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

**双福科技（ 1.0.1版本）   
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。  
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | 双福科技 |
| 版本 | 1.0.1 |
| 包名 | uni.UNI678app101.shuangfu |
| 域名线索 | 76条 |
| URL线索 | 74条 |
| APP图标 |  |
| 分析日期 | 2025年6月26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 | 双福科技.apk |
| 文件大小 | 149.95MB |
| MD5值 | 554c9a64ca55418a777ce4129220b902 |
| SHA1值 | a5611d4f6ba5942519e29e1065c9d45432ffe019 |
| SHA256值 | 4790a16cc750fbe81bbb2e06cb349c30f2f8b01390cd82926a968683def602e8 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 双福科技 |
| 包名 | uni.UNI678app101.shuangfu |
| 主活动Activity | io.dcloud.PandoraEntry |
| 安卓版本名称 | 1.0.1 |
| 安卓版本 | 101 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| lbs-3dtiles-service.amap.com | IP: 110.253.189.212  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| abroad.apilocate.amap.com | IP: 59.82.44.11  所属国家: China  地区: Shanghai  城市: Shanghai |
| adiu.amap.com | IP: 110.253.189.212  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| render.alipay.com | IP: 221.207.101.98  所属国家: China  地区: Heilongjiang  城市: Jiamusi |
| 192.168.2.21 | IP: 192.168.2.21  所属国家: -  地区: -  城市: - |
| wprd0d.is.autonavi.com | 没有服务器地理信息. |
| mdc.html5.qq.com | IP: 116.130.223.178  所属国家: China  地区: Beijing  城市: Beijing |
| cdn.uviewui.com | IP: 61.48.83.206  所属国家: China  地区: Beijing  城市: Beijing |
| debugtbs.qq.com | IP: 60.29.240.122  所属国家: China  地区: Tianjin  城市: Tianjin |
| debugx5.qq.com | IP: 60.29.240.122  所属国家: China  地区: Tianjin  城市: Tianjin |
| bit.ly | IP: 67.199.248.10  所属国家: United States of America  地区: New York  城市: New York City |
| quilljs.com | IP: 172.66.40.163  所属国家: United States of America  地区: California  城市: San Francisco |
| www.gjtool.cn | IP: 124.221.150.209  所属国家: China  地区: Beijing  城市: Beijing |
| zhengce.6tyjhrdxdtw5.com | IP: 35.220.240.4  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| dualstack-a.apilocate.amap.com | IP: 59.82.31.183  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| feross.org | IP: 50.116.11.184  所属国家: United States of America  地区: California  城市: Fremont |
| zhengce.4thjeutdtrt.com | IP: 34.92.3.193  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| zy.xinyian8621.com | IP: 91.195.240.94  所属国家: Germany  地区: Nordrhein-Westfalen  城市: Koeln |
| mclient.alipay.com | IP: 116.142.235.203  所属国家: China  地区: Beijing  城市: Beijing |
| ask.dcloud.net.cn | IP: 101.72.227.61  所属国家: China  地区: Hebei  城市: Langfang |
| android.googlesource.com | IP: 192.178.163.82  所属国家: United States of America  地区: California  城市: Mountain View |
| m3w.cn | IP: 124.163.195.61  所属国家: China  地区: Shanxi  城市: Taiyuan |
| cfg.imtt.qq.com | IP: 60.28.172.238  所属国家: China  地区: Tianjin  城市: Tianjin |
| restsdk.amap.com | IP: 106.11.43.113  所属国家: China  地区: Beijing  城市: Beijing |
| lbs.amap.com | IP: 110.253.189.212  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| b1.xinyian8456.com | IP: 91.195.240.94  所属国家: Germany  地区: Nordrhein-Westfalen  城市: Koeln |
| pms.mb.qq.com | IP: 60.29.240.17  所属国家: China  地区: Tianjin  城市: Tianjin |
| loggw-exsdk.alipay.com | IP: 119.42.231.20  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| api2.7k9uhedrcg.com | IP: 43.225.47.124  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| yuntuapi.amap.com | 没有服务器地理信息. |
