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

**None（ 0.6.1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 | None |
| 版本 | 0.6.1 |
| 包名 | com.bestplaceapps.sortup |
| 域名线索 | 109条 |
| URL线索 | 106条 |
| APP图标 |  |
| 分析日期 | 2025年8月27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 | base.apk |
| 文件大小 | 117.56MB |
| MD5值 | 944a786a2f7ab6463484d2131ddf9ad7 |
| SHA1值 | 82255729e1a6aab61ac01303e8f813504f5e909f |
| SHA256值 | 50cbc8ac4b03f0f10082ae867a439651d8d76f90e2ebe28d48d1f1ecbdb1687f |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | None |
| 包名 | com.bestplaceapps.sortup |
| 主活动Activity | com.unity3d.player.UnityPlayerActivity |
| 安卓版本名称 | 0.6.1 |
| 安卓版本 | 613 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| init-mp.fyber.com | IP: 34.49.219.143  所属国家: United States of America  地区: California  城市: Mountain View |
| p16-sign-sg.tiktokcdn.com | IP: 69.171.228.74  所属国家: United States of America  地区: California  城市: Menlo Park |
| xml.org | IP: 104.239.142.8  所属国家: United States of America  地区: Texas  城市: Windcrest |
| sregister.s | 没有服务器地理信息. |
| md.applvn.com | 没有服务器地理信息. |
| md.applovin.com | IP: 34.149.244.207  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| simpression.s | 没有服务器地理信息. |
| sonelink.s | 没有服务器地理信息. |
| market.android.com | IP: 142.250.73.78  所属国家: United States of America  地区: California  城市: Mountain View |
| sadrevenue.s | 没有服务器地理信息. |
| play.google.com | IP: 8.7.198.46  所属国家: United States of America  地区: Louisiana  城市: Monroe |
| d.applovin.com | IP: 34.110.179.88  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| ms.applovin.com | IP: 34.102.162.219  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| schemas.android.com | 没有服务器地理信息. |
| api16-endcard-pack-sg.pangle.io | IP: 23.218.94.205  所属国家: Australia  地区: New South Wales  城市: Sydney |
| b.applovin.com | IP: 35.241.1.16  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| scdn-stestsettings.s | 没有服务器地理信息. |
| config.safedk.com | 没有服务器地理信息. |
| applovin.com | IP: 141.193.213.10  所属国家: United States of America  地区: Texas  城市: Austin |
| smonitorsdk.s | 没有服务器地理信息. |
| www.applovin.com | IP: 141.193.213.11  所属国家: United States of America  地区: Texas  城市: Austin |
| svalidate.s | 没有服务器地理信息. |
| sars.s | 没有服务器地理信息. |
| monetization-support.applovin.com | IP: 34.110.151.135  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| dash.applovin.com | IP: 34.8.47.67  所属国家: United States of America  地区: California  城市: Mountain View |
| schemas.applovin.com | 没有服务器地理信息. |
| sviap.s | 没有服务器地理信息. |
| target.my.com | IP: 89.221.236.19  所属国家: Russian Federation  地区: Moskva  城市: Moscow |
| sinapps.s | 没有服务器地理信息. |
| xmlpull.org | IP: 185.199.111.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| appmetrica.io | IP: 213.180.204.242  所属国家: Russian Federation  地区: Moskva  城市: Moscow |
| adx.ads.vungle.com | IP: 23.23.224.14  所属国家: United States of America  地区: Virginia  城市: Ashburn |
| subscription.adjust.io | IP: 185.151.204.44  所属国家: Germany  地区: Berlin  城市: Berlin |
| analytics.us.tiktok.com | IP: 69.63.176.15  所属国家: United States of America  地区: California  城市: Menlo Park |
| lf-static.tiktokpangle-cdn-us.com | IP: 23.220.70.34  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| rt.applovin.com | IP: 34.117.147.68  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| ns.adobe.com | 没有服务器地理信息. |
| gdpr.s | 没有服务器地理信息. |
| gateway.unityads.unity3d.com | IP: 34.149.76.49  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| prod-a.applovin.comhttps | 没有服务器地理信息. |
