



# MoGua

## 英魂传说 1.1.9.APK 分析报告



APP名称:

英魂传说

|        |                            |
|--------|----------------------------|
| 包名:    | com.jyj.codex              |
| 域名线索:  | 56条                        |
| URL线索: | 56条                        |
| 邮箱线索:  | 6条                         |
| 分析日期:  | 2025年7月22日                 |
| 分析平台:  | <a href="#">摸瓜APK反编译平台</a> |

文件名: codex1.1.9.apk  
文件大小: 173.33MB  
MD5值: 5802a3d8d02f241d5479f3b2aaf0165f  
SHA1值: 5c6d391af5a28c7e9a95dfa64aa7975e3c85ebec  
SHA256值: c14a5a00b8fd277933e59e8df10acaefd0368a273b576b7f35e6b5a9df44ef8e

## i APP 信息

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

## 🔍 域名线索

| 域名                     | 服务器信息                                                                                                |
|------------------------|------------------------------------------------------------------------------------------------------|
| www.apple.com          | IP: 27.148.139.136<br>所属国家: China<br>地区: Fujian<br>城市: Fuzhou<br>纬度: 26.061390<br>经度: 119.306107     |
| mobilegw.alipaydev.com | IP: 110.75.132.131<br>所属国家: China<br>地区: Zhejiang<br>城市: Hangzhou<br>纬度: 30.293650<br>经度: 120.161583 |
| github.com             | IP: 20.205.243.166<br>所属国家: Singapore<br>地区: Singapore                                               |

|                        |                                                                                                                       |
|------------------------|-----------------------------------------------------------------------------------------------------------------------|
|                        | <div>城市: Singapore<br/>纬度: 1.289987<br/>经度: 103.850281</div>                                                          |
| loggw-exsdk.alipay.com | <div>IP: 110.76.6.82<br/>所属国家: China<br/>地区: Zhejiang<br/>城市: Hangzhou<br/>纬度: 30.293650<br/>经度: 120.161583</div>     |
| h5.m.taobao.com        | <div>IP: 125.38.11.131<br/>所属国家: China<br/>地区: Tianjin<br/>城市: Tianjin<br/>纬度: 39.142181<br/>经度: 117.176102</div>     |
| configure.rayjump.com  | <div>IP: 112.126.23.181<br/>所属国家: China<br/>地区: Beijing<br/>城市: Beijing<br/>纬度: 39.907501<br/>经度: 116.397102</div>    |
| mobilegw.alipay.com    | <div>IP: 203.209.250.2<br/>所属国家: China<br/>地区: Zhejiang<br/>城市: Hangzhou<br/>纬度: 30.293650<br/>经度: 120.161583</div>   |
| open.e.kuaishou.com    | <div>IP: 116.136.202.194<br/>所属国家: China<br/>地区: Nei Mongol<br/>城市: Hohhot<br/>纬度: 40.810650<br/>经度: 111.650665</div> |
|                        |                                                                                                                       |

|                         |                                                                                                                                |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| crbug.com               | IP: 216.239.32.29<br>所属国家: United States of America<br>地区: California<br>城市: Mountain View<br>纬度: 37.405991<br>经度: -122.078514 |
| whatwg.org              | IP: 165.227.248.76<br>所属国家: United States of America<br>地区: New Jersey<br>城市: Clifton<br>纬度: 40.858585<br>经度: -74.163605       |
| apps.samsung.com        | IP: 104.17.142.17<br>所属国家: United States of America<br>地区: California<br>城市: San Francisco<br>纬度: 37.775700<br>经度: -122.395203 |
| mobilegwpre.alipay.com  | IP: 110.75.138.35<br>所属国家: China<br>地区: Zhejiang<br>城市: Hangzhou<br>纬度: 30.293650<br>经度: 120.161583                            |
| long.open.weixin.qq.com | IP: 112.65.193.170<br>所属国家: China<br>地区: Shanghai<br>城市: Shanghai<br>纬度: 31.224333<br>经度: 121.468948                           |
| eligrey.com             | IP: 104.236.163.66<br>所属国家: United States of America<br>地区: California<br>城市: San Francisco                                    |

