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

**艾兴合（ 3.8.6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 | 艾兴合 |
| 版本 | 3.8.6 |
| 包名 | uni.UNIE74261C7 |
| 域名线索 | 68条 |
| URL线索 | 40条 |
| APP图标 |  |
| 分析日期 | 2025年8月4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 | 艾兴合(1).apk |
| 文件大小 | 43.98MB |
| MD5值 | 8c845756711669ea6d6056b0c4ed95ae |
| SHA1值 | b88c00ddea2b036e7ce5329ddb8d0fe938e0d461 |
| SHA256值 | 681901204ea9482917c3503faba44391bb3bcc52f140d1c0c9bdfb31a0f08f36 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 艾兴合 |
| 包名 | uni.UNIE74261C7 |
| 主活动Activity | io.dcloud.PandoraEntry |
| 安卓版本名称 | 3.8.6 |
| 安卓版本 | 213 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| cloudauth.aliyuncs.com | IP: 106.11.232.51  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| ns.adobe.com | 没有服务器地理信息. |
| statistic.live.126.net | IP: 220.197.34.76  所属国家: China  地区: Sichuan  城市: Leshan |
| cloudauth-dualstack.aliyuncs.com | IP: 106.11.172.8  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| at.alicdn.com | IP: 120.52.51.114  所属国家: China  地区: Hebei  城市: Langfang |
| momentjs.com | IP: 104.16.32.155  所属国家: United States of America  地区: California  城市: San Francisco |
| work.weixin.qq.com | IP: 106.55.209.39  所属国家: China  地区: Beijing  城市: Beijing |
| cashier.sandpay.com.cn | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| api.next.bspapp.com | IP: 203.107.60.33  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| da.qiyukf.com | IP: 45.254.48.100  所属国家: China  地区: Guangdong  城市: Guangzhou |
| www.payeasenet.com | IP: 210.73.90.4  所属国家: China  地区: Beijing  城市: Beijing |
| lodash.com | IP: 52.220.155.145  所属国家: Singapore  地区: Singapore  城市: Singapore |
| test-shop-api.aixingheshangcheng.com | IP: 106.14.251.212  所属国家: China  地区: Shanghai  城市: Shanghai |
| cn-shanghai-aliyun-cloudauth.oss-cn-shanghai.aliyuncs.com | IP: 140.206.110.66  所属国家: China  地区: Shanghai  城市: Shanghai |
| schemas.android.com | 没有服务器地理信息. |
| wanproxy-hz.127.net | IP: 223.252.196.43  所属国家: China  地区: Guangdong  城市: Guangzhou |
| imtest4.netease.im | IP: 59.111.241.163  所属国家: China  地区: Guangdong  城市: Guangzhou |
| uniapp.dcloud.io | IP: 220.194.123.111  所属国家: China  地区: Tianjin  城市: Tianjin |
| imtest6.netease.im | 没有服务器地理信息. |
| shop-api.aixingheshangcheng.com | IP: 47.101.160.195  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| apis.map.qq.com | IP: 116.130.223.114  所属国家: China  地区: Beijing  城市: Beijing |
| cloudauth-dualstack.cn-beijing.aliyuncs.com | IP: 8.141.244.37  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| er.dcloud.io | 没有服务器地理信息. |
| service.dcloud.net.cn | IP: 110.40.169.99  所属国家: China  地区: Beijing  城市: Beijing |
| play.aixingheshangcheng.com | IP: 39.91.185.244  所属国家: China  地区: Shandong  城市: Linyi |
| mgw.mpaas.cn-hangzhou.aliyuncs.com | IP: 47.118.168.189  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| static-shop.aixingheshangcheng.com | IP: 140.206.110.53  所属国家: China  地区: Shanghai  城市: Shanghai |
| h5.aixingheshangcheng.com | IP: 47.102.99.166  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| cloudauth.cn-beijing.aliyuncs.com | IP: 8.141.244.36  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| ap1.qiyukf.com | IP: 45.254.48.100  所属国家: China  地区: Guangdong  城市: Guangzhou |
| lbs.netease.im | IP: 220.197.34.89  所属国家: China  地区: Sichuan  城市: Leshan |
| qiyukf.netease.com | IP: 59.111.222.254  所属国家: China  地区: Guangdong  城市: Guangzhou |
| auth.yunverify.com | IP: 106.11.232.51  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| oss-cn-hangzhou.aliyuncs.com | IP: 118.31.219.189  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| qydev.netease.com | IP: 59.111.48.68  所属国家: China  地区: Guangdong  城市: Guangzhou |
| gw.alipayobjects.com | IP: 116.136.165.42  所属国家: China  地区: Nei Mongol  城市: Hohhot |