| app.s | 没有服务器地理信息. |
| ssrv.adjust.io | IP: 185.151.204.1  所属国家: Germany  地区: Berlin  城市: Berlin |
| googleads.g.doubleclick.net | IP: 114.250.70.38  所属国家: China  地区: Beijing  城市: Beijing |
| www.amazon.com | IP: 18.164.167.27  所属国家: United States of America  地区: California  城市: Los Angeles |
| yandex.ru | IP: 77.88.55.88  所属国家: Russian Federation  地区: Moskva  城市: Moscow |
| www.example.com | IP: 23.56.227.78  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| rt.applvn.com | IP: 34.117.147.68  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| sts.applovin.com | IP: 34.111.80.193  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| sattr.s | 没有服务器地理信息. |
| events.ads.vungle.com | IP: 34.193.147.169  所属国家: United States of America  地区: Virginia  城市: Ashburn |
| aps-webhandler.appsflyer.com | IP: 13.226.210.103  所属国家: United States of America  地区: California  城市: Los Angeles |
| api16-access-sg.pangle.io | IP: 23.218.94.205  所属国家: Australia  地区: New South Wales  城市: Sydney |
| sconversions.s | 没有服务器地理信息. |
| ad.mail.ru | IP: 95.163.41.56  所属国家: Russian Federation  地区: Moskva  城市: Moscow |
| www.pangleglobal.com | IP: 23.218.94.222  所属国家: Australia  地区: New South Wales  城市: Sydney |
| www.w3.org | IP: 104.18.22.19  所属国家: United States of America  地区: California  城市: San Francisco |
| p.applov.in | IP: 34.8.47.67  所属国家: United States of America  地区: California  城市: Mountain View |
| backapi.rustore.ru | IP: 95.163.61.56  所属国家: Russian Federation  地区: Moskva  城市: Moscow |
| gist.github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| whatwg.org | IP: 165.227.248.76  所属国家: United States of America  地区: New Jersey  城市: Clifton |
| subscription.adjust.com | IP: 185.151.204.52  所属国家: Germany  地区: Berlin  城市: Berlin |
| slaunches.s | 没有服务器地理信息. |
| appgallery.cloud.huawei.com | IP: 49.4.35.16  所属国家: China  地区: Guangdong  城市: Guangzhou |
| scdn-ssettings.s | 没有服务器地理信息. |
| scar.unityads.unity3d.com | IP: 34.128.182.103  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| developer.apple.com | IP: 17.253.85.201  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| ssdk-services.s | 没有服务器地理信息. |
| appgallery.huawei.com | IP: 121.36.119.11  所属国家: China  地区: Beijing  城市: Beijing |
| a.applovin.com | IP: 34.117.147.68  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| compliance.iabtechnologylab.com | IP: 185.199.109.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| gdpr.adjust.io | IP: 185.151.204.1  所属国家: Germany  地区: Berlin  城市: Berlin |
| subscription.s | 没有服务器地理信息. |
| privacy.vungle.com | IP: 23.46.130.15  所属国家: Japan  地区: Osaka  城市: Osaka |
| a.applvn.com | IP: 34.117.147.68  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| api16-access-ttp.tiktokpangle.us | IP: 23.193.186.49  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| app.adjust.com | IP: 185.151.204.9  所属国家: Germany  地区: Berlin  城市: Berlin |
| assets.applovin.com | IP: 34.120.175.182  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| sf16-static.i18n-pglstatp.com | IP: 23.220.70.19  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| mobile.yandexadexchange.net | IP: 213.180.193.198  所属国家: Russian Federation  地区: Moskva  城市: Moscow |
| support.google.com | IP: 142.250.69.174  所属国家: United States of America  地区: California  城市: Mountain View |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| edge.safedk.com | IP: 34.120.33.51  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| ms.applvn.com | IP: 34.102.162.219  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| apps.rustore.ru | IP: 95.163.61.56  所属国家: Russian Federation  地区: Moskva  城市: Moscow |
