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

**Aixin（ 2.5.2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 | Aixin |
| 版本 | 2.5.2 |
| 包名 | com.news.gtablu |
| 域名线索 | 50条 |
| URL线索 | 37条 |
| APP图标 |  |
| 分析日期 | 2025年8月10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 | Aixin.apk |
| 文件大小 | 37.39MB |
| MD5值 | cea5f07e8b918802ac3c5424ace54b07 |
| SHA1值 | 1c343498de66e0def219d6060d4cae1e88917648 |
| SHA256值 | 4adef18fd1f02ce00eed0fb26a6f603e1f2e380acb439b20abe6d016be97706d |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | Aixin |
| 包名 | com.news.gtablu |
| 主活动Activity | io.dcloud.PandoraEntry |
| 安卓版本名称 | 2.5.2 |
| 安卓版本 | 20250602 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| ask.dcloud.net.cn | IP: 123.125.244.31  所属国家: China  地区: Beijing  城市: Beijing |
| er.dcloud.net.cn | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| www.aixinchat.xyz | IP: 154.12.25.22  所属国家: United States of America  地区: California  城市: Pasadena |
| m3w.cn | IP: 123.234.2.61  所属国家: China  地区: Shandong  城市: Qingdao |
| schemas.android.com | 没有服务器地理信息. |
| im.raingad.com | IP: 47.109.42.217  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| www.google.com | IP: 31.13.112.9  所属国家: Ireland  地区: Dublin  城市: Dublin |
| api.multiavatar.com | IP: 104.21.90.212  所属国家: United States of America  地区: California  城市: San Francisco |
| oss-cn-hangzhou.aliyuncs.com | IP: 118.31.219.232  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| api.next.bspapp.com | IP: 203.107.60.33  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| 203.107.1.1 | IP: 203.107.1.1  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| oss.aliyuncs.com | IP: 118.178.29.5  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| api.bspapp.com | IP: 39.96.249.142  所属国家: China  地区: Beijing  城市: Beijing |
| aixin-chat.oss-cn-hongkong.aliyuncs.com | IP: 47.79.64.213  所属国家: United States of America  地区: California  城市: San Mateo |
| pop.yuncloudauth.com | IP: 106.11.232.51  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| bugzilla.mozilla.org | IP: 34.110.178.183  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| cn-shanghai-aliyun-cloudauth.oss-cn-shanghai.aliyuncs.com | IP: 140.206.110.110  所属国家: China  地区: Shanghai  城市: Shanghai |
| gitee.com | IP: 180.76.199.13  所属国家: China  地区: Beijing  城市: Beijing |
| webapi.amap.com | IP: 27.221.122.9  所属国家: China  地区: Shandong  城市: Jinan |
| www.w3.org | IP: 104.18.23.19  所属国家: United States of America  地区: California  城市: San Francisco |
| cloudauth-dualstack.aliyuncs.com | IP: 106.11.172.8  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| er.dcloud.io | 没有服务器地理信息. |
| im.file.raingad.com | 没有服务器地理信息. |
| mgw.mpaas.cn-hangzhou.aliyuncs.com | IP: 47.118.168.189  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| render.alipay.com | IP: 116.196.143.230  所属国家: China  地区: Zhejiang  城市: Jinhua |
| apis.map.qq.com | IP: 116.130.223.114  所属国家: China  地区: Beijing  城市: Beijing |
| api.map.baidu.com | IP: 111.206.208.72  所属国家: China  地区: Beijing  城市: Beijing |
| cloudauth.aliyuncs.com | IP: 106.11.232.51  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| gist.github.com | IP: 243.185.187.39  所属国家: -  地区: -  城市: - |
| auth.yunverify.com | IP: 59.82.44.22  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 |
| bugs.chromium.org | IP: 142.250.73.147  所属国家: United States of America  地区: California  城市: Mountain View |
| tianshu.alicdn.com | IP: 175.19.126.219  所属国家: China  地区: Jilin  城市: Changchun |
| map.qq.com | IP: 116.130.224.19  所属国家: China  地区: Beijing  城市: Beijing |
| 127.0.0.1 | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| tools.ietf.org | IP: 104.16.44.99  所属国家: United States of America  地区: California  城市: San Francisco |
| draft.ortc.org | IP: 185.199.108.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| heycam.github.io | IP: 185.199.108.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| cloudauth-dualstack.cn-beijing.aliyuncs.com | IP: 39.97.154.8  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| image.cnamedomain.com | 没有服务器地理信息. |
| cloudauth.cn-beijing.aliyuncs.com | IP: 39.97.154.134  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| uniapp.dcloud.net.cn | IP: 123.125.244.31  所属国家: China  地区: Beijing  城市: Beijing |
| vuejs.org | IP: 15.197.167.90  所属国家: United States of America  地区: Washington  城市: Seattle |
| maps.googleapis.com | IP: 142.250.69.170  所属国家: United States of America  地区: California  城市: Mountain View |
| ns.adobe.com | 没有服务器地理信息. |
| rawgit.com | IP: 103.200.30.143  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| w3c.github.io | IP: 185.199.110.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| oss-cn-.aliyuncs.comor | 没有服务器地理信息. |
| service.dcloud.net.cn | IP: 111.229.199.57  所属国家: China  地区: Beijing  城市: Beijing |

