SHA1值 | 711b17537820cbca97e5918fcf3bb3e653327904 |
| SHA256值 | 1b824828e83b2c554f8ab0ef495dfbc04dd096d39263d4d2b594b9d1c50d824a |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 直播管家 |
| 包名 | com.dada.live.pusher |
| 主活动Activity | com.qennnsad.aknkaksd.presentation.module.splash.SplashActivity |
| 安卓版本名称 | 3.14.0 |
| 安卓版本 | 2029 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| www.a | 没有服务器地理信息.  |
| westus.api.cognitive.microsoft.com | IP: 20.59.86.7 所属国家: United States of America 地区: California 城市: San Francisco  |
| .css | 没有服务器地理信息.  |
| avatar.trtc.tencent-cloud.com | IP: 61.162.174.60 所属国家: China 地区: Shandong 城市: Qingdao  |
| 1.0.0.1 | IP: 1.0.0.1 所属国家: United States of America 地区: California 城市: San Jose  |
| stackoverflow.com | IP: 104.18.32.7 所属国家: United States of America 地区: California 城市: San Francisco  |
| javax.xml.xmlconstants | 没有服务器地理信息.  |
| mcgw.alipay.com | IP: 123.125.216.241 所属国家: China 地区: Beijing 城市: Beijing  |
| www.rmp-streaming.com | IP: 104.26.2.180 所属国家: United States of America 地区: California 城市: San Francisco  |
| api.moonscap.com | IP: 104.21.22.58 所属国家: United States of America 地区: California 城市: San Francisco  |
| mobilegw.stable.alipay.net | 没有服务器地理信息.  |
| 223.5.5.5 | IP: 223.5.5.5 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| h5.m.taobao.com | IP: 218.11.15.30 所属国家: China 地区: Hebei 城市: Shijiazhuang  |
| www.lia | 没有服务器地理信息.  |
| metrics.telarycover.io | IP: 35.201.145.186 所属国家: Taiwan (Province of China) 地区: Taipei 城市: Taipei  |
| apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.text-decoration | 没有服务器地理信息.  |
| mobilegw-1-64.test.alipay.net | 没有服务器地理信息.  |
| videodev.ksyun.com | 没有服务器地理信息.  |
| www.years | 没有服务器地理信息.  |
| www.css | 没有服务器地理信息.  |
| raw.githubusercontent.com | IP: 0.0.0.0 所属国家: - 地区: - 城市: -  |
| cloudflare-dns.com | IP: 104.16.249.249 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.world | IP: 75.2.38.108 所属国家: United States of America 地区: Washington 城市: Seattle  |
| trace-ldns.ksyun.com | IP: 110.43.221.241 所属国家: China 地区: Beijing 城市: Beijing  |
| webman.moonscap.com | 没有服务器地理信息.  |
| recaptcha.akxdp.com | IP: 172.67.189.134 所属国家: United States of America 地区: California 城市: San Francisco  |
| license.vod-control.com | IP: 43.132.80.137 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| api.placeholder.com | 没有服务器地理信息.  |
| dev.testwebmessenger.ml | 没有服务器地理信息.  |
| www.interpretation | 没有服务器地理信息.  |
| media.giphy.com | IP: 151.101.42.2 所属国家: United States of America 地区: California 城市: San Francisco  |
| centertime.ksyun.com | IP: 60.28.198.144 所属国家: China 地区: Tianjin 城市: Tianjin  |
| xmlpull.org | IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| doh.pub | IP: 1.12.12.12 所属国家: China 地区: Beijing 城市: Beijing  |
| www.style | IP: 75.2.38.108 所属国家: United States of America 地区: Washington 城市: Seattle  |
| www.wencodeuricomponent | 没有服务器地理信息.  |
| www.recent | 没有服务器地理信息.  |
| play.google.com | IP: 59.24.3.174 所属国家: Korea (Republic of) 地区: Gyeonggi-do 城市: Seongnam  |
| schemas.android.com | 没有服务器地理信息.  |