| ssrv.adjust.com | IP: 185.151.204.2  所属国家: Germany  地区: Berlin  城市: Berlin |
| my.com | 没有服务器地理信息. |
| logs.ads.vungle.com | IP: 3.210.210.120  所属国家: United States of America  地区: Virginia  城市: Ashburn |
| gdpr.adjust.com | IP: 185.151.204.50  所属国家: Germany  地区: Berlin  城市: Berlin |
| config.ads.vungle.com | IP: 18.180.45.184  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| ssrv.s | 没有服务器地理信息. |
| vid.applovin.com | IP: 34.160.64.118  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| webview.unityads.unity3d.com | IP: 3.167.212.74  所属国家: United States of America  地区: Washington  城市: Seattle |
| schemas.microsoft.com | IP: 13.107.246.73  所属国家: United States of America  地区: Washington  城市: Redmond |
| www.fyber.com | IP: 151.101.91.52  所属国家: United States of America  地区: California  城市: San Francisco |
| cdn2.inner-active.mobi | IP: 151.101.91.52  所属国家: United States of America  地区: California  城市: San Francisco |
| www.youtube.com | IP: 142.250.217.110  所属国家: United States of America  地区: California  城市: Mountain View |
| www.samsungapps.com | IP: 52.31.24.56  所属国家: Ireland  地区: Dublin  城市: Dublin |
| sdlsdk.s | 没有服务器地理信息. |
| startup.mobile.yandex.net | IP: 213.180.204.244  所属国家: Russian Federation  地区: Moskva  城市: Moscow |
| sgcdsdk.s | 没有服务器地理信息. |
| d.applvn.com | IP: 34.110.179.88  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| www.googletagmanager.com | IP: 114.250.65.41  所属国家: China  地区: Beijing  城市: Beijing |
| exoplayer.dev | IP: 185.199.111.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| developer.android.com | IP: 142.250.69.174  所属国家: United States of America  地区: California  城市: Mountain View |
| sapp.s | 没有服务器地理信息. |
| svalidate-and-log.s | 没有服务器地理信息. |
| developers.applovin.com | IP: 34.160.22.255  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| app.adjust.io | IP: 185.151.204.1  所属国家: Germany  地区: Berlin  城市: Berlin |
| sf16-scmcdn-sg.ibytedtos.com | IP: 23.220.68.145  所属国家: Japan  地区: Tokyo  城市: Tokyo |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://app.adjust.com | com/adjust/sdk/Constants.java |
| https://app.%s | com/adjust/sdk/Constants.java |
| https://gdpr.adjust.com | com/adjust/sdk/Constants.java |
| https://gdpr.%s | com/adjust/sdk/Constants.java |
| https://ssrv.adjust.com | com/adjust/sdk/Constants.java |
| https://ssrv.%s | com/adjust/sdk/Constants.java |
| https://subscription.adjust.com | com/adjust/sdk/Constants.java |
| https://subscription.%s | com/adjust/sdk/Constants.java |
| https://github.com/adjust/android\_sdk | com/adjust/sdk/ActivityHandler.java |
| https://app.adjust.io | com/adjust/sdk/network/UrlStrategy.java |
| https://gdpr.adjust.io | com/adjust/sdk/network/UrlStrategy.java |
| https://ssrv.adjust.io | com/adjust/sdk/network/UrlStrategy.java |
| https://subscription.adjust.io | com/adjust/sdk/network/UrlStrategy.java |
| https://app. | com/adjust/sdk/network/UrlStrategy.java |
| https://gdpr. | com/adjust/sdk/network/UrlStrategy.java |
| https://ssrv. | com/adjust/sdk/network/UrlStrategy.java |
| https://subscription. | com/adjust/sdk/network/UrlStrategy.java |
| https://support.google.com/admob/answer/13554116 | com/applovin/impl/l6.java |
| https://applovin.com. | com/applovin/impl/c3.java |
| https://sts.applovin.com/v1/stats/sdk | com/applovin/impl/l4.java |
| https://prod-a.applovin.com,https://rt.applovin.com/4.0/pix, | com/applovin/impl/l4.java |
