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

**Treasure Master（ 1.0.23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 | Treasure Master |
| 版本 | 1.0.23 |
| 包名 | com.gimica.treasuremaster |
| 域名线索 | 74条 |
| URL线索 | 77条 |
| APP图标 |  |
| 分析日期 | 2025年7月3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 | TreasureMaster.apk |
| 文件大小 | 67.83MB |
| MD5值 | 635ffac11094a22b67924d1dd914f456 |
| SHA1值 | adca5150997be360558563fa944bc31832cb0dda |
| SHA256值 | 0ec365c3507638583f155b64a2b82a3c993ef061c1c97740aedc5d1292ac7d68 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | Treasure Master |
| 包名 | com.gimica.treasuremaster |
| 主活动Activity | com.google.firebase.MessagingUnityPlayerActivity |
| 安卓版本名称 | 1.0.23 |
| 安卓版本 | 24 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| www.applovin.com | IP: 141.193.213.20 所属国家: United States of America 地区: Texas 城市: Austin  |
| edge.safedk.com | IP: 34.120.33.51 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| i.l.inmobicdn.net | IP: 205.185.216.42 所属国家: United States of America 地区: Texas 城市: Dallas  |
| assets.applovin.com | IP: 34.120.175.182 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| lazy.rayjump.com | IP: 59.110.124.183 所属国家: China 地区: Beijing 城市: Beijing  |
| adc3-launch-staging.adcolony.com | IP: 52.204.26.114 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| app.ssp.yahoo.com | IP: 107.22.26.74 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| issuetracker.google.com | IP: 172.217.163.46 所属国家: United States of America 地区: California 城市: Mountain View  |
| ms.applovin.com | IP: 34.102.162.219 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| developer.android.com | IP: 142.251.43.14 所属国家: United States of America 地区: California 城市: Mountain View  |
| d1tru86qrby720.cloudfront.net | IP: 108.138.255.43 所属国家: United States of America 地区: California 城市: San Francisco  |
| a.applvn.com | IP: 104.18.226.70 所属国家: United States of America 地区: California 城市: San Francisco  |
| d.applvn.com | IP: 104.18.226.70 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.example.com | IP: 93.184.216.34 所属国家: United States of America 地区: California 城市: Los Angeles  |
| play.google.com | IP: 142.251.42.238 所属国家: United States of America 地区: California 城市: Mountain View  |
| crash-metrics.sdk.inmobi.com | IP: 20.33.3.249 所属国家: United States of America 地区: Virginia 城市: Washington  |
| monetization-support.applovin.com | IP: 34.110.151.135 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| schemas.microsoft.com | IP: 13.107.213.74 所属国家: United States of America 地区: Washington 城市: Redmond  |
| config.safedk.com | 没有服务器地理信息.  |
| www.inmobi.com | IP: 20.81.69.107 所属国家: United States of America 地区: Virginia 城市: Washington  |
| gist.github.com | IP: 243.185.187.39 所属国家: - 地区: - 城市: -  |
| s3-us-west-2.amazonaws.com | IP: 52.92.229.192 所属国家: United States of America 地区: Oregon 城市: Boardman  |
| api.vungle.com | IP: 52.71.41.23 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| init.supersonicads.com | IP: 108.139.1.26 所属国家: United States of America 地区: California 城市: San Francisco  |
| unif-id.ssp.inmobi.com | IP: 20.39.58.118 所属国家: United States of America 地区: Virginia 城市: Washington  |
| ads.api.vungle.com | IP: 18.177.175.152 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| config.inmobi.com | 没有服务器地理信息.  |
| data.flurry.com | IP: 69.147.88.7 所属国家: United States of America 地区: New York 城市: New York City  |
| schemas.android.com | 没有服务器地理信息.  |
| policy.rayjump.com | IP: 59.110.124.183 所属国家: China 地区: Beijing 城市: Beijing  |
| yahoo.com | IP: 98.137.11.163 所属国家: United States of America 地区: New York 城市: New York City  |