| hydra.alibaba.com | IP: 203.119.169.241 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| isea-im-android.firebaseio.com | IP: 34.120.206.254 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| www.smpte-ra.org | IP: 52.20.185.129 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| mediacloud-76607.gzc.vod.tencent-cloud.com | IP: 27.44.123.101 所属国家: China 地区: Guangdong 城市: Dongguan  |
| mobilegw.alipay.com | IP: 203.209.255.238 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| m.alipay.com | IP: 203.209.245.74 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| .jpg | 没有服务器地理信息.  |
| static.moonscap.com | IP: 172.67.202.250 所属国家: United States of America 地区: California 城市: San Francisco  |
| app.posthog.com | IP: 104.22.59.181 所属国家: United States of America 地区: California 城市: San Francisco  |
| license.youtu.qq.com | IP: 220.194.116.113 所属国家: China 地区: Tianjin 城市: Tianjin  |
| www.language | 没有服务器地理信息.  |
| api.giphy.com | IP: 151.101.42.2 所属国家: United States of America 地区: California 城市: San Francisco  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| js.hcaptcha.com | IP: 104.18.124.91 所属国家: United States of America 地区: California 城市: San Francisco  |
| 1.1.1.1 | IP: 1.1.1.1 所属国家: United States of America 地区: California 城市: San Jose  |
| www.c | 没有服务器地理信息.  |
| www.icon | 没有服务器地理信息.  |
| sdk.ks-live.com | 没有服务器地理信息.  |
| www.hortcut | 没有服务器地理信息.  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| devinfo.ks-live.com | 没有服务器地理信息.  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://schemas.android.com/apk/res/android  | com/alimuzaffar/lib/pin/PinEntryEditText.java  |
| http://mobilegw.stable.alipay.net/mgw.htm  | com/alipay/apmobilesecuritysdk/face/APSecuritySdk.java  |
| https://mobilegw.alipay.com/mgw.htm  | com/alipay/apmobilesecuritysdk/face/APSecuritySdk.java  |
| http://mobilegw-1-64.test.alipay.net/mgw.htm  | com/alipay/apmobilesecuritysdk/face/APSecuritySdk.java  |
| http://mobilegw.alipay.com/mgw.htm  | com/alipay/sdk/cons/a.java  |
| http://m.alipay.com/?action=h5quit  | com/alipay/sdk/cons/a.java  |
| http://h5.m.taobao.com/trade/paySuccess.html?bizOrderId=$OrderId$&  | com/alipay/sdk/data/a.java  |
| http://mcgw.alipay.com/sdklog.do  | com/alipay/sdk/packet/impl/c.java  |
| https://mobilegw.alipay.com/mgw.htm  | com/alipay/security/mobile/module/a/a/a.java  |
| http://javax.xml.XMLConstants/feature/secure-processing  | com/fasterxml/jackson/databind/ext/DOMDeserializer.java  |
| http://apache.org/xml/features/disallow-doctype-decl  | com/fasterxml/jackson/databind/ext/DOMDeserializer.java  |
| http://apache.org/xml/features/nonvalidating/load-external-dtd  | com/fasterxml/jackson/databind/ext/DOMDeserializer.java  |
| http://javax.xml.XMLConstants/feature/secure-processing  | com/fasterxml/jackson/databind/ext/DOMSerializer.java  |
| https://api.giphy.com/  | com/giphy/glide/rest/service/GiphyService.java  |
| http://www.smpte-ra.org/schemas/2052-1/2010/smpte-tt  | com/googlecode/mp4parser/authoring/tracks/SMPTETTTrackImpl.java  |
| http://www.w3.org/ns/ttml  | com/googlecode/mp4parser/authoring/tracks/SMPTETTTrackImpl.java  |
| http://schemas.android.com/apk/res/android  | com/hbb20/CountryCodePicker.java  |
| https://js.hcaptcha.com/1/api.js',\n  | com/hcaptcha/sdk/HCaptchaHtml.java  |
| https://js.hcaptcha.com/1/api.js  | com/hcaptcha/sdk/HCaptchaConfig.java  |