| m5.amap.com | IP: 106.11.43.74  所属国家: China  地区: Beijing  城市: Beijing |
| imgcache.qq.com | IP: 112.64.213.137  所属国家: China  地区: Shanghai  城市: Shanghai |
| api.xinyian8526.com | IP: 91.195.240.94  所属国家: Germany  地区: Nordrhein-Westfalen  城市: Koeln |
| api.bspapp.com | IP: 39.96.249.142  所属国家: China  地区: Beijing  城市: Beijing |
| mqqad.html5.qq.com | IP: 0.0.0.1  所属国家: -  地区: -  城市: - |
| uniapp.dcloud.net.cn | IP: 101.72.227.61  所属国家: China  地区: Hebei  城市: Langfang |
| dualstack-arestapi.amap.com | IP: 203.119.169.174  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| www.google.com | IP: 31.13.88.26  所属国家: Ireland  地区: Dublin  城市: Dublin |
| apiinit.amap.com | IP: 106.11.43.113  所属国家: China  地区: Beijing  城市: Beijing |
| new125.oss-cn-guangzhou.aliyuncs.com | IP: 8.134.41.203  所属国家: China  地区: Guangdong  城市: Guangzhou |
| mths.be | IP: 83.137.145.144  所属国家: Netherlands  地区: Groningen  城市: Groningen |
| log.tbs.qq.com | IP: 124.95.231.218  所属国家: China  地区: Liaoning  城市: Shenyang |
| apis.map.qq.com | IP: 116.130.224.140  所属国家: China  地区: Beijing  城市: Beijing |
| w.wallhaven.cc | IP: 162.125.80.5  所属国家: United States of America  地区: California  城市: San Francisco |
| wb.amap.com | IP: 110.253.188.147  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| mobilegwpre.alipay.com | IP: 110.75.138.35  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| unpkg.com | IP: 104.18.1.22  所属国家: United States of America  地区: California  城市: San Francisco |
| schemas.android.com | 没有服务器地理信息. |
| secure.livechatinc.com | IP: 23.215.212.237  所属国家: Australia  地区: Western Australia  城市: Perth |
| h5.m.taobao.com | IP: 125.39.155.59  所属国家: China  地区: Tianjin  城市: Tianjin |
| restapi.amap.com | IP: 59.82.132.217  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| www.w3.org | IP: 104.18.23.19  所属国家: United States of America  地区: California  城市: San Francisco |
| ns.adobe.com | 没有服务器地理信息. |
| wap.amap.com | IP: 175.19.126.234  所属国家: China  地区: Jilin  城市: Changchun |
| mpsapi.amap.com | IP: 203.119.169.143  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| www.goeasy.io | IP: 222.134.1.29  所属国家: China  地区: Shandong  城市: Binzhou |
| www.apache.org | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| api.next.bspapp.com | IP: 203.107.60.33  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| cgicol.amap.com | IP: 110.253.189.212  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| tbsrecovery.imtt.qq.com | IP: 220.194.120.36  所属国家: China  地区: Tianjin  城市: Tianjin |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| mobilegw.alipay.com | IP: 203.209.250.8  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| mcgw.alipay.com | IP: 116.142.234.145  所属国家: China  地区: Beijing  城市: Beijing |
| apistore.amap.com | IP: 59.82.133.102  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| mst01.is.autonavi.com | IP: 110.253.189.211  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| mobilegw.alipaydev.com | IP: 110.75.132.131  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| apilocate.amap.com | IP: 59.82.31.183  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| service.dcloud.net.cn | IP: 110.40.169.99  所属国家: China  地区: Beijing  城市: Beijing |