| analytics.rayjump.com | IP: 123.56.168.170 所属国家: China 地区: Beijing 城市: Beijing  |
| luee-wally-v2-cpc.appspot.com | IP: 157.240.6.35 所属国家: Colombia 地区: Distrito Capital de Bogota 城市: Bogota  |
| vungle.com | IP: 141.193.213.11 所属国家: United States of America 地区: Texas 城市: Austin  |
| check.rayjump.com | IP: 59.110.124.183 所属国家: China 地区: Beijing 城市: Beijing  |
| outcome-arm-ext-med-ext.sonic-us.supersonicads.com | IP: 18.173.121.98 所属国家: United States of America 地区: California 城市: San Jose  |
| www.google.com | IP: 128.242.240.212 所属国家: United States of America 地区: Washington 城市: Redmond  |
| privacy.vungle.com | IP: 104.81.122.10 所属国家: Poland 地区: Mazowieckie 城市: Warsaw  |
| www.youtube.com | IP: 162.125.32.6 所属国家: United States of America 地区: California 城市: San Francisco  |
| xmlpull.org | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.yahoo.com | IP: 180.222.102.202 所属国家: Taiwan (Province of China) 地区: Taipei 城市: Taipei  |
| a.applovin.com | IP: 34.117.147.68 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| outcome-crash-report.supersonicads.com | IP: 18.155.202.115 所属国家: United States of America 地区: California 城市: San Francisco  |
| webview.unityads.unity3d.com | IP: 23.45.232.49 所属国家: Malaysia 地区: Wilayah Persekutuan Kuala Lumpur 城市: Kuala Lumpur  |
| d.applovin.com | IP: 34.110.179.88 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| recommends.yahoo.com | IP: 74.6.160.106 所属国家: United States of America 地区: New York 城市: New York City  |
| net.rayjump.com | IP: 39.107.225.241 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| adc-ad-assets.adtilt.com | IP: 23.45.51.26 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| whatwg.org | IP: 165.227.248.76 所属国家: United States of America 地区: New Jersey 城市: Clifton  |
| vid.applovin.com | IP: 34.160.64.118 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| rt.applvn.com | IP: 104.17.6.24 所属国家: United States of America 地区: California 城市: San Francisco  |
| ads.inmobi.com | 没有服务器地理信息.  |
| telemetry.sdk.inmobi.com | IP: 52.186.42.194 所属国家: United States of America 地区: Virginia 城市: Washington  |
| wd.adcolony.com | IP: 44.218.116.84 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| cfg.flurry.com | IP: 98.136.147.20 所属国家: United States of America 地区: New York 城市: New York City  |
| api.login.yahoo.com | IP: 74.6.160.138 所属国家: United States of America 地区: New York 城市: New York City  |
| schemas.applovin.com | 没有服务器地理信息.  |
| detect.rayjump.com | IP: 52.86.37.78 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| outcome-ssp.supersonicads.com | IP: 13.227.74.123 所属国家: United States of America 地区: California 城市: San Francisco  |
| prod-a.applovin.comhttps | 没有服务器地理信息.  |
| adc3-launch.adcolony.com | IP: 34.36.45.50 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| cdn-adn-https.rayjump.com | IP: 103.254.188.50 所属国家: China 地区: Beijing 城市: Beijing  |
| vastproxy.brand.inmobi.com | IP: 20.39.59.133 所属国家: United States of America 地区: Virginia 城市: Washington  |
| www.amazon.com | IP: 162.219.225.118 所属国家: United States of America 地区: Washington 城市: Seattle  |
| mtg-native.rayjump.com | IP: 42.81.61.107 所属国家: China 地区: Tianjin 城市: Tianjin  |
| ads.nexage.com | IP: 107.22.26.74 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| rt.applovin.com | IP: 34.117.147.68 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| configure.rayjump.com | IP: 59.110.124.183 所属国家: China 地区: Beijing 城市: Beijing  |
| www.samsungapps.com | IP: 52.31.24.56 所属国家: Ireland 地区: Dublin 城市: Dublin  |
| www.fyber.com | IP: 141.193.213.20 所属国家: United States of America 地区: Texas 城市: Austin  |