|                           |                                                                                                                                |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------|
|                           | 纬度: 37.774929<br>经度: -122.419418                                                                                               |
| xmlpull.org               | IP: 185.199.108.153<br>所属国家: United States of America<br>地区: Pennsylvania<br>城市: California<br>纬度: 40.065647<br>经度: -79.891724 |
| schemas.microsoft.com     | IP: 13.107.246.73<br>所属国家: United States of America<br>地区: Washington<br>城市: Redmond<br>纬度: 47.682899<br>经度: -122.120903       |
| mclient.alipay.com        | IP: 116.142.234.199<br>所属国家: China<br>地区: Beijing<br>城市: Beijing<br>纬度: 39.907501<br>经度: 116.397102                            |
| mobilegw.dl.alipaydev.com | IP: 110.75.132.25<br>所属国家: China<br>地区: Zhejiang<br>城市: Hangzhou<br>纬度: 30.293650<br>经度: 120.161583                            |
| pitk.birdgesdk.com        | IP: 39.108.103.199<br>所属国家: China<br>地区: Guangdong<br>城市: Shenzhen<br>纬度: 22.545673<br>经度: 114.068108                          |
|                           | IP: 123.126.74.16                                                                                                              |

|                       |                                                                                                                                                                       |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mores.toponad.com     | <b>所属国家:</b> China<br><b>地区:</b> Beijing<br><b>城市:</b> Beijing<br><b>纬度:</b> 39.907501<br><b>经度:</b> 116.397102                                                       |
| mcgw.alipay.com       | <b>IP:</b> 124.95.190.88<br><b>所属国家:</b> China<br><b>地区:</b> Liaoning<br><b>城市:</b> Shenyang<br><b>纬度:</b> 41.792221<br><b>经度:</b> 123.432877                         |
| www.saxproject.org    | <b>IP:</b> 204.68.111.100<br><b>所属国家:</b> United States of America<br><b>地区:</b> California<br><b>城市:</b> San Diego<br><b>纬度:</b> 32.799797<br><b>经度:</b> -117.137047 |
| www.cocos.com         | <b>IP:</b> 221.194.141.162<br><b>所属国家:</b> China<br><b>地区:</b> Hebei<br><b>城市:</b> Langfang<br><b>纬度:</b> 39.509720<br><b>经度:</b> 116.694717                          |
| analytics.rayjump.com | <b>IP:</b> 123.56.168.170<br><b>所属国家:</b> China<br><b>地区:</b> Beijing<br><b>城市:</b> Beijing<br><b>纬度:</b> 39.907501<br><b>经度:</b> 116.397102                          |
| wappaygw.alipay.com   | <b>IP:</b> 124.95.190.88<br><b>所属国家:</b> China<br><b>地区:</b> Liaoning<br><b>城市:</b> Shenyang<br><b>纬度:</b> 41.792221<br><b>经度:</b> 123.432877                         |

|                            |                                                                                                                        |
|----------------------------|------------------------------------------------------------------------------------------------------------------------|
| open.weixin.qq.com         | IP: 220.196.139.154<br>所属国家: China<br>地区: Jiangsu<br>城市: Yangzhou<br>纬度: 32.397221<br>经度: 119.435600                   |
| sf6-ttcdn-tos.pstatp.com   | IP: 14.205.45.114<br>所属国家: China<br>地区: Yunnan<br>城市: Chuxiong<br>纬度: 25.045555<br>经度: 101.528053                      |
| apps.oceanengine.com       | IP: 42.56.93.212<br>所属国家: China<br>地区: Liaoning<br>城市: Shenyang<br>纬度: 41.792221<br>经度: 123.432877                     |
| cdn-adn-https.rayjump.com  | IP: 123.126.74.18<br>所属国家: China<br>地区: Beijing<br>城市: Beijing<br>纬度: 39.907501<br>经度: 116.397102                      |
| s3-us-west-2.amazonaws.com | IP: 52.218.182.152<br>所属国家: United States of America<br>地区: Oregon<br>城市: Boardman<br>纬度: 45.839859<br>经度: -119.700577 |
|                            | IP: 52.0.111.172<br>所属国家: United States of America<br>地区: Virginia                                                     |