| wappaygw.alipay.com | IP: 116.142.234.145  所属国家: China  地区: Beijing  城市: Beijing |
| www.xarg.org | IP: 185.244.195.154  所属国家: Germany  地区: Baden-Wurttemberg  城市: Karlsruhe |
| er.dcloud.net.cn | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| image.wufazhuce.com | IP: 123.117.132.41  所属国家: China  地区: Beijing  城市: Beijing |
| tbs.imtt.qq.com | IP: 122.188.45.181  所属国家: China  地区: Hubei  城市: Jingzhou |
| www.mescroll.com | IP: 185.199.110.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| at.alicdn.com | IP: 221.194.182.9  所属国家: China  地区: Hebei  城市: Langfang |
| er.dcloud.io | 没有服务器地理信息. |

### **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://mobilegw.alipay.com/mgw.htm | com/alipay/sdk/m/l/a.java |
| https://mobilegw.alipaydev.com/mgw.htm | com/alipay/sdk/m/l/a.java |
| https://mcgw.alipay.com/sdklog.do | com/alipay/sdk/m/l/a.java |
| https://loggw-exsdk.alipay.com/loggw/logUpload.do | com/alipay/sdk/m/l/a.java |
| https://wappaygw.alipay.com/home/exterfaceAssign.htm? | com/alipay/sdk/m/l/a.java |
| https://mclient.alipay.com/home/exterfaceAssign.htm? | com/alipay/sdk/m/l/a.java |
| https://h5.m.taobao.com/mlapp/olist.html | com/alipay/sdk/m/m/a.java |
| https://render.alipay.com/p/s/i?scheme=%s | com/alipay/sdk/app/OpenAuthTask.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://adiu.amap.com/ws/device/adius | com/amap/api/col/p0003sl/ku.java |
| http://apiinit.amap.com/v3/log/init | com/amap/api/col/p0003sl/ij.java |
| http://cgicol.amap.com/collection/collectData?src=baseCol&ver=v74& | com/amap/api/col/p0003sl/mp.java |
| http://restsdk.amap.com/v3 | com/amap/api/col/p0003sl/fp.java |
| https://restsdk.amap.com/v3 | com/amap/api/col/p0003sl/fp.java |
| http://restsdk.amap.com/v4 | com/amap/api/col/p0003sl/fp.java |
| https://restsdk.amap.com/v4 | com/amap/api/col/p0003sl/fp.java |
| http://restsdk.amap.com/v5 | com/amap/api/col/p0003sl/fp.java |
| https://restsdk.amap.com/v5 | com/amap/api/col/p0003sl/fp.java |
| http://yuntuapi.amap.com | com/amap/api/col/p0003sl/fp.java |
| https://yuntuapi.amap.com | com/amap/api/col/p0003sl/fp.java |
| http://restsdk.amap.com/rest/me/cpoint | com/amap/api/col/p0003sl/fp.java |
| https://restsdk.amap.com/rest/me/cpoint | com/amap/api/col/p0003sl/fp.java |
| http://apistore.amap.com | com/amap/api/col/p0003sl/fp.java |
| https://apistore.amap.com | com/amap/api/col/p0003sl/fp.java |
| http://m5.amap.com/ws/mapapi/shortaddress/transform | com/amap/api/col/p0003sl/fp.java |
| https://m5.amap.com/ws/mapapi/shortaddress/transform | com/amap/api/col/p0003sl/fp.java |
| https://restsdk.amap.com/v3/iasdkauth | com/amap/api/col/p0003sl/ii.java |
| https://dualstack-arestapi.amap.com/v3/iasdkauth | com/amap/api/col/p0003sl/ii.java |
| https://restsdk.amap.com/sdk/compliance/params | com/amap/api/col/p0003sl/ke.java |
| http://restsdk.amap.com/sdk/compliance/params | com/amap/api/col/p0003sl/ke.java |
| http://restsdk.amap.com | com/amap/api/col/p0003sl/is.java |
| https://restapi.amap.com/rest/aaid/get | com/amap/api/col/p0003sl/jc.java |
| http://restapi.amap.com/rest/aaid/get | com/amap/api/col/p0003sl/jc.java |
| http://restsdk.amap.com/v3/place/text? | com/amap/api/col/p0003sl/a.java |
| http://restsdk.amap.com/v3/place/around? | com/amap/api/col/p0003sl/a.java |
| http://restsdk.amap.com/v3/config/district? | com/amap/api/col/p0003sl/a.java |