| api.ads.yahoo.com | IP: 69.147.88.7 所属国家: United States of America 地区: New York 城市: New York City  |
| cdn2.inner-active.mobi | IP: 23.45.51.26 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| ms.applvn.com | IP: 104.18.226.70 所属国家: United States of America 地区: California 城市: San Francisco  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://adc3-launch.adcolony.com/v4/launch  | com/adcolony/sdk/k.java  |
| https://wd.adcolony.com/logs  | com/adcolony/sdk/g0.java  |
| https://adc3-launch-staging.adcolony.com/v4/launch  | com/adcolony/sdk/AdColonyAppOptions.java  |
| https://adc-ad-assets.adtilt.com/launch/\_\_controllers\_\_/4.0.0/controller.js\  | com/adcolony/adcolonysdk/BuildConfig.java  |
| https://adc-ad-assets.adtilt.com/launch/\_\_libs\_\_/omsdk/omsdk-v1.js\  | com/adcolony/adcolonysdk/BuildConfig.java  |
| https://adc3-launch.adcolony.com/v4/launch  | com/adcolony/adcolonysdk/BuildConfig.java  |
| http://schemas.android.com/apk/lib/com.inmobi.ads  | com/inmobi/ads/InMobiBanner.java  |
| http://www.google.com  | com/inmobi/media/h.java  |
| https://unif-id.ssp.inmobi.com/fetch  | com/inmobi/media/gh.java  |
| https://config.inmobi.com/config-server/v1/config/secure.cfg  | com/inmobi/media/gg.java  |
| https://crash-metrics.sdk.inmobi.com/trace  | com/inmobi/media/gd.java  |
| http://\  | com/inmobi/media/q.java  |
| https://\  | com/inmobi/media/q.java  |
| https://ads.inmobi.com/sdk  | com/inmobi/media/ft.java  |
| https://i.l.inmobicdn.net/sdk/sdk/500/android/mraid.js  | com/inmobi/media/ft.java  |
| https://i.l.inmobicdn.net/sdk/sdk/OMID/omsdk-v1.3.17.js  | com/inmobi/media/ft.java  |
| https://www.inmobi.com/products/sdk/  | com/inmobi/media/hx.java  |
| https://config.inmobi.com/config-server/v1/config/secure.cfg  | com/inmobi/media/ga.java  |
| https://telemetry.sdk.inmobi.com/metrics  | com/inmobi/media/gi.java  |
| https://config.safedk.com/  | com/safedk/android/SafeDK.java  |
| https://edge.safedk.com  | com/safedk/android/SafeDK.java  |
| https://www.youtube.com/watch?v=  | com/safedk/android/utils/j.java  |
| https://play.google.com/store/apps/details?id=  | com/safedk/android/utils/j.java  |
| https://www.amazon.com/gp/mas/dl/android?p=  | com/safedk/android/utils/j.java  |
| https://www.samsungapps.com/appquery/appDetail.as?appId=  | com/safedk/android/utils/j.java  |
| http://play.google.com/store/apps/details?id=  | com/safedk/android/utils/j.java  |
| https://www.youtube.com/watch?v=%s  | com/safedk/android/utils/j.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://dummyurl  | com/safedk/android/analytics/brandsafety/InterstitialFinder.java  |
| https://play.google.com/store/apps/details?id=%s  | com/safedk/android/analytics/brandsafety/f.java  |
| https://privacy.vungle.com/  | com/safedk/android/analytics/brandsafety/creatives/discoveries/k.java  |
| http://vastproxy.brand.inmobi.com/g/  | com/safedk/android/analytics/brandsafety/creatives/discoveries/e.java  |
| https://www\\.youtube\\.com/watch\\?v(\\\\x3d)(.\*?)(\\\\x26)  | com/safedk/android/analytics/brandsafety/creatives/discoveries/b.java  |
| https://webview.unityads.unity3d.com/webview/  | com/safedk/android/internal/SafeDKWebAppInterface.java  |
| https://edge.safedk.com  | com/safedk/android/internal/d.java  |
| https://ads.api.vungle.com/  | com/vungle/warren/VungleApiClient.java  |
| https://api.vungle.com/  | com/vungle/warren/VungleApiClient.java  |
| https://vungle.com/privacy/  | com/vungle/warren/ui/presenter/LocalAdPresenter.java  |
| https://cdn2.inner-active.mobi/client/ia-js-tags/omsdk/%s.js  | com/fyber/inneractive/sdk/measurement/d.java  |