| imtest-gy.netease.im | IP: 111.124.202.90  所属国家: China  地区: Guizhou  城市: Zunyi |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| oss-cn-.aliyuncs.comor | 没有服务器地理信息. |
| openjsf.org | IP: 76.76.21.21  所属国家: United States of America  地区: California  城市: Walnut |
| dr.netease.im | IP: 220.197.34.84  所属国家: China  地区: Sichuan  城市: Leshan |
| open.weixin.qq.com | IP: 140.207.191.167  所属国家: China  地区: Shanghai  城市: Shanghai |
| quilljs.com | IP: 172.66.40.163  所属国家: United States of America  地区: California  城市: San Francisco |
| da.qytest.netease.com | IP: 111.124.202.64  所属国家: China  地区: Guizhou  城市: Zunyi |
| npms.io | IP: 104.21.64.1  所属国家: United States of America  地区: California  城市: San Francisco |
| www.google.com | IP: 31.13.68.169  所属国家: Ireland  地区: Dublin  城市: Dublin |
| www.bouncycastle.org | IP: 43.250.142.130  所属国家: Australia  地区: Queensland  城市: Warren |
| feross.org | IP: 50.116.11.184  所属国家: United States of America  地区: California  城市: Fremont |
| api.bspapp.com | IP: 39.96.249.142  所属国家: China  地区: Beijing  城市: Beijing |
| download.shieye-property.com | IP: 47.100.184.139  所属国家: China  地区: Shanghai  城市: Shanghai |
| er.dcloud.net.cn | IP: 43.142.57.168  所属国家: China  地区: Beijing  城市: Beijing |
| nosup-hz1.127.net | IP: 122.156.129.106  所属国家: China  地区: Heilongjiang  城市: Heihe |
| ask.dcloud.net.cn | IP: 220.194.123.111  所属国家: China  地区: Tianjin  城市: Tianjin |
| da.qiyukf.netease.com | IP: 59.111.222.254  所属国家: China  地区: Guangdong  城市: Guangzhou |
| aixinghemall.oss-cn-shanghai.aliyuncs.com | IP: 140.206.110.66  所属国家: China  地区: Shanghai  城市: Shanghai |
| underscorejs.org | IP: 104.21.25.112  所属国家: United States of America  地区: California  城市: San Francisco |
| aixinghe-bucket.oss-cn-shanghai.aliyuncs.com | IP: 140.206.110.53  所属国家: China  地区: Shanghai  城市: Shanghai |
| www.w3.org | IP: 104.18.23.19  所属国家: United States of America  地区: California  城市: San Francisco |
| m3w.cn | IP: 125.38.214.65  所属国家: China  地区: Tianjin  城市: Tianjin |
| aq1.qytest.netease.com | IP: 111.124.202.64  所属国家: China  地区: Guizhou  城市: Zunyi |
| long.open.weixin.qq.com | IP: 112.65.193.170  所属国家: China  地区: Shanghai  城市: Shanghai |
| image.cnamedomain.com | 没有服务器地理信息. |
| render.alipay.com | IP: 221.204.78.211  所属国家: China  地区: Shanxi  城市: Taiyuan |
| imtest.netease.im | IP: 111.124.202.79  所属国家: China  地区: Guizhou  城市: Zunyi |
| pop.yuncloudauth.com | IP: 59.82.44.22  所属国家: China  地区: Shanghai  城市: Shanghai |
| p.mailuo.plus | IP: 119.23.64.26  所属国家: China  地区: Guangdong  城市: Shenzhen |
| uniapp.dcloud.net.cn | IP: 119.188.180.230  所属国家: China  地区: Shandong  城市: Jinan |
| lbs-qiyu.netease.im | IP: 220.197.34.90  所属国家: China  地区: Sichuan  城市: Leshan |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://ip. | com/alibaba/sdk/android/oss/OSSImpl.java |
| http://oss-cn-\*\*\*\*.aliyuncs.com',or | com/alibaba/sdk/android/oss/OSSImpl.java |
| http://image.cnamedomain.com'! | com/alibaba/sdk/android/oss/OSSImpl.java |
| http://oss-cn-hangzhou.aliyuncs.com | com/alibaba/sdk/android/oss/common/OSSConstants.java |
| http://oss-cn-\*\*\*\*.aliyuncs.com',or | com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java |
| http://image.cnamedomain.com'! | com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java |
| https://mgw.mpaas.cn-hangzhou.aliyuncs.com | com/alipay/alipaysecuritysdk/common/config/Configuration.java |
| https://cloudauth-dualstack.aliyuncs.com | com/dtf/face/api/DTFacadeExt.java |
| https://cloudauth.aliyuncs.com | com/dtf/face/api/DTFacadeExt.java |
| https://cloudauth-dualstack.cn-beijing.aliyuncs.com | com/dtf/face/api/DTFacadeExt.java |
| https://cloudauth.cn-beijing.aliyuncs.com | com/dtf/face/api/DTFacadeExt.java |
| https://auth.yunverify.com | com/dtf/face/api/DTFacadeExt.java |
| https://pop.yuncloudauth.com | com/dtf/face/api/DTFacadeExt.java |