| https://media.giphy.com/media/%s/giphy.gif  | com/im/freechat/data/SyncRepositoryImplKt.java  |
| https://223.5.5.5/resolve?name=\_messager.\_tls.api.moonscap.com&type=33  | com/im/freechat/data/sources/api/RemoteApi.java  |
| https://doh.pub/dns-query?name=\_messager.\_tls.api.moonscap.com&type=33  | com/im/freechat/data/sources/api/RemoteApi.java  |
| https://1.1.1.1/dns-query?name=\_messager.\_tls.api.moonscap.com&type=SRV&ct=application/dns-json  | com/im/freechat/data/sources/api/RemoteApi.java  |
| https://1.0.0.1/dns-query?name=\_messager.\_tls.api.moonscap.com&type=SRV&ct=application/dns-json  | com/im/freechat/data/sources/api/RemoteApi.java  |
| https://cloudflare-dns.com/dns-query?name=\_messager.\_tls.api.moonscap.com&type=SRV&ct=application/dns-json  | com/im/freechat/data/sources/api/RemoteApi.java  |
| https://dev.testwebmessenger.ml/admin  | com/im/freechat/ui/settings/SettingsFragment.java  |
| http://videodev.ksyun.com:8980/univ/intervalquery?  | com/ksy/statlibrary/util/Constants.java  |
| http://videodev.ksyun.com:8980/univ/monitorclient?  | com/ksy/statlibrary/util/Constants.java  |
| http://sdk.ks-live.com:8989/api/CanHWDecode/2017-01-01  | com/ksyun/media/player/KSYHardwareDecodeWhiteList.java  |
| https://trace-ldns.ksyun.com/getlocaldns  | com/ksyun/media/player/d/d.java  |
| http://trace-ldns.ksyun.com/getlocaldns  | com/ksyun/media/streamer/logstats/StatsConstant.java  |
| http://videodev.ksyun.com:8980/univ/clientcounter  | com/ksyun/media/streamer/logstats/d.java  |
| http://videodev.ksyun.com:8980/univ/clientcounter?accesskey=  | com/ksyun/media/streamer/logstats/d.java  |
| http://centertime.ksyun.com/time  | com/ksyun/media/streamer/util/TimeDeltaUtil.java  |
| http://devinfo.ks-live.com:8420/info  | com/ksyun/media/streamer/util/device/DeviceInfoTools.java  |
| http://devinfo.ks-live.com:8420/info?model=  | com/ksyun/media/streamer/util/device/DeviceInfoTools.java  |
| https://github.com/yyued/SVGAPlayer-Android  | com/opensource/svgaplayer/SVGAParser$FileDownloader$resume$1.java  |
| https://app.posthog.com  | com/posthog/android/PostHog.java  |
| https://api.placeholder.com/OpenAPI/  | com/qennnsad/aknkaksd/BuildConfig.java  |
| https://webman.moonscap.com  | com/qennnsad/aknkaksd/data/repository/AnyHostApiKt.java  |
| https://raw.githubusercontent.com/  | com/qennnsad/aknkaksd/data/repository/RetrofitApi.java  |
| https://api.placeholder.com/OpenAPI/  | com/qennnsad/aknkaksd/data/repository/RetrofitStaticSource.java  |
| https://api.placeholder.com/OpenAPI/  | com/qennnsad/aknkaksd/data/repository/RetrofitSource.java  |
| https://api.moonscap.com/OpenAPI/v1/  | com/qennnsad/aknkaksd/data/repository/RetrofitSource.java  |
| https://play.google.com  | com/qennnsad/aknkaksd/data/repository/dns/OverseasDetector.java  |
| https://api.moonscap.com  | com/qennnsad/aknkaksd/data/repository/dns/DnsResolver.java  |
| https://metrics.telarycover.io  | com/qennnsad/aknkaksd/initializers/PosthogInitializer.java  |
| https://recaptcha.akxdp.com  | com/qennnsad/aknkaksd/presentation/module/auth/captcha/ReCaptchaDialogKt.java  |
| https://recaptcha.akxdp.com  | com/qennnsad/aknkaksd/presentation/module/auth/captcha/ReCaptchaDialog.java  |