| http://xmlpull.org/v1/doc/features.html  | com/fyber/inneractive/sdk/response/h.java  |
| http://www.fyber.com  | com/fyber/inneractive/sdk/util/d0.java  |
| https://cdn2.inner-active.mobi/client/ia-js-tags/MRAID-VIDEO.js  | com/fyber/inneractive/sdk/cache/g.java  |
| https://cdn2.inner-active.mobi/IA-JSTag/Production/centering\_v1.css  | com/fyber/inneractive/sdk/cache/g.java  |
| https://cdn2.inner-active.mobi/IA-JSTag/Production/centering\_v1.js  | com/fyber/inneractive/sdk/cache/g.java  |
| https://cdn2.inner-active.mobi/client/ia-js-tags/MRAID-VIDEO.js\  | com/fyber/inneractive/sdk/web/a.java  |
| https://cdn2.inner-active.mobi/IA-JSTag/Production/centering\_v1.css\  | com/fyber/inneractive/sdk/web/a.java  |
| https://cdn2.inner-active.mobi/IA-JSTag/Production/centering\_v1.js\  | com/fyber/inneractive/sdk/web/a.java  |
| https://cfg.flurry.com/sdk/v1/config  | com/flurry/sdk/by.java  |
| http://www.example.com  | com/flurry/sdk/ed.java  |
| https://data.flurry.com/v1/flr.do  | com/flurry/sdk/br.java  |
| https://cfg.flurry.com/sdk/v1/config  | com/flurry/sdk/cl.java  |
| https://api.login.yahoo.com/oauth2/device\_session  | com/flurry/sdk/ef.java  |
| http://schemas.applovin.com/android/1.0  | com/applovin/adview/AppLovinAdView.java  |
| http://developer.android.com/google/play-services/setup.html.  | com/applovin/impl/sdk/utils/c.java  |
| https://ms.applovin.com/  | com/applovin/impl/sdk/c/a.java  |
| https://ms.applvn.com/  | com/applovin/impl/sdk/c/a.java  |
| https://prod-a.applovin.com,https://rt.applovin.com/4.0/pix,  | com/applovin/impl/sdk/c/b.java  |
| https://rt.applvn.com/4.0/pix,https://ms.applovin.com/,https://ms.applvn.com/  | com/applovin/impl/sdk/c/b.java  |
| https://ms.applovin.com/  | com/applovin/impl/sdk/c/b.java  |
| https://ms.applvn.com/  | com/applovin/impl/sdk/c/b.java  |
| https://a.applovin.com/  | com/applovin/impl/sdk/c/b.java  |
| https://a.applvn.com/  | com/applovin/impl/sdk/c/b.java  |
| https://d.applovin.com/  | com/applovin/impl/sdk/c/b.java  |
| https://d.applvn.com/  | com/applovin/impl/sdk/c/b.java  |
| https://rt.applovin.com/  | com/applovin/impl/sdk/c/b.java  |
| https://rt.applvn.com/  | com/applovin/impl/sdk/c/b.java  |
| https://ms.applovin.com/1.0/sdk/error  | com/applovin/impl/sdk/c/b.java  |
| https://assets.applovin.com/gdpr/flow\_v1/gdpr-flow-1.html  | com/applovin/impl/sdk/c/b.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/sdk/c/b.java  |
| https://www.applovin.com/privacy/  | com/applovin/impl/sdk/nativeAd/e.java  |
| https://monetization-support.applovin.com/hc/en-us/articles/236114328-How-can-I-expose-verbose-logging-for-the-SDK>  | com/applovin/impl/sdk/e/n.java  |
| https://applovin.com.  | com/applovin/impl/mediation/debugger/ui/b/a.java  |
| https://developer.android.com/training/articles/security-config  | com/applovin/impl/mediation/debugger/b/b/c.java  |
| http://schemas.android.com/apk/res/android  | com/applovin/mediation/ads/MaxAdView.java  |
| https://cdn-adn-https.rayjump.com/cdn-adn/v2/portal/19/08/20/11/06/5d5b63cb457e2.js  | com/mbridge/msdk/c/b.java  |
| https://mtg-native.rayjump.com/omsdk/omsdkjs\_common\_js.txt  | com/mbridge/msdk/c/b.java  |
| http://whatwg.org/html/common-microsyntaxes.html  | com/mbridge/msdk/c/b/b.java  |
| http://whatwg.org/html/webappapis.html  | com/mbridge/msdk/c/b/b.java  |
| https://gist.github.com/atk/1020396\n  | com/mbridge/msdk/c/b/b.java  |
| http://whatwg.org/C  | com/mbridge/msdk/c/b/b.java  |
| https://play.google.com/  | com/mbridge/msdk/click/a.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://mtg-native.rayjump.com/omsdk/omsdkjs\_common\_js.txt  | com/mbridge/msdk/foundation/controller/b.java  |