| https://render.alipay.com/p/f/fd-j8l9yjja/index.html | com/dtf/face/config/NavigatePage.java |
| https://gw.alipayobjects.com/render/p/yuyan\_npm/@alipay\_dtfconfig/1.0.1/lib/toyger.face.android.wasm | com/dtf/face/utils/ModelDownloadUtil.java |
| https://cn-shanghai-aliyun-cloudauth.oss-cn-shanghai.aliyuncs.com/model/toyger.face.dat | com/dtf/face/utils/ModelDownloadUtil.java |
| https://statistic.live.126.net/dispatcher/req | com/qiyukf/nimlib/c/b.java |
| https://statistic.live.126.net/ | com/qiyukf/nimlib/c/b/c/b.java |
| https://imtest-gy.netease.im/lbs/conf | com/qiyukf/nimlib/f/e.java |
| https://imtest.netease.im/1.gif | com/qiyukf/nimlib/f/e.java |
| https://imtest4.netease.im/test/ | com/qiyukf/nimlib/f/e.java |
| https://imtest6.netease.im:8012/ | com/qiyukf/nimlib/f/e.java |
| https://lbs.netease.im/lbs/conf.jsp | com/qiyukf/nimlib/f/e.java |
| https://lbs-qiyu.netease.im/lbs/conf.jsp?devflag=qyonline | com/qiyukf/nimlib/f/e.java |
| https://dr.netease.im/1.gif | com/qiyukf/nimlib/f/e.java |
| https://wanproxy-hz.127.net/lbs | com/qiyukf/nimlib/f/g.java |
| https://nosup-hz1.127.net | com/qiyukf/nimlib/f/g.java |
| http://aq1.qytest.netease.com | com/qiyukf/unicorn/i/a/c.java |
| http://qiyukf.netease.com | com/qiyukf/unicorn/i/a/c.java |
| http://qydev.netease.com | com/qiyukf/unicorn/i/a/c.java |
| https://ap1.qiyukf.com | com/qiyukf/unicorn/i/a/c.java |
| http://da.qytest.netease.com | com/qiyukf/unicorn/i/a/c.java |
| http://da.qiyukf.netease.com | com/qiyukf/unicorn/i/a/c.java |
| https://da.qiyukf.com | com/qiyukf/unicorn/i/a/c.java |
| http://schemas.android.com/apk/res/android | com/hjq/permissions/AndroidManifestParser.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 |
| http://ns.adobe.com/xap/1.0/\u0000 | io/dcloud/common/util/ExifInterface.java |
| https://m3w.cn/s/ | io/dcloud/common/util/ShortCutUtil.java |
| https://ask.dcloud.net.cn/article/282 | io/dcloud/common/constant/DOMException.java |
| https://ask.dcloud.net.cn/article/35627 | io/dcloud/e/b/a.java |
| https://ask.dcloud.net.cn/article/35877 | io/dcloud/e/b/a.java |
| https://er.dcloud.io/rv | io/dcloud/e/c/h/c.java |
| https://er.dcloud.net.cn/rv | io/dcloud/e/c/h/c.java |
| https://er.dcloud.io/sc | io/dcloud/feature/gg/dcloud/ADHandler.java |
| https://er.dcloud.net.cn/sc | io/dcloud/feature/gg/dcloud/ADHandler.java |
| https://ask.dcloud.net.cn/article/283 | io/dcloud/feature/utsplugin/ProxyModule.java |
| https://ask.dcloud.net.cn/article/35058 | io/dcloud/feature/audio/AudioRecorderMgr.java |
| https://ask.dcloud.net.cn/article/283 | io/dcloud/g/b.java |
| https://ask.dcloud.net.cn/article/287 | io/dcloud/share/IFShareApi.java |
| http://www.bouncycastle.org) | org/eid\_bc/bouncycastle/LICENSE.java |
| http://schemas.android.com/apk/res/android | pl/droidsonroids/gif/GifViewUtils.java |
| http://schemas.android.com/apk/res/android | pl/droidsonroids/gif/GifTextureView.java |
| http://schemas.android.com/apk/res/android | pl/droidsonroids/gif/GifTextView.java |
| https://ask.dcloud.net.cn/article/36199 | 摸瓜V1引擎 |
| https://render.alipay.com/p/yuyan/180020010001208736/aliyunFacewelcome.html | 摸瓜V1引擎 |
| https://apis.map.qq.com/jsapi?qt=translate&type=1&points= | 摸瓜V2引擎 |
| https://apis.map.qq.com/uri/v1/routeplan?type=drive&to= | 摸瓜V2引擎 |
| https://www.google.com/maps/?daddr= | 摸瓜V2引擎 |
| https://www.google.com/maps/ | 摸瓜V2引擎 |
| https://quilljs.com/ | 摸瓜V2引擎 |
| https://quilljs.com | 摸瓜V2引擎 |
| https://download.shieye-property.com/privacy/shop/license.html\ | 摸瓜V2引擎 |
| https://download.shieye-property.com/privacy/shop/privacy.html\ | 摸瓜V2引擎 |
| http://feross.org> | 摸瓜V2引擎 |
| http://uniapp.dcloud.io | 摸瓜V2引擎 |
| http://uniapp.dcloud.io/ | 摸瓜V2引擎 |
| https://lodash.com/> | 摸瓜V2引擎 |
| https://openjsf.org/> | 摸瓜V2引擎 |
| https://lodash.com/license> | 摸瓜V2引擎 |
| http://underscorejs.org/LICENSE> | 摸瓜V2引擎 |
