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

**英魂传说（ 1.1.9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 | 英魂传说 |
| 版本 | 1.1.9 |
| 包名 | com.jyj.codex |
| 域名线索 | 56条 |
| URL线索 | 56条 |
| APP图标 |  |
| 分析日期 | 2025年7月22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 | codex1.1.9.apk |
| 文件大小 | 173.33MB |
| MD5值 | 5802a3d8d02f241d5479f3b2aaf0165f |
| SHA1值 | 5c6d391af5a28c7e9a95dfa64aa7975e3c85ebec |
| SHA256值 | c14a5a00b8fd277933e59e8df10acaefd0368a273b576b7f35e6b5a9df44ef8e |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 英魂传说 |
| 包名 | com.jyj.codex |
| 主活动Activity | org.cocos2dx.javascript.AppActivity |
| 安卓版本名称 | 1.1.9 |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| www.apple.com | IP: 27.148.139.136 所属国家: China 地区: Fujian 城市: Fuzhou  |
| mobilegw.alipaydev.com | IP: 110.75.132.131 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| loggw-exsdk.alipay.com | IP: 110.76.6.82 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| h5.m.taobao.com | IP: 125.38.11.131 所属国家: China 地区: Tianjin 城市: Tianjin  |
| configure.rayjump.com | IP: 112.126.23.181 所属国家: China 地区: Beijing 城市: Beijing  |
| mobilegw.alipay.com | IP: 203.209.250.2 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| open.e.kuaishou.com | IP: 116.136.202.194 所属国家: China 地区: Nei Mongol 城市: Hohhot  |
| crbug.com | IP: 216.239.32.29 所属国家: United States of America 地区: California 城市: Mountain View  |
| whatwg.org | IP: 165.227.248.76 所属国家: United States of America 地区: New Jersey 城市: Clifton  |
| apps.samsung.com | IP: 104.17.142.17 所属国家: United States of America 地区: California 城市: San Francisco  |
| mobilegwpre.alipay.com | IP: 110.75.138.35 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| long.open.weixin.qq.com | IP: 112.65.193.170 所属国家: China 地区: Shanghai 城市: Shanghai  |
| eligrey.com | IP: 104.236.163.66 所属国家: United States of America 地区: California 城市: San Francisco  |
| xmlpull.org | IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| schemas.microsoft.com | IP: 13.107.246.73 所属国家: United States of America 地区: Washington 城市: Redmond  |
| mclient.alipay.com | IP: 116.142.234.199 所属国家: China 地区: Beijing 城市: Beijing  |
| mobilegw.dl.alipaydev.com | IP: 110.75.132.25 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| pitk.birdgesdk.com | IP: 39.108.103.199 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| mores.toponad.com | IP: 123.126.74.16 所属国家: China 地区: Beijing 城市: Beijing  |
| mcgw.alipay.com | IP: 124.95.190.88 所属国家: China 地区: Liaoning 城市: Shenyang  |
| www.saxproject.org | IP: 204.68.111.100 所属国家: United States of America 地区: California 城市: San Diego  |
| www.cocos.com | IP: 221.194.141.162 所属国家: China 地区: Hebei 城市: Langfang  |
| analytics.rayjump.com | IP: 123.56.168.170 所属国家: China 地区: Beijing 城市: Beijing  |
| wappaygw.alipay.com | IP: 124.95.190.88 所属国家: China 地区: Liaoning 城市: Shenyang  |
| open.weixin.qq.com | IP: 220.196.139.154 所属国家: China 地区: Jiangsu 城市: Yangzhou  |
| sf6-ttcdn-tos.pstatp.com | IP: 14.205.45.114 所属国家: China 地区: Yunnan 城市: Chuxiong  |
| apps.oceanengine.com | IP: 42.56.93.212 所属国家: China 地区: Liaoning 城市: Shenyang  |
| cdn-adn-https.rayjump.com | IP: 123.126.74.18 所属国家: China 地区: Beijing 城市: Beijing  |
| s3-us-west-2.amazonaws.com | IP: 52.218.182.152 所属国家: United States of America 地区: Oregon 城市: Boardman  |
| detect.rayjump.com | IP: 52.0.111.172 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| gist.github.com | IP: 243.185.187.39 所属国家: - 地区: - 城市: -  |
| policy.rayjump.com | IP: 112.126.23.181 所属国家: China 地区: Beijing 城市: Beijing  |
| www.khronos.org | IP: 159.65.181.57 所属国家: United States of America 地区: New Jersey 城市: Clifton  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| play.google.com | IP: 142.250.217.78 所属国家: United States of America 地区: California 城市: Mountain View  |
| i.snssdk.com | IP: 123.125.216.198 所属国家: China 地区: Beijing 城市: Beijing  |