| http://restsdk.amap.com/v4/grasproad/driving? | com/amap/api/col/p0003sl/ic.java |
| http://restsdk.amap.com/v4/gridmap? | com/amap/api/col/p0003sl/dg.java |
| http://wprd0%d.is.autonavi.com/appmaptile? | com/amap/api/col/p0003sl/df.java |
| http://restsdk.amap.com/v4/gridmap? | com/amap/api/col/p0003sl/df.java |
| http://restsdk.amap.com/v4 | com/amap/api/col/p0003sl/t.java |
| http://restsdk.amap.com/v4 | com/amap/api/col/p0003sl/cs.java |
| http://restsdk.amap.com | com/amap/api/col/p0003sl/w.java |
| http://wb.amap.com/?r=%f,%f,%s,%f,%f,%s,%d,%d,%d,%s,%s,%s&sourceapplication=openapi/0 | com/amap/api/col/p0003sl/hw.java |
| http://wb.amap.com/?q=%f,%f,%s&sourceapplication=openapi/0 | com/amap/api/col/p0003sl/hw.java |
| http://wb.amap.com/?n=%f,%f,%f,%f,%d&sourceapplication=openapi/0 | com/amap/api/col/p0003sl/hw.java |
| http://wb.amap.com/?p=%s,%f,%f,%s,%s&sourceapplication=openapi/0 | com/amap/api/col/p0003sl/hw.java |
| http://mpsapi.amap.com/ws/mps/lyrdata/ugc/\ | com/amap/api/col/p0003sl/m.java |
| https://restapi.amap.com/rest/lbs/geohub/3d/tiles?z=%d&x=%d&y=%d&id= | com/amap/api/col/p0003sl/l.java |
| http://wap.amap.com/ | com/amap/api/maps/AMapUtils.java |
| https://lbs-3dtiles-service.amap.com/basemap/tiles/staging?compose=building@1669011850923&compose=tree@1668678765481&z=%d&x=%d&y=%d | com/amap/api/maps/model/amap3dmodeltile/AMap3DModelTileProvider.java |
| http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/ | com/amap/api/location/AMapLocation.java |
| http://apilocate.amap.com/mobile/binary | com/autonavi/aps/amapapi/utils/b.java |
| http://dualstack-a.apilocate.amap.com/mobile/binary | com/autonavi/aps/amapapi/utils/b.java |
| http://abroad.apilocate.amap.com/mobile/binary | com/autonavi/aps/amapapi/utils/b.java |
| http://abroad.apilocate.amap.com/mobile/binary | com/autonavi/aps/amapapi/utils/h.java |
| http://abroad.apilocate.amap.com/mobile/binary | com/autonavi/aps/amapapi/trans/a.java |
| http://dualstack-arestapi.amap.com/v3/geocode/regeo | com/autonavi/aps/amapapi/trans/c.java |
| http://restsdk.amap.com/v3/geocode/regeo | com/autonavi/aps/amapapi/trans/c.java |
| http://restsdk.amap.com/rest/lbs/dem/data?z=%d&x=%d&y=%d&type=2 | com/autonavi/base/ae/gmap/TerrainOverlayProvider.java |
| http://mst01.is.autonavi.com/appmaptile?z=%d&x=%d&y=%d&lang=zh\_cn&size=1&scale=1&style=6 | com/autonavi/base/ae/gmap/TerrainOverlayProvider.java |
| http://mpsapi.amap.com/ | com/autonavi/base/ae/gmap/GLMapEngine.java |
| http://m5.amap.com/ | com/autonavi/base/ae/gmap/GLMapEngine.java |
| http://m5.amap.com/ | com/autonavi/base/amap/mapcore/maploader/AMapLoader.java |
| http://schemas.android.com/apk/res/android | com/hjq/permissions/AndroidManifestParser.java |
| https://debugtbs.qq.com | com/tencent/smtt/sdk/WebView.java |
| https://debugx5.qq.com | com/tencent/smtt/sdk/WebView.java |
| https://debugtbs.qq.com?10000\ | com/tencent/smtt/sdk/WebView.java |
| https://pms.mb.qq.com/rsp204 | com/tencent/smtt/sdk/l.java |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=50079 | com/tencent/smtt/sdk/stat/MttLoader.java |