| https://api.moonscap.com/home/static/web/app/fan-page/exchange?token=  | com/qennnsad/aknkaksd/presentation/module/main/gamecenter/gamelist/GameListFragment$initViews$1$5.java  |
| http://stackoverflow.com/questions/23074446/java-lang-classcastexception-java-lang-class-cannot-be-cast-to-java-lang-reflec  | com/qennnsad/aknkaksd/presentation/ui/base/PresenterExtKt.java  |
| https://www.rmp-streaming.com/media/big-buck-bunny-360p.mp4  | com/qennnsad/aknkaksd/presentation/ui/room/player/player/PlayerActivity.java  |
| https://api.placeholder.com/OpenAPI/  | com/qennnsad/aknkaksd/util/NetworkUtility.java  |
| https://api.moonscap.com  | com/qennnsad/aknkaksd/util/NetworkUtility.java  |
| https://static.moonscap.com  | com/qennnsad/aknkaksd/util/NetworkUtility.java  |
| https://static.  | com/qennnsad/aknkaksd/util/NetworkUtility.java  |
| https://web.  | com/qennnsad/aknkaksd/util/NetworkUtility.java  |
| http://hydra.alibaba.com/  | com/ta/utdid2/aid/AidRequester.java  |
| http://xmlpull.org/v1/doc/features.html  | com/ta/utdid2/core/persistent/FastXmlSerializer.java  |
| http://xmlpull.org/v1/doc/features.html  | com/ta/utdid2/core/persistent/XmlUtils.java  |
| https://license.vod-control.com/license/v2/1315247704\_1/v\_cube.license  | com/tencent/demo/XMagicImpl.java  |
| https://license.youtu.qq.com/youtu/sdklicenseapi/license\_generate  | com/tencent/xmagic/auth/Auth.java  |
| https://avatar.trtc.tencent-cloud.com/avatar/base/v1/analyze  | com/tencent/xmagic/c/a.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/Flowable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Observable.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://dictionaryperceptionrevolutionfoundationpx;height:successfulsupportersmillenniumhis  | org/brotli/dec/Dictionary.java  |
| http://mathematicsmargin-top:eventually  | org/brotli/dec/Dictionary.java  |
| http://Descriptionrelatively  | org/brotli/dec/Dictionary.java  |
| http://applicationslink\  | org/brotli/dec/Dictionary.java  |
| http://navigation\  | org/brotli/dec/Dictionary.java  |
| http://px;  | org/brotli/dec/Dictionary.java  |
| https://www.World  | org/brotli/dec/Dictionary.java  |
| http://www.years  | org/brotli/dec/Dictionary.java  |
| http://interested  | org/brotli/dec/Dictionary.java  |
| http://familiar  | org/brotli/dec/Dictionary.java  |
| https://was  | org/brotli/dec/Dictionary.java  |
| https://aIn  | org/brotli/dec/Dictionary.java  |
| http://whether  | org/brotli/dec/Dictionary.java  |
| http://interpreted  | org/brotli/dec/Dictionary.java  |
| http://\  | org/brotli/dec/Dictionary.java  |
| http://);  | org/brotli/dec/Dictionary.java  |
| http://addEventListenerresponsible  | org/brotli/dec/Dictionary.java  |
| http://.jpg  | org/brotli/dec/Dictionary.java  |
| http://<a  | org/brotli/dec/Dictionary.java  |
| https://<div  | org/brotli/dec/Dictionary.java  |
| http://according  | org/brotli/dec/Dictionary.java  |
| http://www.interpretation  | org/brotli/dec/Dictionary.java  |
| http://s;text-align:centerfont-weight:  | org/brotli/dec/Dictionary.java  |
| http://html4/loose.dtd\  | org/brotli/dec/Dictionary.java  |
| http://style=\  | org/brotli/dec/Dictionary.java  |
| http://staticsuggested  | org/brotli/dec/Dictionary.java  |