### **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 |
| https://203.107.1.1/181345/d?host= | com/alibaba/sdk/android/oss/common/utils/HttpdnsMini.java |
| http://oss.aliyuncs.com | com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java |
| http://127.0.0.1 | com/alibaba/sdk/android/oss/internal/InternalRequestOperation.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://tianshu.alicdn.com/7504f3f0-aca8-4636-b486-e396559d3efb.png | 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 |
| http://schemas.android.com/apk/res/android | com/hjq/permissions/AndroidManifestParser.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://ask.dcloud.net.cn/article/283 | io/dcloud/feature/utsplugin/ProxyModule.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/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://render.alipay.com/p/yuyan/180020010001208736/aliyunFacewelcome.html | 摸瓜V1引擎 |
| https://github.com/uuidjs/uuid | 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://im.raingad.com/static/img/emoji/twitter/1f600.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f62c.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f601.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f602.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f923.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f973.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f974.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f979.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f603.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f604.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f605.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f606.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f607.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f608.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f609.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f60a.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f642.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f643.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/263a.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f60b.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f60c.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f60d.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f970.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f618.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f617.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f619.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f61a.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f61c.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f92a.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f928.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f9d0.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f61d.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f61b.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f911.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f913.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f60e.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f929.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f921.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f920.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f917.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f60f.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f636.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f610.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f611.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f612.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f644.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f914.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f925.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f927.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f92d.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f92b.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f92c.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f92f.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f633.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f61e.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f61f.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f620.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1f621.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1fae0.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1fae1.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1fae2.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1fae3.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1fae4.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1fae5.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/1faf0.png | 摸瓜V2引擎 |
| https://im.raingad.com/static/img/emoji/twitter/2639.png | 摸瓜V2引擎 |
| https://api.multiavatar.com/raingad1.png?apikey=zdvXV3W4MjwhP9 | 摸瓜V2引擎 |
| https://api.multiavatar.com/raingad2.png?apikey=zdvXV3W4MjwhP9 | 摸瓜V2引擎 |
| https://aixin-chat.oss-cn-hongkong.aliyuncs.com/17cb53661c644ed59850e037117b23eb.json?t=$ | 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://$ | 摸瓜V2引擎 |
| http://$ | 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://im.file.raingad.com/logo/logo.png | 摸瓜V2引擎 |
| https://gitee.com/raingad/instant-chat-uniapp.git | 摸瓜V2引擎 |
| https://www.aixinchat.xyz/static/img/wallet.png | 摸瓜V2引擎 |
| https://www.aixinchat.xyz/static/img/bj.png | 摸瓜V2引擎 |
| https://vuejs.org/error-reference/ | 摸瓜V2引擎 |
| https://service.dcloud.net.cn/uniapp/feedback.html | 摸瓜V2引擎 |
| https://map.qq.com/api/js?v=2.exp& | 摸瓜V2引擎 |
| https://maps.googleapis.com/maps/api/js? | 摸瓜V2引擎 |
| https://webapi.amap.com/maps?v=2.0& | 摸瓜V2引擎 |
| https://api.map.baidu.com/api?type=webgl&v=1.0& | 摸瓜V2引擎 |
| https://bugs.chromium.org/p/webrtc/issues/detail?id=7815 | 摸瓜V2引擎 |
| https://w3c.github.io/webrtc-stats/ | 摸瓜V2引擎 |
| https://w3c.github.io/webrtc-pc/ | 摸瓜V2引擎 |
| https://bugs.chromium.org/p/webrtc/issues/detail?id=8419 | 摸瓜V2引擎 |
| https://bugzilla.mozilla.org/show\_bug.cgi?id=1426831 | 摸瓜V2引擎 |
| https://bugzilla.mozilla.org/show\_bug.cgi?id=1425697 | 摸瓜V2引擎 |
| https://bugs.chromium.org/p/webrtc/issues/detail?id=6145 | 摸瓜V2引擎 |
| https://bugzilla.mozilla.org/show\_bug.cgi?id=1265827 | 摸瓜V2引擎 |
| https://bugs.chromium.org/p/chromium/issues/detail?id=978582 | 摸瓜V2引擎 |
| https://bugzilla.mozilla.org/show\_bug.cgi?id=1173851 | 摸瓜V2引擎 |
| https://github.com/webrtcHacks/adapter/issues/998 | 摸瓜V2引擎 |
| https://bugzilla.mozilla.org/show\_bug.cgi?id=1396918 | 摸瓜V2引擎 |
| https://heycam.github.io/webidl/ | 摸瓜V2引擎 |
| https://gist.github.com/jed/982883 | 摸瓜V2引擎 |
| https://rawgit.com/aboba/edgertc/master/msortc-rs4.html | 摸瓜V2引擎 |
| http://draft.ortc.org/ | 摸瓜V2引擎 |
| https://tools.ietf.org/html/draft-ietf-rtcweb-jsep-20 | 摸瓜V2引擎 |
| https://w3c.github.io/webrtc-pc/ | 摸瓜V2引擎 |
| https://bugs.chromium.org/p/webrtc/issues/detail?id=8419 | 摸瓜V2引擎 |
| https://bugzilla.mozilla.org/show\_bug.cgi?id=1426831 | 摸瓜V2引擎 |
| https://bugzilla.mozilla.org/show\_bug.cgi?id=1425697 | 摸瓜V2引擎 |
| https://bugs.chromium.org/p/webrtc/issues/detail?id=6145 | 摸瓜V2引擎 |
| https://bugzilla.mozilla.org/show\_bug.cgi?id=1265827 | 摸瓜V2引擎 |
| https://bugs.chromium.org/p/chromium/issues/detail?id=978582 | 摸瓜V2引擎 |
| https://bugs.chromium.org/p/webrtc/issues/detail?id=7815 | 摸瓜V2引擎 |
| https://w3c.github.io/webrtc-stats/ | 摸瓜V2引擎 |
| https://bugzilla.mozilla.org/show\_bug.cgi?id=1173851 | 摸瓜V2引擎 |
| https://github.com/webrtcHacks/adapter/issues/998 | 摸瓜V2引擎 |
| https://bugzilla.mozilla.org/show\_bug.cgi?id=1396918 | 摸瓜V2引擎 |
| https://heycam.github.io/webidl/ | 摸瓜V2引擎 |