|                    |                                                                                                                                                                           |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| detect.rayjump.com | <b>城市:</b> Ashburn<br><b>纬度:</b> 39.039474<br><b>经度:</b> -77.491806                                                                                                       |
| gist.github.com    | <b>IP:</b> 243.185.187.39<br><b>所属国家:</b> -<br><b>地区:</b> -<br><b>城市:</b> -<br><b>纬度:</b> 0.000000<br><b>经度:</b> 0.000000                                                 |
| policy.rayjump.com | <b>IP:</b> 112.126.23.181<br><b>所属国家:</b> China<br><b>地区:</b> Beijing<br><b>城市:</b> Beijing<br><b>纬度:</b> 39.907501<br><b>经度:</b> 116.397102                              |
| www.khronos.org    | <b>IP:</b> 159.65.181.57<br><b>所属国家:</b> United States of America<br><b>地区:</b> New Jersey<br><b>城市:</b> Clifton<br><b>纬度:</b> 40.858585<br><b>经度:</b> -74.163605         |
| www.w3.org         | <b>IP:</b> 104.18.22.19<br><b>所属国家:</b> United States of America<br><b>地区:</b> California<br><b>城市:</b> San Francisco<br><b>纬度:</b> 37.775700<br><b>经度:</b> -122.395203   |
| play.google.com    | <b>IP:</b> 142.250.217.78<br><b>所属国家:</b> United States of America<br><b>地区:</b> California<br><b>城市:</b> Mountain View<br><b>纬度:</b> 37.405991<br><b>经度:</b> -122.078514 |

|                               |                                                                                                                                |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| i.snssdk.com                  | IP: 123.125.216.198<br>所属国家: China<br>地区: Beijing<br>城市: Beijing<br>纬度: 39.907501<br>经度: 116.397102                            |
| apps.bytesfield-b.com         | IP: 106.74.132.34<br>所属国家: China<br>地区: Shandong<br>城市: Jinan<br>纬度: 36.668331<br>经度: 116.997223                               |
| www.openssl.org               | IP: 34.49.79.89<br>所属国家: United States of America<br>地区: California<br>城市: Mountain View<br>纬度: 37.405991<br>经度: -122.078514   |
| heycam.github.io              | IP: 185.199.108.153<br>所属国家: United States of America<br>地区: Pennsylvania<br>城市: California<br>纬度: 40.065647<br>经度: -79.891724 |
| www.samsungapps.com           | IP: 54.229.93.185<br>所属国家: Ireland<br>地区: Dublin<br>城市: Dublin<br>纬度: 53.344151<br>经度: -6.267249                               |
| d1tru86qrby720.cloudfront.net | IP: 18.172.39.192<br>所属国家: Japan<br>地区: Tokyo<br>城市: Tokyo<br>纬度: 35.689499                                                    |

|                        |                                                                                                      |
|------------------------|------------------------------------------------------------------------------------------------------|
|                        | 经度: 139.692322                                                                                       |
| aa.birdgesdk.com       | IP: 120.78.94.142<br>所属国家: China<br>地区: Zhejiang<br>城市: Hangzhou<br>纬度: 30.293650<br>经度: 120.161583  |
| hybird.rayjump.com     | IP: 123.126.74.16<br>所属国家: China<br>地区: Beijing<br>城市: Beijing<br>纬度: 39.907501<br>经度: 116.397102    |
| mp.weixin.qq.com       | IP: 220.196.139.154<br>所属国家: China<br>地区: Jiangsu<br>城市: Yangzhou<br>纬度: 32.397221<br>经度: 119.435600 |
| lazy.rayjump.com       | IP: 112.126.23.181<br>所属国家: China<br>地区: Beijing<br>城市: Beijing<br>纬度: 39.907501<br>经度: 116.397102   |
| mtg-native.rayjump.com | IP: 123.125.46.38<br>所属国家: China<br>地区: Beijing<br>城市: Beijing<br>纬度: 39.907501<br>经度: 116.397102    |
|                        | IP: 112.126.23.181<br>所属国家: China                                                                    |