| http://www.a  | org/brotli/dec/Dictionary.java  |
| http://An  | org/brotli/dec/Dictionary.java  |
| https://www.recent  | org/brotli/dec/Dictionary.java  |
| http://In  | org/brotli/dec/Dictionary.java  |
| http://www./div></div><div  | org/brotli/dec/Dictionary.java  |
| http://cript\  | org/brotli/dec/Dictionary.java  |
| http://\n<script  | org/brotli/dec/Dictionary.java  |
| http://www.wencodeURIComponent(\  | org/brotli/dec/Dictionary.java  |
| http://encoding=\  | org/brotli/dec/Dictionary.java  |
| http://www.icon\  | org/brotli/dec/Dictionary.java  |
| http://imEnglish  | org/brotli/dec/Dictionary.java  |
| http://i  | org/brotli/dec/Dictionary.java  |
| http://www.<li><a  | org/brotli/dec/Dictionary.java  |
| http://site\_name\  | org/brotli/dec/Dictionary.java  |
| http://www.hortcut  | org/brotli/dec/Dictionary.java  |
| http://</a></li><li  | org/brotli/dec/Dictionary.java  |
| http://<div  | org/brotli/dec/Dictionary.java  |
| http://iparticipation  | org/brotli/dec/Dictionary.java  |
| http://www.\  | org/brotli/dec/Dictionary.java  |
| http://www.w3.org/shortcut  | org/brotli/dec/Dictionary.java  |
| http://xt/css\  | org/brotli/dec/Dictionary.java  |
| http://link  | org/brotli/dec/Dictionary.java  |
| http://www.text-decoration:underthe  | org/brotli/dec/Dictionary.java  |
| http://option><option  | org/brotli/dec/Dictionary.java  |
| http://www</a><a  | org/brotli/dec/Dictionary.java  |
| http://w  | org/brotli/dec/Dictionary.java  |
| http://.css\  | org/brotli/dec/Dictionary.java  |
| http://www.style=\  | org/brotli/dec/Dictionary.java  |
| http://www.css\  | org/brotli/dec/Dictionary.java  |
| http://ator\  | org/brotli/dec/Dictionary.java  |
| http://www.language=\  | org/brotli/dec/Dictionary.java  |
| http://www-//W3C//DTD  | org/brotli/dec/Dictionary.java  |
| http://UA-Compatible\  | org/brotli/dec/Dictionary.java  |
| http://www.C//DTD  | org/brotli/dec/Dictionary.java  |
| http://www.  | org/brotli/dec/Dictionary.java  |
| http://undefined/  | org/jsoup/helper/HttpConnection.java  |
| https://isea-im-android.firebaseio.com  | Mogua Engine V1  |
| https://mediacloud-76607.gzc.vod.tencent-cloud.com/TencentEffect/demoMotion/encrypted\_motion/motion/  | Mogua Engine V2  |
| https://mediacloud-76607.gzc.vod.tencent-cloud.com/TencentEffect/demoMotion/encrypted\_motion/icon/  | Mogua Engine V2  |
| https://mediacloud-76607.gzc.vod.tencent-cloud.com/TencentEffect/demoMotion/encrypted\_lut/lut/  | Mogua Engine V2  |
| https://mediacloud-76607.gzc.vod.tencent-cloud.com/TencentEffect/demoMotion/encrypted\_lut/icon/  | Mogua Engine V2  |
| https://westus.api.cognitive.microsoft.com  | lib/arm64-v8a/libMicrosoft.CognitiveServices.Speech.core.so  |
| http://www.w3.org/2001/10/synthesis'  | lib/arm64-v8a/libMicrosoft.CognitiveServices.Speech.core.so  |
| http://www.w3.org/2001/mstts'  | lib/arm64-v8a/libMicrosoft.CognitiveServices.Speech.core.so  |
| http://www.w3.org/2009/10/emotionml'  | lib/arm64-v8a/libMicrosoft.CognitiveServices.Speech.core.so  |
| https://([^\.]+)\..+/issuetoken  | lib/arm64-v8a/libMicrosoft.CognitiveServices.Speech.core.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| xxx@email.elided  | com/tencent/liteav/base/PiiElider.java  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869184  | com/ksyun/media/player/KSYMediaMeta.java  |