| https://rt.applvn.com/4.0/pix,https://ms.applovin.com/,https://ms.applvn.com/ | com/applovin/impl/l4.java |
| https://ms.applovin.com/ | com/applovin/impl/l4.java |
| https://ms.applvn.com/ | com/applovin/impl/l4.java |
| https://a.applovin.com/ | com/applovin/impl/l4.java |
| https://a.applvn.com/ | com/applovin/impl/l4.java |
| https://d.applovin.com/ | com/applovin/impl/l4.java |
| https://d.applvn.com/ | com/applovin/impl/l4.java |
| https://rt.applovin.com/ | com/applovin/impl/l4.java |
| https://rt.applvn.com/ | com/applovin/impl/l4.java |
| https://b.applovin.com/ | com/applovin/impl/l4.java |
| https://vid.applovin.com/,https://stage-vid.applovin.com/,https://pdn.applovin.com/,https://stage-pdn.applovin.com/,https://img.applovin.com/,https://stage-img.applovin.com/,https://d.applovin.com/,https://assets.applovin.com/,https://stage-assets.applovin.com/,https://cdnjs.cloudflare.com/,http://vid.applovin.com/,http://stage-vid.applovin.com/,http://pdn.applovin.com/,http://stage-pdn.applovin.com/,http://img.applovin.com/,http://stage-img.applovin.com/,http://d.applovin.com/,http://assets.applovin.com/,http://stage-assets.applovin.com/,http://cdnjs.cloudflare.com/,http://u.appl.vn/,https://u.appl.vn/,https://res.applovin.com/,https://res1.applovin.com/,https://res2.applovin.com/,https://res3.applovin.com/,http://res.applovin.com/,http://res1.applovin.com/,http://res2.applovin.com/,http://res3.applovin.com/ | com/applovin/impl/l4.java |
| https://developers.applovin.com/en/android/overview/terms-and-privacy-policy-flow | com/applovin/impl/l4.java |
| https://developers.applovin.com/en/unity/overview/terms-and-privacy-policy-flow | com/applovin/impl/l4.java |
| https://applovin.com | com/applovin/impl/l4.java |
| https://ms.applovin.com/ | com/applovin/impl/g3.java |
| https://ms.applvn.com/ | com/applovin/impl/g3.java |
| https://md.applovin.com/ | com/applovin/impl/g3.java |
| https://md.applvn.com/ | com/applovin/impl/g3.java |
| http://developer.android.com/google/play-services/setup.html. | com/applovin/impl/u.java |
| https://ms.applovin.com/1.0/sdk/error? | com/applovin/impl/z1.java |
| https://compliance.iabtechnologylab.com/compliance-js/omid-validation-verification-script-v1-APPLOVIN-01102024.js | com/applovin/impl/x3.java |
| https://play.google.com/store/apps/details?id= | com/applovin/impl/i5.java |
| https://developers.applovin.com/en/android/overview/integration | com/applovin/impl/x2.java |
| https://support.google.com/admob/answer/13554116 | com/applovin/impl/e3.java |
| https://developers.applovin.com/en/android/overview/terms-and-privacy-policy-flow | com/applovin/impl/e3.java |
| https://developers.applovin.com/en/android/overview/integration | com/applovin/impl/e3.java |
| https://dash.applovin.com/o/account?r=2 | com/applovin/impl/e3.java |
| https://developers.applovin.com/en/getting-started | com/applovin/impl/t5.java |
| https://monetization-support.applovin.com/hc/en-us/articles/236114328-How-can-I-expose-verbose-logging-for-the-SDK> | com/applovin/impl/q5.java |
| https://developers.applovin.com/en/android/overview/integration | com/applovin/impl/sdk/k.java |
| https://www.applovin.com/privacy/ | com/applovin/impl/sdk/nativeAd/AppLovinNativeAdImpl.java |
| https://assets.applovin.com/sound\_off.png | com/applovin/impl/sdk/ad/b.java |
| https://p.applov.in/ | com/applovin/impl/sdk/ad/b.java |
| https://assets.applovin.com/sound\_on.png | com/applovin/impl/sdk/ad/b.java |