|                     |                                                                                                                                 |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------|
| check.rayjump.com   | 地区: Beijing<br>城市: Beijing<br>纬度: 39.907501<br>经度: 116.397102                                                                   |
| apps.bytesfield.com | IP: 106.74.132.38<br>所属国家: China<br>地区: Shandong<br>城市: Jinan<br>纬度: 36.668331<br>经度: 116.997223                                |
| p1-lm.adkwai.com    | IP: 116.153.46.55<br>所属国家: China<br>地区: Jiangxi<br>城市: Nanchang<br>纬度: 28.683331<br>经度: 115.883331                              |
| purl.eligrey.com    | IP: 104.236.163.66<br>所属国家: United States of America<br>地区: California<br>城市: San Francisco<br>纬度: 37.774929<br>经度: -122.419418 |
| static.yximgs.com   | IP: 101.73.101.241<br>所属国家: China<br>地区: Hebei<br>城市: Shijiazhuang<br>纬度: 38.041599<br>经度: 114.478081                           |
| cdn.jsdelivr.net    | IP: 151.101.89.229<br>所属国家: United States of America<br>地区: California<br>城市: San Francisco<br>纬度: 37.775700<br>经度: -122.395203 |
|                     |                                                                                                                                 |

|                       |                                                                                                                          |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------|
| cn-magnet.rayjump.com | IP: 47.94.43.17<br>所属国家: China<br>地区: Zhejiang<br>城市: Hangzhou<br>纬度: 30.293650<br>经度: 120.161583                        |
| dom.spec.whatwg.org   | IP: 165.227.248.76<br>所属国家: United States of America<br>地区: New Jersey<br>城市: Clifton<br>纬度: 40.858585<br>经度: -74.163605 |
| net.rayjump.com       | IP: 8.147.107.120<br>所属国家: China<br>地区: Zhejiang<br>城市: Hangzhou<br>纬度: 30.293650<br>经度: 120.161583                      |

 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-                                                                                     | com/kwad/components/offline/c/b/a.java                            |

|                                                                                                                                                                                                                                                                                   |                                                   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|
| KSAdSDK/tachikoma/3.3.58/ks_tk_so_v8_lite_3358                                                                                                                                                                                                                                    |                                                   |
| <a href="https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/tachikoma/3.3.58/ks_tk_so_v8_3358">https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/tachikoma/3.3.58/ks_tk_so_v8_3358</a>                                                                                     | com/kwad/components/offline/c/b/a.java            |
| <a href="https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/tachikoma/3.3.58/ks_tk_so_v7_lite_3358">https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/tachikoma/3.3.58/ks_tk_so_v7_lite_3358</a>                                                                           | com/kwad/components/offline/c/b/a.java            |
| <a href="https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/tachikoma/3.3.58/ks_tk_so_v7_3358">https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/tachikoma/3.3.58/ks_tk_so_v7_3358</a>                                                                                     | com/kwad/components/offline/c/b/a.java            |
| <a href="https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/offline_components/obiwan/ks_so-obiwanNoSoRelease-3.3.56-445ef4f109-409.zip">https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/offline_components/obiwan/ks_so-obiwanNoSoRelease-3.3.56-445ef4f109-409.zip</a> | com/kwad/components/offline/b/b.java              |
| <a href="https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/offline_components/adLive/ks_so-adLiveNoSoRelease-3.3.59-5a16210b94-483.zip">https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/offline_components/adLive/ks_so-adLiveNoSoRelease-3.3.59-5a16210b94-483.zip</a> | com/kwad/components/offline/a/b.java              |
| <a href="https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/adLive/ks_so-adLiveArm64v8aRelease-3.3.44.2-e8fbb3a5f8-666.apk">https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/adLive/ks_so-adLiveArm64v8aRelease-3.3.44.2-e8fbb3a5f8-666.apk</a>                           | com/kwad/components/offline/a/a/a.java            |
| <a href="https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/adLive/ks_so-adLiveArmeabiv7aRelease-3.3.44.2-e8fbb3a5f8-666.apk">https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/adLive/ks_so-adLiveArmeabiv7aRelease-3.3.44.2-e8fbb3a5f8-666.apk</a>                       | com/kwad/components/offline/a/a/a.java            |
| <a href="https://github.com/lingochamp/FileDownloader/wiki/filedownloader.properties">https://github.com/lingochamp/FileDownloader/wiki/filedownloader.properties</a>                                                                                                             | com/kwad/framework/filedownloader/services/a.java |
| <a href="https://open.e.kuaishou.com/rest/e/v3/open/sdk2">https://open.e.kuaishou.com/rest/e/v3/open/sdk2</a>                                                                                                                                                                     | com/kwad/sdk/api/loader/u.java                    |
| <a href="https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDK/ks_so-appStatusArm64v8aRelease-3.3.14.apk">https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDK/ks_so-appStatusArm64v8aRelease-3.3.14.apk</a>                                                                   | com/kwad/sdk/collector/d.java                     |
| <a href="https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDK/ks_so-appStatusArmeabiv7aRelease-3.3.14.apk">https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDK/ks_so-appStatusArmeabiv7aRelease-3.3.14.apk</a>                                                               | com/kwad/sdk/collector/d.java                     |
| <a href="http://%s:%d/%s">http://%s:%d/%s</a>                                                                                                                                                                                                                                     | com/kwad/sdk/core/video/cache/f.java              |
|                                                                                                                                                                                                                                                                                   |                                                   |