| https://analytics.rayjump.com  | com/mbridge/msdk/foundation/same/net/f/d.java  |
| https://net.rayjump.com  | com/mbridge/msdk/foundation/same/net/f/d.java  |
| https://configure.rayjump.com  | com/mbridge/msdk/foundation/same/net/f/d.java  |
| https://detect.rayjump.com/mapi/find  | com/mbridge/msdk/foundation/same/net/f/d.java  |
| https://detect.rayjump.com/mapi/result  | com/mbridge/msdk/foundation/same/net/f/d.java  |
| https://d1tru86qrby720.cloudfront.net/hostsetting  | com/mbridge/msdk/foundation/same/net/f/d.java  |
| https://policy.rayjump.com  | com/mbridge/msdk/foundation/same/net/f/d.java  |
| https://lazy.rayjump.com  | com/mbridge/msdk/foundation/same/net/f/d.java  |
| https://check.rayjump.com  | com/mbridge/msdk/foundation/same/net/f/d.java  |
| https://play.google.com/store/apps/details?id=  | com/mbridge/msdk/foundation/tools/x.java  |
| https://play.google.com/  | com/mbridge/msdk/foundation/tools/x.java  |
| https://play.google.com  | com/mbridge/msdk/mbsignalcommon/windvane/WindVaneWebView.java  |
| https://s3-us-west-2.amazonaws.com/omsdk-files/compliance-js/omid-validation-verification-script-v1.js  | com/mbridge/msdk/a/b.java  |
| https://api.ads.yahoo.com/geo/v1/user/location/current  | com/yahoo/ads/YASAds.java  |
| http://yahoo.com/ads  | com/yahoo/ads/VideoPlayerView.java  |
| http://www.yahoo.com  | com/yahoo/ads/EnvironmentInfo.java  |
| https://app.ssp.yahoo.com  | com/yahoo/ads/yahoosspwaterfallprovider/YahooSSPWaterfallProvider.java  |
| https://app.ssp.yahoo.com  | com/yahoo/ads/yahoosspreporter/YahooSSPReporter.java  |
| https://issuetracker.google.com/issues/68454482  | com/yahoo/ads/support/utils/ViewUtils.java  |
| http://xmlpull.org/v1/doc/features.html  | com/yahoo/ads/vastcontroller/VASTParser.java  |
| https://app.ssp.yahoo.com  | com/yahoo/ads/yahoosspconfigprovider/YahooSSPConfigProvider.java  |
| https://recommends.yahoo.com  | com/yahoo/ads/recommendscontrol/RecommendsControl$loadWebView$2.java  |
| http://ads.nexage.com  | com/yahoo/ads/webview/YASAdsWebView.java  |
| https://luee-wally-v2-cpc.appspot.com/gdpr\_consent\_games.html?package\_name=  | com/sba/unitypluginsharing/GDPRConsent.java  |
| https://outcome-crash-report.supersonicads.com/reporter  | com/ironsource/environment/e.java  |
| https://outcome-ssp.supersonicads.com/mediation?adUnit=3  | com/ironsource/mediationsdk/utils/j.java  |
| https://outcome-arm-ext-med-ext.sonic-us.supersonicads.com/aemData  | com/ironsource/mediationsdk/utils/b.java  |
| https://outcome-ssp.supersonicads.com/mediation?adUnit=3  | com/ironsource/mediationsdk/utils/l.java  |
| https://outcome-arm-ext-med-ext.sonic-us.supersonicads.com/aemData  | com/ironsource/mediationsdk/utils/l.java  |
| https://init.supersonicads.com/sdk/v  | com/ironsource/mediationsdk/server/ServerURL.java  |
| https://outcome-arm-ext-med-ext.sonic-us.supersonicads.com/aemData  | com/ironsource/mediationsdk/impressionData/a.java  |
| https://outcome-ssp.supersonicads.com/mediation?adUnit=2  | com/ironsource/mediationsdk/a/e.java  |
| https://outcome-ssp.supersonicads.com/mediation?adUnit=3  | com/ironsource/mediationsdk/a/f.java  |