| https://developers.applovin.com/en/max/android/overview/advanced-settings | com/applovin/impl/mediation/MediationServiceImpl.java |
| https://developers.applovin.com/en/max/android/ad-formats/banner-and-mrec-ads | com/applovin/impl/mediation/ads/MaxAdViewImpl.java |
| https://developers.applovin.com/en/android/overview/terms-and-privacy-policy-flow | com/applovin/impl/privacy/cmp/CmpServiceImpl.java |
| https://www.googletagmanager.com/gtag/js?id=<G-TRACKING\_ID>'></script><script>window.dataLayer | com/applovin/impl/adview/a.java |
| http://schemas.android.com/apk/res/android | com/applovin/mediation/ads/MaxAdView.java |
| http://schemas.applovin.com/android/1.0 | com/applovin/adview/AppLovinAdView.java |
| https://aps-webhandler.appsflyer.com/api/trigger | com/appsflyer/internal/AFj1xSDK.java |
| https://sf16-static.i18n-pglstatp.com/obj/ad-pattern-sg/static/images/ | com/bytedance/sdk/component/adexpress/dynamic/XM/YL.java |
| https://www.pangleglobal.com/ | com/bytedance/sdk/openadsdk/TTAdConstant.java |
| https://p16-sign-sg.tiktokcdn.com/v0201/fd71964ced204df586b63b9d8fa3198a | com/bytedance/sdk/openadsdk/component/reward/sLA.java |
| https://api16-endcard-pack-sg.pangle.io/union/endcard/1695802627329057/?rit=901121365&req\_id=68ebda22-9cbd-423f-98ce-78f571b6308bu5599&ad\_sdk\_version=3.6.0.0&os=android&lang=zh&union\_imei=702f89a658bd1f189c6e8e24587cd9ce&app\_version=%E8%A1%A5%E5%85%85%E4%B8%AD&app\_name=&developer\_name=%E8%A1%A5%E5%85%85%E4%B8%AD%EF%BC%8C%E5%8F%AF%E4%BA%8E%E5%BA%94%E7%94%A8%E5%AE%98%E7%BD%91%E6%9F%A5%E7%9C%8B&is\_dsp=False&lpt=1&style\_id=1535776&comment\_num=92&like\_num=109&share\_num=96\ | com/bytedance/sdk/openadsdk/component/reward/sLA.java |
| https://sf16-scmcdn-sg.ibytedtos.com/obj/goofy-sg/ad/pangle/homepage/\_next/static/assets/images/reward.c7cdf2f9.mp4\ | com/bytedance/sdk/openadsdk/component/reward/sLA.java |
| https://lf-static.tiktokpangle-cdn-us.com/obj/ad-pattern-tx/static/images/2023620white.jpeg | com/bytedance/sdk/openadsdk/core/yJi.java |
| https://lf-static.tiktokpangle-cdn-us.com/obj/ad-pattern-tx/3p\_monitor.9db44671.js | com/bytedance/sdk/openadsdk/core/settings/GbB.java |
| https://lf-static.tiktokpangle-cdn-us.com/obj/ad-pattern-tx/ | com/bytedance/sdk/openadsdk/core/settings/fU.java |
| https://lf-static.tiktokpangle-cdn-us.com/obj/ad-pattern-tx/ | com/bytedance/sdk/openadsdk/core/settings/vY.java |
| https://lf-static.tiktokpangle-cdn-us.com/obj/ad-pattern-tx/ | com/bytedance/sdk/openadsdk/core/settings/sLA.java |
| http://xmlpull.org/v1/doc/features.html | com/bytedance/sdk/openadsdk/core/tQ/YL/YL/XM.java |
| https://pag\_open\_icon\_id/appicon.png | com/bytedance/sdk/openadsdk/core/fU/YL/yJi.java |
| https://api16-access-sg.pangle.io/api/ad/union/sdk/get\_ads/?aid=1371&device\_platform=android&version\_code=4250 | com/bytedance/sdk/openadsdk/core/ZN/PoC.java |
| http://www.example.com | com/bytedance/sdk/openadsdk/core/act/YL.java |
| https://lf-static.tiktokpangle-cdn-us.com/obj/ad-pattern-tx/renderer/package\_tx.json | com/bytedance/sdk/openadsdk/utils/KOG.java |
| https://api16-access-ttp.tiktokpangle.us/service/2/app\_log/ | com/bytedance/sdk/openadsdk/utils/KOG.java |
| https://www.example.com | com/bytedance/sdk/openadsdk/utils/KOG.java |
| https://cdn2.inner-active.mobi/ia-sdk-config/features\_config.json | com/fyber/inneractive/sdk/config/global/m.java |
| https://cdn2.inner-active.mobi/ia-sdk-config/config\_android.json | com/fyber/inneractive/sdk/cache/d.java |
| https://cdn2.inner-active.mobi/client/ia-js-tags/dt-mraid-video-controller.js | com/fyber/inneractive/sdk/cache/j.java |