|                                                                                                                                                                                                                                                                                                       |                                               |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|
| <a href="https://github.com/danikula/AndroidVideoCache/issues/88">https://github.com/danikula/AndroidVideoCache/issues/88</a> .                                                                                                                                                                       | com/kwad/sdk/core/video/cache/h.java          |
| <a href="https://github.com/danikula/AndroidVideoCache/issues/43">https://github.com/danikula/AndroidVideoCache/issues/43</a> .                                                                                                                                                                       | com/kwad/sdk/core/video/cache/h.java          |
| <a href="https://github.com/danikula/AndroidVideoCache/issues">https://github.com/danikula/AndroidVideoCache/issues</a> .                                                                                                                                                                             | com/kwad/sdk/core/video/cache/h.java          |
| <a href="https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/so/exception/202305301754/ks_so-exceptionArm64v8aRelease-3.3.47-e8fbb3a5f8-666.apk">https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/so/exception/202305301754/ks_so-exceptionArm64v8aRelease-3.3.47-e8fbb3a5f8-666.apk</a>       | com/kwad/sdk/crash/g.java                     |
| <a href="https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/so/exception/202305301754/ks_so-exceptionArmeabi-v7aRelease-3.3.47-e8fbb3a5f8-666.apk">https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/so/exception/202305301754/ks_so-exceptionArmeabi-v7aRelease-3.3.47-e8fbb3a5f8-666.apk</a> | com/kwad/sdk/crash/g.java                     |
| <a href="http://apps.samsung.com/appquery/appDetail.as?appId=">http://apps.samsung.com/appquery/appDetail.as?appId=</a>                                                                                                                                                                               | com/kwad/sdk/Utils/d.java                     |
| <a href="https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/kmac/ks_kmac64">https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/kmac/ks_kmac64</a>                                                                                                                                               | com/kwad/sdk/kgeo/c.java                      |
| <a href="https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/kmac/ks_kmac32">https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/kmac/ks_kmac32</a>                                                                                                                                               | com/kwad/sdk/kgeo/c.java                      |
| <a href="https://hybird.rayjump.com/rv/authoriztion.html">https://hybird.rayjump.com/rv/authoriztion.html</a>                                                                                                                                                                                         | com/mbridge/msdk/a.java                       |
| <a href="https://analytics.rayjump.com">https://analytics.rayjump.com</a>                                                                                                                                                                                                                             | com/mbridge/msdk/foundation/same/net/f/d.java |
| <a href="https://net.rayjump.com">https://net.rayjump.com</a>                                                                                                                                                                                                                                         | com/mbridge/msdk/foundation/same/net/f/d.java |
| <a href="https://configure.rayjump.com">https://configure.rayjump.com</a>                                                                                                                                                                                                                             | com/mbridge/msdk/foundation/same/net/f/d.java |
| <a href="https://cn-magnet.rayjump.com/mini/scheme">https://cn-magnet.rayjump.com/mini/scheme</a>                                                                                                                                                                                                     | com/mbridge/msdk/foundation/same/net/f/d.java |
| <a href="https://detect.rayjump.com/mapi/find">https://detect.rayjump.com/mapi/find</a>                                                                                                                                                                                                               | com/mbridge/msdk/foundation/same/net/f/d.java |
| <a href="https://detect.rayjump.com/mapi/result">https://detect.rayjump.com/mapi/result</a>                                                                                                                                                                                                           | com/mbridge/msdk/foundation/same/net/f/d.java |
| <a href="https://d1tru86qrby720.cloudfront.net/hostsetting">https://d1tru86qrby720.cloudfront.net/hostsetting</a>                                                                                                                                                                                     | com/mbridge/msdk/foundation/same/net/f/d.java |