### **4.3 邮箱线索**

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17222222222  | com/fyber/inneractive/sdk/player/exoplayer2/extractor/mkv/a.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=Google Inc., OU=Android, CN=Android 签名算法: rsassa\_pkcs1v15 有效期自: 2021-11-16 15:39:20+00:00 有效期至: 2051-11-16 15:39:20+00:00 发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android 序列号: 0x8b87dbd2ad55f638ea4b308d40b99c9c7c83a366 哈希算法: sha256 md5值: 69cd6249c4f3453ee99668b61fd1739d sha1值: 7d4225f54cf920125ba0aa09aa6c4dd0959e6cb4 sha256值: 9ec8d76e226e115e92e6528d9026b37da4df4f72372735a5a2d423aa28b3ee81 sha512值: 7abded1effaf87938ee965f4f369961bbda78bd4030bc1e602573f054d4b724c68dbe5a6d0b793dd9cc9c9d47cbbab5f3adefb1a06669c126f4aaa7243ca6daa 公钥算法: rsa 密钥长度: 4096 指纹: 899d14e3982795d5912d9a23117f87ebd165ccc98fc88aa1d374920b53d683b2**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "com.google.firebase.crashlytics.unity\_version" : "2020.3.33f1"  |
| "com\_facebook\_device\_auth\_instructions" : "Visit <b>facebook.com/device</b> and enter the code shown above."  |
| "google\_api\_key" : "AIzaSyDlmJQ5l8y-gdwCkOc-mAy2UjHsrB078QI"  |
| "google\_crash\_reporting\_api\_key" : "AIzaSyDlmJQ5l8y-gdwCkOc-mAy2UjHsrB078QI"  |
| "com\_facebook\_device\_auth\_instructions" : "Gå til <b>facebook.com/device</b> og indtast koden, som er vist ovenfor."  |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b>にアクセスして、上のコードを入力してください。"  |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> 'ਤੇ ਵਿਜਿਟ ਕਰੋ ਅਤੇ ਉੱਪਰ ਦਿੱਤੇ ਕੋਡ ਨੂੰ ਦਾਖ਼ਲ ਕਰੋ।"  |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> ஐப் பார்வையிட்டு, மேலே காட்டப்பட்ட குறியீட்டை உள்ளிடவும்."  |
| "com\_facebook\_device\_auth\_instructions" : "Gå til <b>facebook.com/device</b> og skriv inn koden som vises over."  |
| "com\_facebook\_device\_auth\_instructions" : "Gehe zu <b>facebook.com/device</b> und gib den oben angezeigten Code ein."  |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b>ని సందర్శించి ఎగువన చూపిన కోడ్‌ను నమోదు చేయండి."  |
| "com\_facebook\_device\_auth\_instructions" : "Besoek <b>facebook.com/device</b> en voer die kode wat hierbo gewys word, in."  |
| "com\_facebook\_device\_auth\_instructions" : "ไปที่ <b>facebook.com/device</b> แล้วป้อนรหัสที่ปรากฏด้านล่าง"  |
| "com\_facebook\_device\_auth\_instructions" : "Siirry osoitteeseen <b>facebook.com/device</b> ja anna oheinen koodi."  |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> पर विज़िट करें और ऊपर दिखाया गया कोड डालें."  |
| "com\_facebook\_device\_auth\_instructions" : "Truy cập <b>facebook.com/device</b> và nhập mã được hiển thị bên trên."  |
| "com\_facebook\_device\_auth\_instructions" : "Navštívte stránku <b>facebook.com/device</b> a zadajte kód zobrazený vyššie."  |
| "com\_facebook\_device\_auth\_instructions" : "Πηγαίνετε στη διεύθυνση <b>facebook.com/device</b> και εισαγάγετε τον παραπάνω κωδικό."  |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> സന്ദർശിച്ച് മുകളിൽ കാണിച്ചിരിക്കുന്ന കോഡ് നൽകുക."  |
| "com\_facebook\_device\_auth\_instructions" : "Ga naar <b>facebook.com/device</b> en voer de bovenstaande code in."  |
| "com\_facebook\_device\_auth\_instructions" : "Odwiedź stronę <b>facebook.com/device</b> i wprowadź powyższy kod."  |
| "com\_facebook\_device\_auth\_instructions" : "Puntahan ang <b>facebook.com/device</b> at ilagay ang code na ipinapakita sa itaas."  |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> দেখুন এবং উপরে দেখানো কোডটিকে প্রবেশ করান৷"  |
| "com\_facebook\_device\_auth\_instructions" : "Kunjungi <b>facebook.com/device</b> dan masukkan kode yang ditampilkan di bawah ini."  |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> ಗೆ ಭೇಟಿ ನೀಡಿ ಮತ್ತು ಮೇಲೆ ತೋರಿಸಿದ ಕೋಡ್ ಅನ್ನು ನಮೂದಿಸಿ."  |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b>에 방문하여 위 코드를 입력하세요."  |
| "com\_facebook\_device\_auth\_instructions" : "Vizitează <b>facebook.com/device</b> şi introdu codul de mai sus."  |
| "com\_facebook\_device\_auth\_instructions" : "تفضل بزيارة <b>facebook.com/device</b> وإدخال الرمز الموضح أعلاه."  |