| https://npms.io/search?q=ponyfill. | 摸瓜V2引擎 |
| https://shop-api.aixingheshangcheng.com | 摸瓜V2引擎 |
| https://static-shop.aixingheshangcheng.com/static/wx\_xcx | 摸瓜V2引擎 |
| https://h5.aixingheshangcheng.com/ | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/sc\_xx\_icon.png | 摸瓜V2引擎 |
| https://work.weixin.qq.com/kfid/kfc3984c75946009cb0 | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/integral/activity/pin\_detail/pin\_detail?id= | 摸瓜V2引擎 |
| https://test-shop-api.aixingheshangcheng.com | 摸瓜V2引擎 |
| http://momentjs.com/guides/ | 摸瓜V2引擎 |
| https://api.next.bspapp.com | 摸瓜V2引擎 |
| https://api.bspapp.com | 摸瓜V2引擎 |
| https://uniapp.dcloud.net.cn/uniCloud/secure-network.html | 摸瓜V2引擎 |
| https://uniapp.dcloud.net.cn/uniCloud/faq?id=promise | 摸瓜V2引擎 |
| https://static-shop.aixingheshangcheng.com/icon/shop.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/new\_crbg.png | 摸瓜V2引擎 |
| https://download.shieye-property.com/privacy/shop/privacy.html | 摸瓜V2引擎 |
| https://download.shieye-property.com/privacy/shop/license.html | 摸瓜V2引擎 |
| https://static-shop.aixingheshangcheng.com/static/wx\_xcx/wechatpay-icon.png | 摸瓜V2引擎 |
| https://static-shop.aixingheshangcheng.com/static/wx\_xcx/alipay-icon.png | 摸瓜V2引擎 |
| https://static-shop.aixingheshangcheng.com/static/images/user/user\_31.png | 摸瓜V2引擎 |
| https://static-shop.aixingheshangcheng.com/static/images/new\_user/user2\_26.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/6.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/555.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/star\_r.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/star\_b.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/star\_y.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/star\_y2.png | 摸瓜V2引擎 |
| https://github.com/facebook/regenerator/blob/main/LICENSE | 摸瓜V2引擎 |
| https://feross.org/opensource> | 摸瓜V2引擎 |
| https://cashier.sandpay.com.cn/static/fastpay/page/agree.html | 摸瓜V2引擎 |
| https://static-shop.aixingheshangcheng.com/icon/axhPay/ | 摸瓜V2引擎 |
| https://www.payeasenet.com/2.0/agreement/expressPayment?cashier=/237c18356e1e4b50b52047abf0659757 | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/show2.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/show1.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/no-login.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/balance/no-record02.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/upload-pic.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/store\_r.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/right\_o.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/order\_goods\_more.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/b\_phone.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/b\_code.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/b\_pw.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/balance/close-icon.png) | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/balance/right-white-icon.png) | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/balance/tip\_icon\_red.png) | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/title\_tip.png) | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/arrow\_right\_b.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/addr\_border.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/cart\_gou.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/checkbox.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/new\_user/haibao.jpg | 摸瓜V2引擎 |