|                                                                                                                                                                                       |                                                                        |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|
| <a href="https://policy.rayjump.com">https://policy.rayjump.com</a>                                                                                                                   | com/mbridge/msdk/foundation/same/net/f/d.java                          |
| <a href="https://lazy.rayjump.com">https://lazy.rayjump.com</a>                                                                                                                       | com/mbridge/msdk/foundation/same/net/f/d.java                          |
| <a href="https://check.rayjump.com">https://check.rayjump.com</a>                                                                                                                     | com/mbridge/msdk/foundation/same/net/f/d.java                          |
| <a href="https://play.google.com/store/apps/details?id=">https://play.google.com/store/apps/details?id=</a>                                                                           | com/mbridge/msdk/foundation/tools/ad.java                              |
| <a href="https://play.google.com/">https://play.google.com/</a>                                                                                                                       | com/mbridge/msdk/foundation/tools/ad.java                              |
| <a href="https://cdn-adn-https.rayjump.com/cdn-adn/v2/portal/19/08/20/11/06/5d5b63cb457e2.js">https://cdn-adn-https.rayjump.com/cdn-adn/v2/portal/19/08/20/11/06/5d5b63cb457e2.js</a> | com/mbridge/msdk/foundation/controller/b.java                          |
| <a href="https://mtg-native.rayjump.com/omsdk/omsdkjs_common_js.txt">https://mtg-native.rayjump.com/omsdk/omsdkjs_common_js.txt</a>                                                   | com/mbridge/msdk/foundation/controller/b.java                          |
| <a href="https://play.google.com/store/apps/details?id=">https://play.google.com/store/apps/details?id=</a>                                                                           | com/mbridge/msdk/foundation/webview/a.java                             |
| <a href="https://play.google.com/">https://play.google.com/</a>                                                                                                                       | com/mbridge/msdk/click/b.java                                          |
| <a href="http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense">http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense</a>                                     | com/mbridge/msdk/playercommon/exoplayer2/drm/HttpMediaDrmCallback.java |
| <a href="https://play.google.com">https://play.google.com</a>                                                                                                                         | com/mbridge/msdk/mbjscommon/windvane/WindVaneWebView.java              |
| <a href="https://cdn-adn-https.rayjump.com/cdn-adn/v2/portal/19/08/20/11/06/5d5b63cb457e2.js">https://cdn-adn-https.rayjump.com/cdn-adn/v2/portal/19/08/20/11/06/5d5b63cb457e2.js</a> | com/mbridge/msdk/c/b.java                                              |
| <a href="https://mtg-native.rayjump.com/omsdk/omsdkjs_common_js.txt">https://mtg-native.rayjump.com/omsdk/omsdkjs_common_js.txt</a>                                                   | com/mbridge/msdk/c/b.java                                              |
| <a href="http://whatwg.org/html/common-microsyntaxes.html">http://whatwg.org/html/common-microsyntaxes.html</a>                                                                       | com/mbridge/msdk/c/b/c.java                                            |
| <a href="http://whatwg.org/html/webappapis.html">http://whatwg.org/html/webappapis.html</a>                                                                                           | com/mbridge/msdk/c/b/c.java                                            |
| <a href="https://gist.github.com/atk/1020396\n">https://gist.github.com/atk/1020396\n</a>                                                                                             | 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&uuiid=%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                                                                         |
|                                                                                                          |                                                                                |