| https://cdn2.inner-active.mobi/IA-JSTag/Production/centering\_v1.css | com/fyber/inneractive/sdk/cache/j.java |
| https://cdn2.inner-active.mobi/IA-JSTag/Production/centering\_v1.js | com/fyber/inneractive/sdk/cache/j.java |
| https://cdn2.inner-active.mobi/client/ia-js-tags/playable\_detect.js | com/fyber/inneractive/sdk/cache/j.java |
| https://cdn2.inner-active.mobi/app-detail-page-v0/[BUNDLE\_ID].html | com/fyber/inneractive/sdk/flow/w.java |
| https://init-mp.fyber.com/init | com/fyber/inneractive/sdk/network/a0.java |
| http://www.fyber.com | com/fyber/inneractive/sdk/click/l.java |
| https://play.google.com/store/apps/details?id= | com/fyber/inneractive/sdk/click/e.java |
| https://cdn2.inner-active.mobi/client/ia-js-tags/omsdk/ | com/fyber/inneractive/sdk/measurement/e.java |
| https://cdn2.inner-active.mobi/client/ia-js-tags/omsdk/omid-session-client- | com/fyber/inneractive/sdk/measurement/e.java |
| https://cdn2.inner-active.mobi/client/ia-js-tags/omsdk/dt-omsdk-mraid-video-tracker.js | com/fyber/inneractive/sdk/measurement/e.java |
| https://cdn2.inner-active.mobi/client/ia-js-tags/dt-mraid-video-controller.js\ | com/fyber/inneractive/sdk/util/RunnableC0579d.java |
| https://cdn2.inner-active.mobi/IA-JSTag/Production/centering\_v1.css\ | com/fyber/inneractive/sdk/util/RunnableC0579d.java |
| https://cdn2.inner-active.mobi/IA-JSTag/Production/centering\_v1.js\ | com/fyber/inneractive/sdk/util/RunnableC0579d.java |
| http://xmlpull.org/v1/doc/features.html | com/fyber/inneractive/sdk/response/h.java |
| https://cdn2.inner-active.mobi/client/fyber-i-icon/index.html | com/fyber/inneractive/sdk/activities/FyberReportAdActivity.java |
| http://xmlpull.org/v1/doc/features.html | com/caverock/androidsvg/SVGParser.java |
| http://xml.org/sax/features/external-general-entities | com/caverock/androidsvg/SVGParser.java |
| http://xml.org/sax/features/external-parameter-entities | com/caverock/androidsvg/SVGParser.java |
| http://xml.org/sax/properties/lexical-handler | com/caverock/androidsvg/SVGParser.java |
| https://play.google.com/ | com/mbridge/msdk/foundation/tools/s0.java |
| https://play.google.com/store/apps/details?id= | com/mbridge/msdk/foundation/tools/s0.java |
| https://play.google.com/store/apps/details?id= | com/mbridge/msdk/foundation/webview/a.java |
| https://play.google.com/ | com/mbridge/msdk/click/a.java |
| https://play.google.com | com/mbridge/msdk/mbsignalcommon/windvane/WindVaneWebView.java |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense | com/mbridge/msdk/playercommon/exoplayer2/drm/HttpMediaDrmCallback.java |
| http://whatwg.org/html/common-microsyntaxes.html | com/mbridge/msdk/setting/util/b.java |
| http://whatwg.org/html/webappapis.html | com/mbridge/msdk/setting/util/b.java |
| https://gist.github.com/atk/1020396\n | com/mbridge/msdk/setting/util/b.java |
| http://whatwg.org/C | com/mbridge/msdk/setting/util/b.java |
| https://ad.mail.ru/sdk/log/ | com/my/target/p5.java |
| http://play.google.com | com/my/target/ib.java |
| https://play.google.com | com/my/target/ib.java |
| http://market.android.com | com/my/target/ib.java |
| https://market.android.com | com/my/target/ib.java |
| https://appgallery.huawei.com/ | com/my/target/ib.java |
| https://appgallery.cloud.huawei.com/ | com/my/target/ib.java |
| https://apps.rustore.ru | com/my/target/ib.java |
| https://backapi.rustore.ru | com/my/target/ib.java |
| https://ad.mail.ru/sdk/ms/ | com/my/target/g6.java |