| https://static-shop.aixingheshangcheng.com/static/images/right\_o.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/search-d.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/mcc\_04\_w.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/close3.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/balance/tip\_icon\_red.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/arrow\_left\_b.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/shop/shop\_default\_logo.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/goods\_img\_play.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/order\_w.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/delete-icon.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/shop/tejia\_bg02.jpg) | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/shop/jingpin\_bg02.jpg) | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/shop/rmai\_bg02.jpg) | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/user/share-friend-banner02.png) | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/close.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/del\_b.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/value\_minus.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/value\_add.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/Shoppingcart.png | 摸瓜V2引擎 |
| https://p.mailuo.plus/static/wx\_xcx/user\_setting\_bg.png);background-size:100% | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/index/pay\_ewm.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/right\_icon.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/line\_left.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/line\_right.png | 摸瓜V2引擎 |
| https://play.aixingheshangcheng.com/e8150eccc1bc1a9efcfdd0146e5c6694/4446662629376965.m3u8?auth\_key=1694080620-0-0-d02b71ad29642b0b03a51c341d4db98d | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/del\_search.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/result-success.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/pay\_error\_tip.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/icon/logo\_1024.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/right\_o2.png | 摸瓜V2引擎 |
| https://aixinghemall.oss-cn-shanghai.aliyuncs.com/data/upload/wxapp/under-review.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/store\_b.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/reg\_voucher\_close.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/close2.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/shop/girht\_white.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/back-top.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/order\_sel.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/nothave.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/new\_user/user\_top\_bg.png) | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/new\_user/user\_m\_bg2.png) | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/new\_user/user\_m\_btn.png) | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/user\_ltr.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/new\_user/user2\_set.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/new\_user/user2\_1.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/new\_user/user2\_3.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/new\_user/user2\_2.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/new\_user/user2\_4.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/new\_user/user\_share\_p2.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/new\_user/user2\_12.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/new\_user/user2\_13.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/new\_user/user2\_14.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/new\_user/user2\_22.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/new\_user/user2\_18.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/new\_user/user2\_23.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/new\_user/store\_in2.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/sld\_cha@2x.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/index-updata.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/login\_pass\_hide.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/login\_pass\_show.png | 摸瓜V2引擎 |