|                                                                                                                                                                         |        |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|
| <a href="http://eligrey.com">http://eligrey.com</a>                                                                                                                     | 摸瓜V2引擎 |
| <a href="https://github.com/dsamarin">https://github.com/dsamarin</a>                                                                                                   | 摸瓜V2引擎 |
| <a href="https://github.com/eligrey/Blob.js/blob/master/LICENSE.md">https://github.com/eligrey/Blob.js/blob/master/LICENSE.md</a>                                       | 摸瓜V2引擎 |
| <a href="http://purl.eligrey.com/github/Blob.js/blob/master/Blob.js">http://purl.eligrey.com/github/Blob.js/blob/master/Blob.js</a>                                     | 摸瓜V2引擎 |
| <a href="https://dom.spec.whatwg.org/">https://dom.spec.whatwg.org/</a>                                                                                                 | 摸瓜V2引擎 |
| <a href="https://heycam.github.io/webidl/">https://heycam.github.io/webidl/</a>                                                                                         | 摸瓜V2引擎 |
| <a href="https://github.com/taylorhakes">https://github.com/taylorhakes</a>                                                                                             | 摸瓜V2引擎 |
| <a href="https://github.com/taylorhakes/promise-polyfill/blob/master/LICENSE">https://github.com/taylorhakes/promise-polyfill/blob/master/LICENSE</a>                   | 摸瓜V2引擎 |
| <a href="https://cdn.jsdelivr.net/npm/promise-polyfill@8/dist/polyfill.js">https://cdn.jsdelivr.net/npm/promise-polyfill@8/dist/polyfill.js</a>                         | 摸瓜V2引擎 |
| <a href="http://www.cocos.com">http://www.cocos.com</a>                                                                                                                 | 摸瓜V2引擎 |
| <a href="https://www.khronos.org/registry/OpenGL/extensions/ARB/ARB_texture_float.txt">https://www.khronos.org/registry/OpenGL/extensions/ARB/ARB_texture_float.txt</a> | 摸瓜V2引擎 |
| <a href="http://www.saxproject.org/apidoc/org/xml/sax/helpers/DefaultHandler.html">http://www.saxproject.org/apidoc/org/xml/sax/helpers/DefaultHandler.html</a>         | 摸瓜V2引擎 |
| <a href="http://www.saxproject.org/apidoc/org/xml/sax/ContentHandler.html">http://www.saxproject.org/apidoc/org/xml/sax/ContentHandler.html</a>                         | 摸瓜V2引擎 |
| <a href="http://www.saxproject.org/apidoc/org/xml/sax/ErrorHandler.html">http://www.saxproject.org/apidoc/org/xml/sax/ErrorHandler.html</a>                             | 摸瓜V2引擎 |
| <a href="http://www.saxproject.org/apidoc/org/xml/sax/ext/LexicalHandler.html">http://www.saxproject.org/apidoc/org/xml/sax/ext/LexicalHandler.html</a>                 | 摸瓜V2引擎 |
| <a href="http://www.saxproject.org/apidoc/org/xml/sax/ext/DeclHandler.html">http://www.saxproject.org/apidoc/org/xml/sax/ext/DeclHandler.html</a>                       | 摸瓜V2引擎 |
| <a href="http://www.saxproject.org/apidoc/org/xml/sax/ext/EntityResolver2.html">http://www.saxproject.org/apidoc/org/xml/sax/ext/EntityResolver2.html</a>               | 摸瓜V2引擎 |
| <a href="http://www.saxproject.org/apidoc/org/xml/sax/DTDHandler.html">http://www.saxproject.org/apidoc/org/xml/sax/DTDHandler.html</a>                                 | 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 |

 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.tnby3_                     | 摸瓜V2引擎                              |
| yth@i.ivy34tㄣ                  | 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     |

 手机线索

# 🌸 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

# 🔑 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" : "违法违规"    |

# 🌀 加壳分析

| 加壳类型      | 所属文件 |
|-----------|------|
| 登陆摸瓜网站后查看 |      |

## 第三方插件

| 名称        | 分类 | URL链接 |
|-----------|----|-------|
| 登陆摸瓜网站后查看 |    |       |

## 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                      |

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](#) 自动生成，并非包含所有检测结果，有疑问请联系管理员。