| apps.bytesfield-b.com | IP: 106.74.132.34 所属国家: China 地区: Shandong 城市: Jinan  |
| www.openssl.org | IP: 34.49.79.89 所属国家: United States of America 地区: California 城市: Mountain View  |
| heycam.github.io | IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| www.samsungapps.com | IP: 54.229.93.185 所属国家: Ireland 地区: Dublin 城市: Dublin  |
| d1tru86qrby720.cloudfront.net | IP: 18.172.39.192 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| aa.birdgesdk.com | IP: 120.78.94.142 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| hybird.rayjump.com | IP: 123.126.74.16 所属国家: China 地区: Beijing 城市: Beijing  |
| mp.weixin.qq.com | IP: 220.196.139.154 所属国家: China 地区: Jiangsu 城市: Yangzhou  |
| lazy.rayjump.com | IP: 112.126.23.181 所属国家: China 地区: Beijing 城市: Beijing  |
| mtg-native.rayjump.com | IP: 123.125.46.38 所属国家: China 地区: Beijing 城市: Beijing  |
| check.rayjump.com | IP: 112.126.23.181 所属国家: China 地区: Beijing 城市: Beijing  |
| apps.bytesfield.com | IP: 106.74.132.38 所属国家: China 地区: Shandong 城市: Jinan  |
| p1-lm.adkwai.com | IP: 116.153.46.55 所属国家: China 地区: Jiangxi 城市: Nanchang  |
| purl.eligrey.com | IP: 104.236.163.66 所属国家: United States of America 地区: California 城市: San Francisco  |
| static.yximgs.com | IP: 101.73.101.241 所属国家: China 地区: Hebei 城市: Shijiazhuang  |
| cdn.jsdelivr.net | IP: 151.101.89.229 所属国家: United States of America 地区: California 城市: San Francisco  |
| cn-magnet.rayjump.com | IP: 47.94.43.17 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| dom.spec.whatwg.org | IP: 165.227.248.76 所属国家: United States of America 地区: New Jersey 城市: Clifton  |
| net.rayjump.com | IP: 8.147.107.120 所属国家: China 地区: Zhejiang 城市: Hangzhou  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://mobilegwpre.alipay.com/mgw.htm  | com/alipay/apmobilesecuritysdk/b/a.java  |
| https://mobilegw.alipay.com/mgw.htm  | com/alipay/apmobilesecuritysdk/b/a.java  |
| https://wappaygw.alipay.com/home/exterfaceAssign.htm?  | com/alipay/sdk/app/PayTask.java  |
| https://mclient.alipay.com/home/exterfaceAssign.htm?  | com/alipay/sdk/app/PayTask.java  |
| https://wappaygw.alipay.com/service/rest.htm  | com/alipay/sdk/app/PayTask.java  |
| http://wappaygw.alipay.com/service/rest.htm  | com/alipay/sdk/app/PayTask.java  |
| https://mclient.alipay.com/service/rest.htm  | com/alipay/sdk/app/PayTask.java  |
| http://mclient.alipay.com/service/rest.htm  | com/alipay/sdk/app/PayTask.java  |
| https://mclient.alipay.com/home/exterfaceAssign.htm  | com/alipay/sdk/app/PayTask.java  |
| http://mclient.alipay.com/home/exterfaceAssign.htm  | com/alipay/sdk/app/PayTask.java  |
| https://mclient.alipay.com/cashier/mobilepay.htm  | com/alipay/sdk/app/PayTask.java  |
| http://mclient.alipay.com/cashier/mobilepay.htm  | com/alipay/sdk/app/PayTask.java  |
| https://mobilegw.alipaydev.com/mgw.htm  | com/alipay/sdk/b/j0/l.java  |
| https://mobilegw.dl.alipaydev.com/mgw.htm  | com/alipay/sdk/b/j0/l.java  |
| https://mobilegw.alipay.com/mgw.htm  | com/alipay/sdk/b/u/a.java  |
| https://h5.m.taobao.com/mlapp/olist.html  | com/alipay/sdk/b/w/a.java  |
| https://mcgw.alipay.com/sdklog.do  | com/alipay/sdk/b/d0/c.java  |
| https://loggw-exsdk.alipay.com/loggw/logUpload.do  | com/alipay/sdk/b/d0/d.java  |
| https://mores.toponad.com/image/default/bg2\_vertical\_720x1280.jpg  | com/anythink/basead/i/d.java  |
| https://mores.toponad.com/image/default/bg1\_horizontal\_1280x720.jpg  | com/anythink/basead/i/d.java  |
| http://xmlpull.org/v1/doc/features.html  | com/anythink/basead/i/b/b.java  |
| https://play.google.com  | com/anythink/basead/mraid/MraidBaseWebView.java  |
| https://play.google.com/store/apps/details?id=  | com/anythink/core/basead/a/c.java  |
| https:///gdpr/PrivacyPolicySetting.html  | com/anythink/core/common/h.java  |
| https:///gdpr/PrivacyPolicySetting.html  | com/anythink/core/common/c/i.java  |
| https:///hostsetting/dmlist/index.html  | com/anythink/core/common/c/i.java  |