| https://at.alicdn.com/t/font\_2225171\_8kdcwk4po24.ttf) | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/balance/balance\_top\_btn\_icon.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/balance/balance\_list\_icon.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/vip/vip-zs.png | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/balance/tip-password.png) | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/ok.png) | 摸瓜V2引擎 |
| https://aixinghe-bucket.oss-cn-shanghai.aliyuncs.com/static/images/goods-browse\_w.png | 摸瓜V2引擎 |
| https://service.dcloud.net.cn/uniapp/feedback.html | 摸瓜V2引擎 |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| sld\_cha@2x.png | 摸瓜V2引擎 |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17950237975 | com/qiyukf/android/extension/servicekeeper/service/ipc/server/a/c.java |
| 15095675534 | org/eid\_bc/bouncycastle/asn1/ua/DSTU4145NamedCurves.java |
| 17179869184 | org/eid\_bc/bouncycastle/pqc/math/linearalgebra/GF2nONBElement.java |
| 17179869183 | org/eid\_bc/bouncycastle/pqc/math/linearalgebra/GF2nONBElement.java |
| 19634136210 | org/eid\_bc/bouncycastle/math/ec/custom/sec/SecT163Field.java |

## **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=CN, ST=, L=, O=Android, OU=Android, CN=cZ19vB4k7fLcH85JPPUTMINCvsWgyCChYrtHl15iUy%2FZSQS1OMfACMEcYE9GDgHE0Olrxsu%2Fock7dw0HiL78uw%3D%3D 签名算法: rsassa\_pkcs1v15 有效期自: 2021-10-21 07:06:09+00:00 有效期至: 2121-09-27 07:06:09+00:00 发行人: C=CN, ST=, L=, O=Android, OU=Android, CN=cZ19vB4k7fLcH85JPPUTMINCvsWgyCChYrtHl15iUy%2FZSQS1OMfACMEcYE9GDgHE0Olrxsu%2Fock7dw0HiL78uw%3D%3D 序列号: 0x1d58e214 哈希算法: sha256 md5值: 7e8108890e84f6edb6823007c012dd1c sha1值: ae9abeb53bc448e4d68d084136d9f43843d7a757 sha256值: a5d517c7f01a6619549aee97c9070e90cf05ee8f7811a8e5d55bc244bdd06a76 sha512值: bd30f50b75db8d09b5d5739cc8d4f3d27557ada3afa44034621662ec736ebf50c28eb176d86d1548315b7bbe97ea363544e34dd27c4dfb4e6782c6db583941c5 公钥算法: rsa 密钥长度: 2048 指纹: b8791322698c99940e0c0c236cd4ba5be10a9f91e3936d8ab6aba12ce04d0904**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "dcloud\_common\_user\_refuse\_api" : "the user denies access to the API" |
| "dcloud\_io\_without\_authorization" : "not authorized" |
| "dcloud\_oauth\_authentication\_failed" : "failed to obtain authorization to log in to the authentication service" |
| "dcloud\_oauth\_empower\_failed" : "the Authentication Service operation to obtain authorized logon failed" |
| "dcloud\_oauth\_logout\_tips" : "not logged in or logged out" |
| "dcloud\_oauth\_oauth\_not\_empower" : "oAuth authorization has not been obtained" |
| "dcloud\_oauth\_token\_failed" : "failed to get token" |
| "dcloud\_permissions\_reauthorization" : "reauthorize" |
| "dcloud\_tips\_certificate" : "certificate" |
| "ysf\_already\_quit\_session" : "You have quit conversation" |
| "ysf\_back\_close\_session" : "Quit Session" |
| "ysf\_close\_session\_fail" : "Failed to quit conversation" |
| "ysf\_dialog\_close\_session" : "Sure to quit the conversation?" |
| "ysf\_menu\_close\_session" : "Exit" |
| "ysf\_session\_already\_end" : "Conversation is over" |
| "ysf\_session\_already\_quit" : "Conversation quit" |
| "ysf\_session\_close\_cannot\_evaluation" : "Conversation is over. Cannot rate" |
| "ysf\_session\_ing\_and\_end\_again\_request" : "There is an ongoing conversation. Sure to end it and initiate a new consultation" |
| "ysf\_work\_sheet\_auth" : "Fill in the information" |
| "ysf\_work\_sheet\_session\_change" : "Work order expired" |
| "ysf\_already\_quit\_session" : "您已退出会话" |
| "ysf\_back\_close\_session" : "关闭会话" |
| "ysf\_close\_session\_fail" : "退出会话失败" |
| "ysf\_dialog\_close\_session" : "确认退出对话？" |
| "ysf\_menu\_close\_session" : "退出" |