| https://mdc.html5.qq.com/mh?channel\_id=50079&u= | com/tencent/smtt/sdk/stat/MttLoader.java |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11047&is64=0 | com/tencent/smtt/sdk/ui/dialog/d.java |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11047&is64=1 | com/tencent/smtt/sdk/ui/dialog/d.java |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11041&is64=0 | com/tencent/smtt/sdk/ui/dialog/d.java |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11041&is64=1 | com/tencent/smtt/sdk/ui/dialog/d.java |
| https://log.tbs.qq.com/ajax?c=pu&v=2&k= | com/tencent/smtt/utils/o.java |
| https://log.tbs.qq.com/ajax?c=pu&tk= | com/tencent/smtt/utils/o.java |
| https://log.tbs.qq.com/ajax?c=dl&k= | com/tencent/smtt/utils/o.java |
| https://cfg.imtt.qq.com/tbs?v=2&mk= | com/tencent/smtt/utils/o.java |
| https://log.tbs.qq.com/ajax?c=ul&v=2&k= | com/tencent/smtt/utils/o.java |
| https://mqqad.html5.qq.com/adjs | com/tencent/smtt/utils/o.java |
| https://log.tbs.qq.com/ajax?c=ucfu&k= | com/tencent/smtt/utils/o.java |
| https://tbsrecovery.imtt.qq.com/getconfig | com/tencent/smtt/utils/o.java |
| https://tbs.imtt.qq.com/plugin/DebugPlugin\_v2.tbs | com/tencent/smtt/utils/d.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/35058 | io/dcloud/feature/audio/AudioRecorderMgr.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 |
| http://lbs.amap.com/api/android-sdk/guide/error/ | io/dcloud/js/map/amap/adapter/AMapLink.java |
| https://ask.dcloud.net.cn/article/35627 | io/dcloud/p/r.java |
| https://ask.dcloud.net.cn/article/35877 | io/dcloud/p/r.java |
| https://ask.dcloud.net.cn/article/283 | io/dcloud/p/h1.java |
| https://er.dcloud.io/rv | io/dcloud/p/d0.java |
| https://er.dcloud.net.cn/rv | io/dcloud/p/d0.java |
| https://ask.dcloud.net.cn/article/287 | io/dcloud/share/IFShareApi.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://zhengce.6tyjhrdxdtw5.com/xieyi.html\ | 摸瓜V2引擎 |
| https://zhengce.6tyjhrdxdtw5.com/yinsi.html\ | 摸瓜V2引擎 |
| https://zhengce.4thjeutdtrt.com/l.html | 摸瓜V2引擎 |
| http://feross.org> | 摸瓜V2引擎 |
| https://github.com/MikeMcl/decimal.js | 摸瓜V2引擎 |
| https://www.mescroll.com/img/mescroll-totop.png | 摸瓜V2引擎 |
| https://bit.ly/2ZqJzkp | 摸瓜V2引擎 |
| https://api.xinyian8526.com/ | 摸瓜V2引擎 |
| https://b1.xinyian8456.com/ | 摸瓜V2引擎 |
| https://zy.xinyian8621.com/uni/ | 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://api2.7k9uhedrcg.com/ | 摸瓜V2引擎 |
| https://github.com/facebook/regenerator/blob/main/LICENSE | 摸瓜V2引擎 |
| https://www.xarg.org/2014/03/rational-numbers-in-javascript/ | 摸瓜V2引擎 |
| https://feross.org/opensource> | 摸瓜V2引擎 |
| http://mths.be/base64 | 摸瓜V2引擎 |
| https://wx- | 摸瓜V2引擎 |
| http://image.wufazhuce.com/Fu25F54bEiX\_eiqZPVgSmVXLo1zp | 摸瓜V2引擎 |
| https://at.alicdn.com/t/font\_2225171\_8kdcwk4po24.ttf) | 摸瓜V2引擎 |
| https://w.wallhaven.cc/full/m3/wallhaven-m3wgem.png | 摸瓜V2引擎 |
| https://service.dcloud.net.cn/uniapp/feedback.html | 摸瓜V2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://new125.oss-cn-guangzhou.aliyuncs.com/74b2f9bf839e6853/c1f4cc587e9dbaca.png | 摸瓜V2引擎 |
| https://new125.oss-cn-guangzhou.aliyuncs.com/29c483e5188ee131/05311cc9a4c4af65.png | 摸瓜V2引擎 |
| https://new125.oss-cn-guangzhou.aliyuncs.com/4d4bc4b6d72ad0dd/047c7d97adff9873.png | 摸瓜V2引擎 |
| https://new125.oss-cn-guangzhou.aliyuncs.com/ee882894c991f57b/278e552a184c8e08.png | 摸瓜V2引擎 |
| https://new125.oss-cn-guangzhou.aliyuncs.com/6b3661befda91822/9e6ab289e5d79e2d.png | 摸瓜V2引擎 |