| https:///hostsetting/mumbai/index.html  | com/anythink/core/common/c/i.java  |
| https:///hostsetting/dmlist/index.html  | com/anythink/core/common/f/a.java  |
| https:///hostsetting/mumbai/index.html  | com/anythink/core/common/f/a.java  |
| https:///gdpr/PrivacyPolicySetting.html  | com/anythink/core/common/f/a.java  |
| https://adx  | com/anythink/core/common/f/a.java  |
| https:///hostsetting/mumbai/index.html  | com/anythink/core/common/f/c.java  |
| https:///hostsetting/dmlist/index.html  | com/anythink/core/common/f/c.java  |
| https://mores.toponad.com/image/adx\_animate/animate5\_recommend1.png  | com/anythink/core/d/a.java  |
| https://mores.toponad.com/image/adx\_animate/animate5\_recommend2.png  | com/anythink/core/d/a.java  |
| https://mores.toponad.com/image/adx\_animate/animate5\_recommend3.png  | com/anythink/core/d/a.java  |
| https://mores.toponad.com/image/adx\_animate/animate5\_recommend4.png  | com/anythink/core/d/a.java  |
| https://i.snssdk.com/  | com/bytedance/sdk/openadsdk/downloadnew/core/AdBaseConstants.java  |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/offline\_components/tk/ks\_so-tachikomaNoSoRelease-3.3.64.1-30279a11a9-537.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-3.3.59-5a16210b94-483.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://open.e.kuaishou.com/rest/e/v3/open/sdk2  | com/kwad/sdk/api/loader/u.java  |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/ks\_so-appStatusArm64v8aRelease-3.3.14.apk  | com/kwad/sdk/collector/d.java  |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/ks\_so-appStatusArmeabiv7aRelease-3.3.14.apk  | com/kwad/sdk/collector/d.java  |
| http://%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/exception/202305301754/ks\_so-exceptionArm64v8aRelease-3.3.47-e8fbb3a5f8-666.apk  | com/kwad/sdk/crash/g.java  |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/so/exception/202305301754/ks\_so-exceptionArmeabiv7aRelease-3.3.47-e8fbb3a5f8-666.apk  | com/kwad/sdk/crash/g.java  |
| http://apps.samsung.com/appquery/appDetail.as?appId=  | com/kwad/sdk/utils/d.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://hybird.rayjump.com/rv/authoriztion.html  | com/mbridge/msdk/a.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://cn-magnet.rayjump.com/mini/scheme  | 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/ad.java  |
| https://play.google.com/  | com/mbridge/msdk/foundation/tools/ad.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://play.google.com/store/apps/details?id=  | com/mbridge/msdk/foundation/webview/a.java  |
| https://play.google.com/  | com/mbridge/msdk/click/b.java  |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense  | com/mbridge/msdk/playercommon/exoplayer2/drm/HttpMediaDrmCallback.java  |
| https://play.google.com  | com/mbridge/msdk/mbjscommon/windvane/WindVaneWebView.java  |
| https://cdn-adn-https.rayjump.com/cdn-adn/v2/portal/19/08/20/11/06/5d5b63cb457e2.js  | com/mbridge/msdk/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/c.java  |
| http://whatwg.org/html/webappapis.html  | com/mbridge/msdk/c/b/c.java  |
| https://gist.github.com/atk/1020396\n  | com/mbridge/msdk/c/b/c.java  |
| http://whatwg.org/C  | com/mbridge/msdk/c/b/c.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://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/c.java  |
| https://apps.bytesfield.com  | com/ss/android/downloadlib/addownload/compliance/s.java  |
| https://apps.bytesfield-b.com  | com/ss/android/downloadlib/addownload/compliance/s.java  |
| https://www.samsungapps.com/appquery/appDetail.as?appId=  | com/ss/android/downloadlib/xd/di.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  |
| https://aa.birdgesdk.com/v1/d\_api  | com/tramini/plugin/a/b/a.java  |
| https://pitk.birdgesdk.com/v1/ptk  | com/tramini/plugin/a/b/a.java  |
| https://rr  | com/tramini/plugin/a/f/a.java  |
| http://www.cocos.com  | 摸瓜V2引擎  |
| https://www.cocos.com/  | 摸瓜V2引擎  |