| https://ad.mail.ru/sdk/log/v2 | com/my/target/k6.java |
| https://target.my.com/ | com/my/target/e2.java |
| https://ad.mail.ru/mobile/adcontext | com/my/target/i7.java |
| https://ad.mail.ru/ | com/my/target/j0.java |
| http://xmlpull.org/v1/doc/features.html | com/my/target/kb.java |
| https://ad.mail.ru/ | com/my/target/m6.java |
| https://my.com/? | com/my/tracker/obfuscated/n.java |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense | com/monetization/ads/exo/drm/o.java |
| https://x</LA\_URL> | com/monetization/ads/exo/drm/n.java |
| https://x | com/monetization/ads/exo/drm/n.java |
| https://developer.apple.com/streaming/emsg-id3 | com/monetization/ads/exo/metadata/emsg/EventMessage.java |
| https://config.safedk.com/ | com/safedk/android/SafeDK.java |
| https://edge.safedk.com | com/safedk/android/SafeDK.java |
| https://edge.safedk.com/v1/events | com/safedk/android/analytics/AppLovinBridge.java |
| https://edge.safedk.com/v1/image\_uploaded | com/safedk/android/analytics/AppLovinBridge.java |
| https://edge.safedk.com/v1/resolved | com/safedk/android/analytics/AppLovinBridge.java |
| https://edge.safedk.com/v1/file\_uploaded | com/safedk/android/analytics/AppLovinBridge.java |
| https://play.google.com/store/apps/details?id=%s | com/safedk/android/analytics/brandsafety/j.java |
| https://privacy.vungle.com/ | com/safedk/android/analytics/brandsafety/creatives/discoveries/s.java |
| https://googleads.g.doubleclick.net/dbm/ad?dbm\_c= | com/safedk/android/analytics/brandsafety/creatives/discoveries/a.java |
| https://googleads.g.doubleclick.net/xbbe/pixel?d | com/safedk/android/analytics/brandsafety/creatives/discoveries/a.java |
| https://edge.safedk.com | com/safedk/android/internal/d.java |
| https://webview.unityads.unity3d.com/webview/ | com/safedk/android/internal/SafeDKWebAppInterface.java |
| https://www\\.youtube\\.com/watch\\?v(\\\\x3d)(.\*?)(\\\\x26) | com/safedk/android/utils/g.java |
| http://play.google.com/store/apps/details?id= | com/safedk/android/utils/n.java |
| https://play.google.com/store/apps/details?id= | com/safedk/android/utils/n.java |
| https://www.youtube.com/watch?v= | com/safedk/android/utils/n.java |
| https://www.amazon.com/gp/mas/dl/android?p= | com/safedk/android/utils/n.java |
| https://www.samsungapps.com/appquery/appDetail.as?appId= | com/safedk/android/utils/n.java |
| https://www.youtube.com/watch?v=%s | com/safedk/android/utils/n.java |
| https://analytics.us.tiktok.com/api/v1/app\_sdk/config | com/tiktok/appevents/TTRequest.java |
| https://gateway.unityads.unity3d.com/v1 | com/unity3d/services/UnityAdsConstants.java |
| https://scar.unityads.unity3d.com/v1/capture-scar-signals | com/unity3d/services/ads/gmascar/utils/ScarConstants.java |
| https://adx.ads.vungle.com/api/ads | com/vungle/ads/internal/Constants.java |
| https://logs.ads.vungle.com/sdk/error\_logs | com/vungle/ads/internal/Constants.java |
| https://logs.ads.vungle.com/sdk/metrics | com/vungle/ads/internal/Constants.java |
| https://config.ads.vungle.com/ | com/vungle/ads/internal/network/VungleApiClient.java |
| https://events.ads.vungle.com/rtadebugging | com/vungle/ads/internal/load/RTADebugger.java |
| https://yandex.ru/dev/mobile-ads/doc/intro/changelog-android.html | com/yandex/mobile/ads/impl/gl.java |
| https://exoplayer.dev/issues/cleartext-not-permitted | com/yandex/mobile/ads/impl/ye0.java |
| https://yandex.ru/dev/mobile-ads/doc/android/quick-start/android-ads-component.html | com/yandex/mobile/ads/impl/e42.java |