| https://new125.oss-cn-guangzhou.aliyuncs.com/c0220979522d8c96/e7d7a05ffe3f35bf.png | 摸瓜V2引擎 |
| http://192.168.2.21:7001/upload | 摸瓜V2引擎 |
| https://cdn.uviewui.com/uview/album/1.jpg | 摸瓜V2引擎 |
| https://cdn.uviewui.com/uview/album/2.jpg | 摸瓜V2引擎 |
| https://cdn.uviewui.com/uview/album/3.jpg | 摸瓜V2引擎 |
| https://cdn.uviewui.com/uview/album/4.jpg | 摸瓜V2引擎 |
| https://cdn.uviewui.com/uview/album/5.jpg | 摸瓜V2引擎 |
| https://cdn.uviewui.com/uview/album/6.jpg | 摸瓜V2引擎 |
| https://cdn.uviewui.com/uview/album/7.jpg | 摸瓜V2引擎 |
| https://cdn.uviewui.com/uview/album/8.jpg | 摸瓜V2引擎 |
| https://cdn.uviewui.com/uview/album/9.jpg | 摸瓜V2引擎 |
| https://cdn.uviewui.com/uview/album/10.jpg | 摸瓜V2引擎 |
| https://imgcache.qq.com/open/qcloud/tim/assets/emoji/ | 摸瓜V2引擎 |
| https://www.goeasy.io/cn/docs/goeasy-2.x/im/message/media/send-media-message.html | 摸瓜V2引擎 |
| https://secure.livechatinc.com/licence/18132384/v2/open\_chat.cgi?groups0 | 摸瓜V2引擎 |
| https://cdn.uviewui.com/uview/album/1.jpg | 摸瓜V2引擎 |
| https://cdn.uviewui.com/uview/album/2.jpg | 摸瓜V2引擎 |
| https://cdn.uviewui.com/uview/album/3.jpg | 摸瓜V2引擎 |
| https://cdn.uviewui.com/uview/album/4.jpg | 摸瓜V2引擎 |
| https://cdn.uviewui.com/uview/album/5.jpg | 摸瓜V2引擎 |
| https://cdn.uviewui.com/uview/album/6.jpg | 摸瓜V2引擎 |
| https://cdn.uviewui.com/uview/album/7.jpg | 摸瓜V2引擎 |
| https://cdn.uviewui.com/uview/album/8.jpg | 摸瓜V2引擎 |
| https://cdn.uviewui.com/uview/album/9.jpg | 摸瓜V2引擎 |
| https://cdn.uviewui.com/uview/album/10.jpg | 摸瓜V2引擎 |
| http://a | 摸瓜V2引擎 |
| http://a/c%20d?e=1 | 摸瓜V2引擎 |
| https://a@b | 摸瓜V2引擎 |
| http://a | 摸瓜V2引擎 |
| http://a/c%20d?e=1 | 摸瓜V2引擎 |
| https://a@b | 摸瓜V2引擎 |
| https://www.gjtool.cn | 摸瓜V2引擎 |
| https://unpkg.com/pdfjs-dist@2.0.943/cmaps/'; | 摸瓜V2引擎 |
| http://www.apache.org/licenses/LICENSE-2.0 | 摸瓜V2引擎 |
| https://github.com/ecomfe/zrender/blob/master/LICENSE.txt | 摸瓜V2引擎 |
| http://www.apache.org/licenses/LICENSE-2.0 | 摸瓜V2引擎 |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11041&is64=1 | 摸瓜V3引擎 |
| http://yuntuapi.amap.com | 摸瓜V3引擎 |
| https://mclient.alipay.com/cashier/mobilepay.htm | 摸瓜V3引擎 |
| http://apistore.amap.com | 摸瓜V3引擎 |
| https://restsdk.amap.com/v3/iasdkauth | 摸瓜V3引擎 |
| https://mclient.alipay.com/home/exterfaceAssign.htm? | 摸瓜V3引擎 |
| http://mpsapi.amap.com/ws/mps/lyrdata/ugc/ | 摸瓜V3引擎 |
| https://mobilegwpre.alipay.com/mgw.htm | 摸瓜V3引擎 |
| http://restsdk.amap.com/v3 | 摸瓜V3引擎 |
| https://restsdk.amap.com/rest/me/cpoint | 摸瓜V3引擎 |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11047&is64=0 | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android//com.taobao.weex.ui.view.listview.WXRecyclerView | 摸瓜V3引擎 |
| https://mclient.alipay.com/service/rest.htm | 摸瓜V3引擎 |
| https://wappaygw.alipay.com/home/exterfaceAssign.htm? | 摸瓜V3引擎 |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11047&is64=1 | 摸瓜V3引擎 |
| https://mobilegw.alipay.com/mgw.htm | 摸瓜V3引擎 |
| https://restsdk.amap.com/v4 | 摸瓜V3引擎 |
| https://ask.dcloud.net.cn/article/283 | 摸瓜V3引擎 |
| http://restapi.amap.com/rest/aaid/get | 摸瓜V3引擎 |
| https://ask.dcloud.net.cn/article/35877 | 摸瓜V3引擎 |
| https://lbs-3dtiles-service.amap.com/basemap/tiles/staging?compose=building | 摸瓜V3引擎 |
| https://ask.dcloud.net.cn/article/35058 | 摸瓜V3引擎 |
| http://wappaygw.alipay.com/service/rest.htm | 摸瓜V3引擎 |
| https://yuntuapi.amap.com | 摸瓜V3引擎 |