| 14058229493  | com/tangxiaolv/telegramgallery/Utils/Utilities.java  |
| 18167426118  | Mogua Engine V2  |
| 18167426118  | Mogua Engine V2  |
| 18167426118  | Mogua Engine V2  |
| 18167426118  | Mogua Engine V2  |
| 18167426118  | Mogua Engine V2  |
| 18167426118  | Mogua Engine V2  |
| 18167426118  | Mogua Engine V2  |
| 18167426118  | Mogua Engine V2  |
| 18408203125  | Mogua Engine V2  |
| 13330078125  | Mogua Engine V2  |

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: CN=KingKr 签名算法: rsassa\_pkcs1v15 有效期自: 2018-06-07 07:05:07+00:00 有效期至: 2043-06-01 07:05:07+00:00 发行人: CN=KingKr 序列号: 0x6cd8a2d7 哈希算法: sha256 md5值: 504caf3c8671aded6d95f97f02bcde2a sha1值: 5c35e55b4e8123b6d258490d7ba7e4bb75c4c0e1 sha256值: fa8af58d0435bee4edc23219bb673204de0eab0ac8d957310a1d92584af2b010 sha512值: e7db054d39063b9465b13ed196e8ad8dfd5a019e50b8876e077bf484df2059fa57c9711909c9ab5ef9e1f8e45e534355d56fec9c8efaa8cbc80d228144d424e6 公钥算法: rsa 密钥长度: 2048 指纹: 79a903cf765557f35ec4d4d484313b8eea946129daabbbc556da6e41474bc4e1**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "auth\_login\_restore\_password" : "找回密码"  |
| "beauty\_lips3\_label" : "珊瑚橘"  |
| "beauty\_redcheeks3\_label" : "害羞"  |
| "check\_noauth\_tip" : "没有权限或资源缺失，若有疑问请请联系接口人咨询"  |
| "firebase\_database\_url" : "https://isea-im-android.firebaseio.com"  |
| "google\_api\_key" : "AIzaSyAI-gy6UwiPNpc6ix0vv6qypKXrYVhxUWE"  |
| "google\_crash\_reporting\_api\_key" : "AIzaSyAI-gy6UwiPNpc6ix0vv6qypKXrYVhxUWE"  |
| "goprivate\_room\_dialog\_level" : "等级限制"  |
| "goprivate\_room\_dialog\_pwd" : "密码进房"  |
| "goprivate\_room\_dialog\_ticket" : "收取金币"  |
| "goprivate\_room\_dialog\_time" : "计时收费"  |
| "goprivate\_room\_dialog\_title" : "私密直播中"  |
| "goprivate\_room\_level\_commit" : "我要升级"  |
| "goprivate\_room\_level\_commit2" : "确认入场"  |
| "goprivate\_room\_level\_fastup" : "是否希望快速升级？"  |
| "goprivate\_room\_level\_min" : "入场等级"  |
| "goprivate\_room\_my\_level" : "你当前的等级：%1$s"  |
| "goprivate\_room\_preview\_balance" : "使用推广奖励时间入场"  |
| "goprivate\_room\_preview\_time" : "免费试看"  |
| "goprivate\_room\_public\_room" : "公开直播"  |
| "goprivate\_room\_pwd\_commit" : "使用金币观看"  |
| "goprivate\_room\_pwd\_edit" : "请输入房间密码"  |
| "goprivate\_room\_ticket\_commit" : "使用金币入场"  |
| "goprivate\_room\_ticket\_money" : "门票价:"  |
| "goprivate\_room\_ticket\_nomoney" : "余额不足，快加钱吧"  |
| "goprivate\_room\_ticket\_recharge" : "我要充值"  |
| "goprivate\_room\_time\_commit" : "使用金币入场"  |
| "jmui\_username" : "用户名"  |
| "no\_such\_user" : "找不到使用者"  |
| "not\_auth" : "权限不足"  |
| "password" : "Password"  |
| "popup\_feel\_secret" : "保密"  |
| "room\_live\_eliminate\_user" : "你被管理员请出房间"  |
| "room\_private\_edit\_null" : "输入的内容怎么可以为空呢"  |
| "room\_private\_edit\_pwd" : "只能输入数字和字母哦"  |
| "room\_private\_level\_edit" : "请输入3位以内整数数字"  |
| "room\_private\_level\_title" : "请设置限制进入用户最小等级"  |
| "room\_private\_pwd\_edit" : "请输入6位字母数字,不区分大小写"  |
| "room\_private\_pwd\_title" : "设置房间密码"  |
| "room\_private\_ticket\_edit" : "请输入6位以内整数数字"  |
| "room\_private\_ticket\_title" : "请设置用户进入时收取的金币数额"  |
| "room\_private\_time\_edit" : "请输入5位以内整数数字"  |