| http://eligrey.com  | 摸瓜V2引擎  |
| https://github.com/dsamarin  | 摸瓜V2引擎  |
| https://github.com/eligrey/Blob.js/blob/master/LICENSE.md  | 摸瓜V2引擎  |
| http://purl.eligrey.com/github/Blob.js/blob/master/Blob.js  | 摸瓜V2引擎  |
| https://dom.spec.whatwg.org/  | 摸瓜V2引擎  |
| https://heycam.github.io/webidl/  | 摸瓜V2引擎  |
| https://github.com/taylorhakes  | 摸瓜V2引擎  |
| https://github.com/taylorhakes/promise-polyfill/blob/master/LICENSE  | 摸瓜V2引擎  |
| https://cdn.jsdelivr.net/npm/promise-polyfill@8/dist/polyfill.js  | 摸瓜V2引擎  |
| http://www.cocos.com  | 摸瓜V2引擎  |
| https://www.khronos.org/registry/OpenGL/extensions/ARB/ARB\_texture\_float.txt  | 摸瓜V2引擎  |
| http://www.saxproject.org/apidoc/org/xml/sax/helpers/DefaultHandler.html  | 摸瓜V2引擎  |
| http://www.saxproject.org/apidoc/org/xml/sax/ContentHandler.html  | 摸瓜V2引擎  |
| http://www.saxproject.org/apidoc/org/xml/sax/ErrorHandler.html  | 摸瓜V2引擎  |
| http://www.saxproject.org/apidoc/org/xml/sax/ext/LexicalHandler.html  | 摸瓜V2引擎  |
| http://www.saxproject.org/apidoc/org/xml/sax/ext/DeclHandler.html  | 摸瓜V2引擎  |
| http://www.saxproject.org/apidoc/org/xml/sax/ext/EntityResolver2.html  | 摸瓜V2引擎  |
| http://www.saxproject.org/apidoc/org/xml/sax/DTDHandler.html  | 摸瓜V2引擎  |
| http://www.apple.com/DTDs/PropertyList-1.0.dtd  | lib/arm64-v8a/libcocos2djs.so  |
| https://www.openssl.org/docs/faq.html  | lib/arm64-v8a/libcocos2djs.so  |
| https://crbug.com/v8/8520  | lib/arm64-v8a/libcocos2djs.so  |
| http://www.apple.com/DTDs/PropertyList-1.0.dtd  | lib/armeabi-v7a/libcocos2djs.so  |
| https://www.openssl.org/docs/faq.html  | lib/armeabi-v7a/libcocos2djs.so  |
| https://crbug.com/v8/8520  | lib/armeabi-v7a/libcocos2djs.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| danikula@gmail.com  | com/kwad/sdk/core/videocache/h.java  |
| .apk@classes.dex  | com/kuaishou/weapon/p0/ac.java  |
| c@3.tnbyз\_  | 摸瓜V2引擎  |
| yth@i.ivy34tݢ  | 摸瓜V2引擎  |
| cocos@cocoss-macbook-pro.local  | lib/arm64-v8a/libcocos2djs.so  |
| cocos@cocoss-macbook-pro.local  | lib/armeabi-v7a/libcocos2djs.so  |

### **4.4 手机号线索**

## **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: C=china, ST=fujian, L=quanzhou, O=jyjgy, OU=jyjgy, CN=linjie 签名算法: rsassa\_pkcs1v15 有效期自: 2024-08-26 07:50:47+00:00 有效期至: 2034-08-24 07:50:47+00:00 发行人: C=china, ST=fujian, L=quanzhou, O=jyjgy, OU=jyjgy, CN=linjie 序列号: 0x776762fe 哈希算法: sha256 md5值: e5fb8735e8f505dd038b3f02f05d5540 sha1值: f045f4c612337d606fa2f4b2c0a42c8802fca204 sha256值: 14c2c8450d060d6174807c9b99ca67ad72c560e18c8435d2b6ffbe2920f4df92 sha512值: 0caaf682627bfea82535746d5c5318c2128b8323cdb062577fa22ba3d244b62856141557c1cff92bed6fd446b5a2a0c2ac7cabd2e64ff845fa60c098c14b6eea 公钥算法: rsa 密钥长度: 1024 指纹: f296a70f2e0cbd6bd36e816f3a05f9bcd86fc24291b3a4af04a5e2e6da79ad75**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "anythink\_myoffer\_feedback\_violation\_of\_laws" : "Illegal"  |
| "dyStrategy.privateAddress" : "privateAddress"  |
| "anythink\_myoffer\_feedback\_violation\_of\_laws" : "违规违法"  |

## **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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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.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.jyj.codex.openadsdk.permission.TT\_PANGOLIN | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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 |
| com.google.android.gms.permission.AD\_ID | 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.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.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 |
| com.asus.msa.SupplementaryDID.ACCESS | 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.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 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| org.cocos2dx.javascript.AppActivity | **Schemes**: uds7qt://,  |

**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。**