| http://restsdk.amap.com/v4/grasproad/driving? | 摸瓜V3引擎 |
| https://m5.amap.com/ws/mapapi/shortaddress/transform | 摸瓜V3引擎 |
| http://restsdk.amap.com/v4/gridmap? | 摸瓜V3引擎 |
| http://mclient.alipay.com/cashier/mobilepay.htm | 摸瓜V3引擎 |
| https://er.dcloud.io/sc | 摸瓜V3引擎 |
| https://ask.dcloud.net.cn/article/36199 | 摸瓜V3引擎 |
| https://restapi.amap.com/rest/aaid/get | 摸瓜V3引擎 |
| https://er.dcloud.net.cn/rv | 摸瓜V3引擎 |
| https://ask.dcloud.net.cn/article/282 | 摸瓜V3引擎 |
| https://er.dcloud.io/rv | 摸瓜V3引擎 |
| http://restsdk.amap.com/v3/place/text? | 摸瓜V3引擎 |
| https://mclient.alipay.com/home/exterfaceAssign.htm | 摸瓜V3引擎 |
| http://restsdk.amap.com/v3/place/around? | 摸瓜V3引擎 |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11041&is64=0 | 摸瓜V3引擎 |
| https://restapi.amap.com/rest/lbs/geohub/3d/tiles?z=%d&x=%d&y=%d&id= | 摸瓜V3引擎 |
| http://cgicol.amap.com/collection/collectData?src=baseCol&ver=v74& | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res-auto | 摸瓜V3引擎 |
| https://restsdk.amap.com/v3 | 摸瓜V3引擎 |
| https://wappaygw.alipay.com/service/rest.htm | 摸瓜V3引擎 |
| http://restsdk.amap.com | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android | 摸瓜V3引擎 |
| https://restsdk.amap.com/v5 | 摸瓜V3引擎 |
| https://er.dcloud.net.cn/sc | 摸瓜V3引擎 |
| http://restsdk.amap.com/v4 | 摸瓜V3引擎 |
| https://ask.dcloud.net.cn/article/35627 | 摸瓜V3引擎 |
| http://restsdk.amap.com/v3/config/district? | 摸瓜V3引擎 |
| http://restsdk.amap.com/rest/me/cpoint | 摸瓜V3引擎 |
| http://mclient.alipay.com/home/exterfaceAssign.htm | 摸瓜V3引擎 |
| https://apistore.amap.com | 摸瓜V3引擎 |
| https://restsdk.amap.com/sdk/compliance/params | 摸瓜V3引擎 |
| http://m5.amap.com/ws/mapapi/shortaddress/transform | 摸瓜V3引擎 |
| http://wprd0%d.is.autonavi.com/appmaptile? | 摸瓜V3引擎 |
| https://adiu.amap.com/ws/device/adius | 摸瓜V3引擎 |
| https://m3w.cn/s/ | 摸瓜V3引擎 |
| http://restsdk.amap.com/sdk/compliance/params | 摸瓜V3引擎 |
| http://restsdk.amap.com/v5 | 摸瓜V3引擎 |
| http://mclient.alipay.com/service/rest.htm | 摸瓜V3引擎 |
| https://android.googlesource.com/toolchain/llvm-project | 摸瓜V3引擎 |
| https://render.alipay.com/p/s/i?scheme=%s | 摸瓜V3引擎 |
| https://dualstack-arestapi.amap.com/v3/iasdkauth | 摸瓜V3引擎 |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| m8ch88l@gmail.com  robert@xarg.org  jhruby.web@gmail.com | 摸瓜V2引擎 |
| back@2x.png  v@2x.png  usdt@2x.png  bank@2x.png  daoda@2x.png  wuliu@2x.png | 摸瓜V2引擎 |
| emoji\_1@2x.png  emoji\_2@2x.png  emoji\_3@2x.png  emoji\_4@2x.png  emoji\_5@2x.png  emoji\_6@2x.png  emoji\_7@2x.png  emoji\_8@2x.png  emoji\_9@2x.png  emoji\_10@2x.png  emoji\_11@2x.png  emoji\_12@2x.png  emoji\_13@2x.png  emoji\_14@2x.png  emoji\_15@2x.png  emoji\_16@2x.png  emoji\_17@2x.png  emoji\_18@2x.png  emoji\_19@2x.png  emoji\_20@2x.png  emoji\_21@2x.png  emoji\_22@2x.png  emoji\_23@2x.png  emoji\_24@2x.png  emoji\_25@2x.png  emoji\_26@2x.png  emoji\_27@2x.png  emoji\_28@2x.png  emoji\_29@2x.png  emoji\_30@2x.png  emoji\_31@2x.png  emoji\_32@2x.png  emoji\_33@2x.png  emoji\_34@2x.png  emoji\_35@2x.png  emoji\_36@2x.png  emoji\_37@2x.png  emoji\_38@2x.png  emoji\_39@2x.png  emoji\_40@2x.png  emoji\_41@2x.png  emoji\_42@2x.png  emoji\_43@2x.png  emoji\_44@2x.png  emoji\_45@2x.png  emoji\_46@2x.png  emoji\_47@2x.png  emoji\_48@2x.png  emoji\_49@2x.png  emoji\_50@2x.png  emoji\_51@2x.png  