| "room\_private\_time\_title" : "请设置每分钟收取的金币数额"  |
| "user" : "User"  |
| "password" : "Passwort"  |
| "user" : "Benutzer"  |
| "password" : "Paswoord"  |
| "user" : "Gebruiker"  |
| "password" : "Hasło"  |
| "user" : "Użytkownik"  |
| "password" : "Mot de passe"  |
| "user" : "Usager"  |
| "popup\_feel\_secret" : "Keep secret"  |
| "room\_live\_eliminate\_user" : "You have been kicked out by adminer"  |
| "popup\_feel\_secret" : "保密"  |
| "room\_live\_eliminate\_user" : "妳被管理員請出房間"  |
| "popup\_feel\_secret" : "Keep secret"  |
| "room\_live\_eliminate\_user" : "You have been kicked out by adminer"  |
| "popup\_feel\_secret" : "保密"  |
| "room\_live\_eliminate\_user" : "妳被管理員請出房間"  |
| "beauty\_lips3\_label" : "Coral"  |
| "beauty\_redcheeks3\_label" : "Shy"  |
| "check\_noauth\_tip" : "Insufficient permission or missing resources. If you have questions, please contact your sales rep."  |
| "not\_auth" : "Insufficient permission"  |
| "password" : "パスワード"  |
| "user" : "ユーザー"  |

## **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.RECEIVE\_USER\_PRESENT | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.WAKE\_LOCK | 正常 | 防止手机睡眠  | 允许应用程序防止手机进入睡眠状态 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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 |
| 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.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.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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.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.ACCESS\_LOCATION\_EXTRA\_COMMANDS | 正常 | 访问额外的位置提供程序命令 | 访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作 |
| android.permission.CHANGE\_NETWORK\_STATE | 正常 | 更改网络连接 | 允许应用程序更改网络连接状态。 |
| android.permission.CAMERA | 危险 | 拍照和录像 | 允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像 |
| android.permission.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| 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.SYSTEM\_OVERLAY\_WINDOW | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.REQUEST\_INSTALL\_PACKAGES | 危险 | 允许应用程序请求安装包。 | 恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。 |
| 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.BROADCAST\_STICKY | 正常 | 发送粘性广播 | 允许应用程序发送粘性广播,在广播结束后保留。恶意应用程序会导致手机使用过多内存,从而使手机运行缓慢或不稳定 |
| android.permission.READ\_LOGS | 危险 | 读取敏感日志数据 | 允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.REQUEST\_DELETE\_PACKAGES | 正常 |  | 允许应用程序请求删除包 |
| android.permission.READ\_MEDIA\_IMAGES | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_VIDEO | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_AUDIO | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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.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 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.qennnsad.aknkaksd.presentation.ui.MainContainerActivity | **Schemes**: live1975212://, **Hosts:** com.didi.live, **Paths:** /gameHall,  |
| com.im.freechat.ui.main.DeeplinkComponent | **Schemes**: https://, **Hosts:** inviter.testwebmessenger.ml, **Path Patterns:** /im/conversations/.\*,  |

**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。**