| "ysf\_session\_already\_end" : "会话已结束" |
| "ysf\_session\_already\_quit" : "会话已退出" |
| "ysf\_session\_close\_cannot\_evaluation" : "会话已结束，无法评价" |
| "ysf\_session\_ing\_and\_end\_again\_request" : "您有会话正在进行中，是否结束会话发起新的咨询" |
| "ysf\_work\_sheet\_auth" : "填写信息" |
| "ysf\_work\_sheet\_session\_change" : "工单已过期" |
| "ysf\_already\_quit\_session" : "您已退出會話" |
| "ysf\_back\_close\_session" : "關閉會話" |
| "ysf\_close\_session\_fail" : "退出會話失敗" |
| "ysf\_dialog\_close\_session" : "確認退出對話？" |
| "ysf\_menu\_close\_session" : "退出" |
| "ysf\_session\_already\_end" : "會話已結束" |
| "ysf\_session\_already\_quit" : "會話已退出" |
| "ysf\_session\_close\_cannot\_evaluation" : "會話已結束，無法評價" |
| "ysf\_session\_ing\_and\_end\_again\_request" : "您有會話正在進行中，是否結束會話發起新的諮詢" |
| "ysf\_work\_sheet\_auth" : "填寫信息" |
| "ysf\_work\_sheet\_session\_change" : "工單已過期" |
| "dcloud\_common\_user\_refuse\_api" : "用户拒绝该API访问" |
| "dcloud\_io\_without\_authorization" : "没有获得授权" |
| "dcloud\_oauth\_authentication\_failed" : "获取授权登录认证服务操作失败" |
| "dcloud\_oauth\_empower\_failed" : "获取授权登录认证服务操作失败" |
| "dcloud\_oauth\_logout\_tips" : "未登录或登录已注销" |
| "dcloud\_oauth\_oauth\_not\_empower" : "尚未获取oauth授权" |
| "dcloud\_oauth\_token\_failed" : "获取token失败" |
| "dcloud\_permissions\_reauthorization" : "重新授权" |
| "dcloud\_tips\_certificate" : "证书" |

## **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.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.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.INSTALL\_PACKAGES | 系统需要 | 直接安装应用程序 | 允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序 |
| 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.ACCESS\_COARSE\_LOCATION | 危险 | 粗定位 | 访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置 |
| android.permission.ACCESS\_FINE\_LOCATION | 危险 | 精细定位（GPS） | 访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量 |
| android.permission.MANAGE\_EXTERNAL\_STORAGE | 危险 | 允许应用程序广泛访问范围存储中的外部存储 | 允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用 |
| android.permission.CALL\_PHONE | 危险 | 直接拨打电话号码 | 允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码 |
| android.permission.CAMERA | 危险 | 拍照和录像 | 允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像 |
| android.permission.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.CHANGE\_WIFI\_STATE | 正常 | 更改Wi-Fi状态 | 允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改 |
| android.permission.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| android.permission.GET\_ACCOUNTS | 危险 | 列出帐户 | 允许访问账户服务中的账户列表 |
| android.permission.MODIFY\_AUDIO\_SETTINGS | 正常 | 更改您的音频设置 | 允许应用程序修改全局音频设置,例如音量和路由 |
| android.permission.MOUNT\_UNMOUNT\_FILESYSTEMS | 危险 | 装载和卸载文件系统 | 允许应用程序为可移动存储安装和卸载文件系统 |
| android.permission.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\_LOGS | 危险 | 读取敏感日志数据 | 允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息 |
| android.permission.READ\_PHONE\_STATE | 危险 | 读取电话状态和身份 | 允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.WAKE\_LOCK | 正常 | 防止手机睡眠 | 允许应用程序防止手机进入睡眠状态 |
| android.permission.WRITE\_GSERVICES | 系统需要 | 修改谷歌服务地图 | 允许应用程序修改谷歌服务地图。不供普通应用程序使用 |
| android.permission.WRITE\_SETTINGS | 危险 | 修改全局系统设置 | 允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。 |
| com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_IMAGES | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_VIDEO | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_VISUAL\_USER\_SELECTED | 未知 | Unknown permission | Unknown permission from android reference |
| com.huawei.android.launcher.permission.CHANGE\_BADGE | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章。 |
| com.vivo.notification.permission.BADGE\_ICON | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.READ\_MEDIA\_AUDIO | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

**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。**