| http://xmlpull.org/v1/doc/features.html | com/yandex/mobile/ads/impl/h52.java |
| https://mobile.yandexadexchange.net | com/yandex/mobile/ads/impl/g4.java |
| https://yandex.ru | com/yandex/mobile/ads/impl/wj.java |
| https://mobile.yandexadexchange.net | com/yandex/mobile/ads/impl/yw.java |
| http://xmlpull.org/v1/doc/features.html | com/yandex/mobile/ads/impl/sc2.java |
| https://yandex.ru/appcry | com/yandex/mobile/ads/impl/c.java |
| http://ns.adobe.com/xap/1.0/ | com/yandex/mobile/ads/impl/tn0.java |
| https://exoplayer.dev/issues/player-accessed-on-wrong-thread | com/yandex/mobile/ads/impl/f40.java |
| https://mobile.yandexadexchange.net | com/yandex/mobile/ads/impl/vc2.java |
| https://startup.mobile.yandex.net/ | io/appmetrica/analytics/BuildConfig.java |
| https://appmetrica.io/docs/mobile-sdk-dg/android/about/android-initialize.html | io/appmetrica/analytics/impl/C0729c0.java |

### **4.3 邮箱线索**

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869184 | com/applovin/impl/sdk/l.java |
| 17179869184 | com/caverock/androidsvg/SVGParser.java |
| 17179869184 | com/caverock/androidsvg/SVG.java |
| 17179869184 | com/caverock/androidsvg/SVGAndroidRenderer.java |

## **5. 签名证书**

**APK已签名 v1 签名: False 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=Google Inc., OU=Android, CN=Android 签名算法: rsassa\_pkcs1v15 有效期自: 2025-03-12 10:16:42+00:00 有效期至: 2055-03-12 10:16:42+00:00 发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android 序列号: 0xa6d7c02284bf47212893459cc102304043cf24e2 哈希算法: sha256 md5值: a77bb2d43ada12495eb024d7551d14e0 sha1值: 267d6b8334f0ea5f3adfeddba5175f1c15c6323c sha256值: 5c613cc83500be8802fa99fe67f465ab36e319ae7dbac54a9786b98b05cb3479 sha512值: 170300e6353a8df604911fae73ca90d4c94c323a720c87af5bb875e03e73ffb5d38dd503ec9a3324ca0628e28487678c48cd268dfa1ad1a259439a2735504dbb 公钥算法: rsa 密钥长度: 4096 指纹: fcf4d7ccdc10ee31dfc3d814bd817fb498410ec364524ef156e32416eebd156b**

## **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 |
| com.google.android.finsky.permission.BIND\_GET\_INSTALL\_REFERRER\_SERVICE | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.gms.permission.AD\_ID | 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.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 |
| com.applovin.array.apphub.permission.BIND\_APPHUB\_SERVICE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ACCESS\_ADSERVICES\_ATTRIBUTION | 未知 | Unknown permission | Unknown permission from android reference |
| com.huawei.appmarket.service.commondata.permission.GET\_COMMON\_DATA | 未知 | Unknown permission | Unknown permission from android reference |
| com.android.vending.BILLING | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ACCESS\_ADSERVICES\_TOPICS | 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.ACCESS\_ADSERVICES\_AD\_ID | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.c2dm.permission.RECEIVE | 合法 | C2DM 权限 | 云到设备消息传递的权限 |
| android.permission.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.providers.gsf.permission.READ\_GSERVICES | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| com.bestplaceapps.sortup.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| com.android.vending.CHECK\_LICENSE | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.google.firebase.auth.internal.GenericIdpActivity | **Schemes**: genericidp://,  **Hosts:** firebase.auth,  **Paths:** /, |
| com.google.firebase.auth.internal.RecaptchaActivity | **Schemes**: recaptcha://,  **Hosts:** firebase.auth,  **Paths:** /, |

**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。**