### **4.3 邮箱线索**

### **4.4 手机号线索**

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

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: True 找到 1 个唯一证书 主题: C=beijing, ST=beijing, L=beijing, O=cf1749792605238, OU=qe1749792605238, CN=gvje 签名算法: rsassa\_pkcs1v15 有效期自: 2025-06-13 05:30:06+00:00 有效期至: 2075-06-01 05:30:06+00:00 发行人: C=beijing, ST=beijing, L=beijing, O=cf1749792605238, OU=qe1749792605238, CN=gvje 序列号: 0x7dbc4311 哈希算法: sha512 md5值: c25c8b602a6975b3aef54edbae9384a5 sha1值: 684ddf06d36ab0da173700f0282f5b3fd8a7edb2 sha256值: 5c3c5ee47f3dd8e19e4dbf4bce084a2d175fa5cefd280feb5efb8865205debab sha512值: 3781fb9f9db8b328a4ff4282742a5df8c3a96ae2d4141e9fbdf7ad8c26fdcfe8e40bfc5438e362446c04caedd425235ef50064395438761641831b431756e33f 公钥算法: rsa 密钥长度: 4096 指纹: 048ffc5dbeb66261b0f5a7b3dbc9716c9a171f2c5f62912cc35ed544a7b13903**

## **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 |
| 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 |
| com.news.gtablu.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.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.GET\_ACCOUNTS | 危险 | 列出帐户 | 允许访问账户服务中的账户列表 |
| android.permission.MANAGE\_APP\_TOKENS | 合法 | 管理应用程序令牌 | 允许应用程序创建和管理它们自己的令牌,绕过它们共同的 Z 排序。普通应用程序永远不需要 |
| android.permission.MANAGE\_DOCUMENTS | 合法 |  | 允许应用程序管理对文档的访问,通常作为文档选择器的一部分 |
| 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.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.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 |

## **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。**