emoji\_52@2x.png  emoji\_53@2x.png  emoji\_54@2x.png  emoji\_55@2x.png  emoji\_56@2x.png  emoji\_57@2x.png  emoji\_58@2x.png  emoji\_59@2x.png  emoji\_60@2x.png  emoji\_61@2x.png  emoji\_62@2x.png  emoji\_63@2x.png  emoji\_64@2x.png  emoji\_65@2x.png  emoji\_66@2x.png  emoji\_67@2x.png  emoji\_68@2x.png  emoji\_69@2x.png  emoji\_70@2x.png  emoji\_71@2x.png  emoji\_72@2x.png  emoji\_73@2x.png  emoji\_74@2x.png  emoji\_75@2x.png  emoji\_76@2x.png  emoji\_77@2x.png  emoji\_78@2x.png  emoji\_79@2x.png  emoji\_80@2x.png  emoji\_81@2x.png  emoji\_82@2x.png  emoji\_83@2x.png  emoji\_84@2x.png  emoji\_85@2x.png  emoji\_86@2x.png  emoji\_87@2x.png  emoji\_88@2x.png  emoji\_89@2x.png  emoji\_90@2x.png  emoji\_91@2x.png  emoji\_92@2x.png  emoji\_93@2x.png  emoji\_94@2x.png  emoji\_95@2x.png  emoji\_96@2x.png  emoji\_97@2x.png  emoji\_98@2x.png  emoji\_99@2x.png  emoji\_100@2x.png  emoji\_101@2x.png  emoji\_102@2x.png  emoji\_103@2x.png  emoji\_104@2x.png  emoji\_105@2x.png  emoji\_106@2x.png  emoji\_107@2x.png  emoji\_108@2x.png  emoji\_109@2x.png  emoji\_110@2x.png  emoji\_111@2x.png  emoji\_112@2x.png  emoji\_113@2x.png  emoji\_114@2x.png  emoji\_115@2x.png  emoji\_116@2x.png  emoji\_117@2x.png  emoji\_118@2x.png | 摸瓜V2引擎 |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869184 | tv/danmaku/ijk/media/player/IjkMediaMeta.java |
| 16487052358 | 摸瓜V2引擎 |

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: True 找到 1 个唯一证书 主题: C=CN, ST=, L=, O=Android, OU=Android, CN=1mDHEoFm5GW2o3%2BDkgVuEK0Nxd9guDEa14IjNqRo9m6PW%2BL5BhLFlIQJb1ZiE%2B%2FnWRiidKcvxJFgW1Hnf88dVg%3D%3D 签名算法: rsassa\_pkcs1v15 有效期自: 2025-04-02 07:39:09+00:00 有效期至: 2125-03-09 07:39:09+00:00 发行人: C=CN, ST=, L=, O=Android, OU=Android, CN=1mDHEoFm5GW2o3%2BDkgVuEK0Nxd9guDEa14IjNqRo9m6PW%2BL5BhLFlIQJb1ZiE%2B%2FnWRiidKcvxJFgW1Hnf88dVg%3D%3D 序列号: 0x1cebdea8 哈希算法: sha256 md5值: c94f3ec5abc61b8f89fb3ea39f5a14a9 sha1值: 9d775689b59302bb9c7304962cb2d3c88c55ec6e sha256值: 7dbfac179f0875a4843305bc0aa63ea95f9280867d5736d91d2284ffc6ab39a2 sha512值: bf4dd1848112a4c55e16892bc083293b2ea506d63a63706fba353a376411425b346f55c472743dde08b738aa20d1cb1532e63c7f0cd5de00b88d7942a98ea80a 公钥算法: rsa 密钥长度: 2048 指纹: d424f68e0b581a7d528cd92da3b4a43a83447edee030091f8fc5b07a91ff7981**

## **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" |
| "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.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.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.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.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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.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 |
| uni.UNI678app101.shuangfu.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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.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\_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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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\_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。 |
| android.permission.ACCESS\_LOCATION\_EXTRA\_COMMANDS | 正常 | 访问额外的位置提供程序命令 | 访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作 |

## **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。**