| "com\_facebook\_device\_auth\_instructions" : "Consultez <b>facebook.com/device</b> et entrez le code affiché ci-dessus."  |
| "com\_facebook\_device\_auth\_instructions" : "Posjetitw <b>facebook.com/device</b> i unesite gore prikazani kôd."  |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> भेट द्या आणि वरील कोड प्रविष्ट करा."  |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> adresine git ve yukarıda gösterilen kodu gir."  |
| "com\_facebook\_device\_auth\_instructions" : "Přejděte na <b>facebook.com/device</b> a zadejte nahoře uvedený kód."  |
| "com\_facebook\_device\_auth\_instructions" : "Ve a <b>facebook.com/device</b> e ingresa el código que se muestra arriba."  |
| "com\_facebook\_device\_auth\_instructions" : "Lawati <b>facebook.com/device</b> dan masukkan kod yang ditunjukkan di atas."  |
| "com\_facebook\_device\_auth\_instructions" : "Visita <b>facebook.com/device</b> e inserisci il codice mostrato qui sotto."  |
| "com\_facebook\_device\_auth\_instructions" : "Acesse <b>facebook.com/device</b> e insira o código mostrado acima."  |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b&gt પર જાઓ અને ઉપર બતાવેલો કોડ દાખલ કરો."  |
| "com\_facebook\_device\_auth\_instructions" : "Keresd fel a <b>facebook.com/device</b> címet, és írd be a fent megjelenített kódot."  |
| "com\_facebook\_device\_auth\_instructions" : "Откройте <b>facebook.com/device</b> и введите код, показанный выше."  |
| "com\_facebook\_device\_auth\_instructions" : "Gå till <b>facebook.com/device</b> och skriv in koden som visas ovan."  |
| "com\_facebook\_device\_auth\_instructions" : "יש לבקר בכתובת facebook.com/device</b&gt ולהזין את הקוד המוצג למעלה."  |
| "com\_facebook\_device\_auth\_instructions" : "Accédez à <b>facebook.com/device</b> et entrez le code affiché ci-dessus."  |
| "com\_facebook\_device\_auth\_instructions" : "前往<b>facebook.com/device</b&gt，並輸入上方顯示的代碼。"  |
| "com\_facebook\_device\_auth\_instructions" : "请访问<b>facebook.com/device</b>并输入以上验证码。"  |
| "com\_facebook\_device\_auth\_instructions" : "Visita <b>facebook.com/device</b> e insere o código apresentado abaixo."  |
| "com\_facebook\_device\_auth\_instructions" : "前往<b>facebook.com/device</b&gt，並輸入上方顯示的代碼。"  |
| "com\_facebook\_device\_auth\_instructions" : "Kunjungi <b>facebook.com/device</b> dan masukkan kode yang ditampilkan di atas."  |
| "com\_facebook\_device\_auth\_instructions" : "Visita <b>facebook.com/device</b> e introduce el código que se muestra más arriba."  |

## **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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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.RECEIVE\_BOOT\_COMPLETED | 正常 | 开机时自动启动 | 允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度 |
| android.permission.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.google.android.gms.permission.AD\_ID | 未知 | Unknown permission | Unknown permission from android reference |
| 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.POST\_NOTIFICATIONS | 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 |
| com.google.android.c2dm.permission.RECEIVE | 合法 | C2DM 权限 | 云到设备消息传递的权限 |
| com.google.android.finsky.permission.BIND\_GET\_INSTALL\_REFERRER\_SERVICE | 未知 | Unknown permission | Unknown permission from android reference |
| com.gimica.treasuremaster.permission.C2D\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.android.vending.BILLING | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.facebook.CustomTabActivity | **Schemes**: fbconnect://, **Hosts:** cct.com.gimica.treasuremaster,  |

**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。**