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

**Yoke（ 1.0.0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 | Yoke |
| 版本 | 1.0.0 |
| 包名 | uni.UNI8B381C5 |
| 域名线索 | 61条 |
| URL线索 | 54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 | 6FE4KeFNWT\_0.apk |
| 文件大小 | 74.74MB |
| MD5值 | 97346b7efb1fe9c7ca967541e93c78c1 |
| SHA1值 | c00dc999edf1065575ae546032fb0da98b885974 |
| SHA256值 | 6f12f4341a923663d73e0ad02bfbc0e9b239cc795165c14a6f0d7acadb8c7750 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | Yoke |
| 包名 | uni.UNI8B381C5 |
| 主活动Activity | io.dcloud.PandoraEntry |
| 安卓版本名称 | 1.0.0 |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| map.qq.com | IP: 116.130.224.82 所属国家: China 地区: Beijing 城市: Beijing  |
| sdk-im-1252463788.cos.accelerate.myqcloud.com | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| miliaoyuyin.oss-cn-hongkong.aliyuncs.com | IP: 47.79.64.155 所属国家: United States of America 地区: California 城市: San Mateo  |
| underscorejs.org | IP: 104.21.25.112 所属国家: United States of America 地区: California 城市: San Francisco  |
| apiind.my-imcloud.com | IP: 124.64.207.114 所属国家: China 地区: Beijing 城市: Beijing  |
| quilljs.com | IP: 172.66.40.163 所属国家: United States of America 地区: California 城市: San Francisco  |
| en.wikipedia.org | IP: 199.59.148.20 所属国家: United States of America 地区: California 城市: San Francisco  |
| boce-cdn.my-imcloud.com | IP: 116.196.150.237 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| gtc.getui.nethttps | 没有服务器地理信息.  |
| im.sdk.qcloud.com | IP: 116.196.150.249 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| intl.cloud.tencent.com | IP: 60.28.220.193 所属国家: China 地区: Tianjin 城市: Tianjin  |
| feross.org | IP: 50.116.11.184 所属国家: United States of America 地区: California 城市: Fremont  |
| buy.cloud.tencent.com | IP: 60.28.220.193 所属国家: China 地区: Tianjin 城市: Tianjin  |
| ask.dcloud.net.cn | IP: 101.72.227.61 所属国家: China 地区: Hebei 城市: Langfang  |
| npms.io | IP: 104.21.64.1 所属国家: United States of America 地区: California 城市: San Francisco  |
| m3w.cn | IP: 116.196.151.14 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| c-hzgt2.getui.com | IP: 124.160.155.57 所属国家: China 地区: Zhejiang 城市: Jiaxing  |
| msg.cmpassport.com | IP: 112.33.111.188 所属国家: China 地区: Anhui 城市: Hefei  |
| web.sdk.qcloud.com | IP: 116.196.150.237 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| lodash.com | IP: 52.76.120.174 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| app.zdr19.com | IP: 61.48.83.196 所属国家: China 地区: Beijing 城市: Beijing  |
| id6.me | IP: 42.123.77.138 所属国家: China 地区: Beijing 城市: Beijing  |
| crbug.com | IP: 216.239.32.29 所属国家: United States of America 地区: California 城市: Mountain View  |
| d-gt.getui.com | 没有服务器地理信息.  |
| apiger.my-imcloud.com | IP: 124.64.207.14 所属国家: China 地区: Beijing 城市: Beijing  |
| apijpn.my-imcloud.com | IP: 106.55.123.101 所属国家: China 地区: Beijing 城市: Beijing  |
| api.bspapp.com | IP: 39.96.249.142 所属国家: China 地区: Beijing 城市: Beijing  |
| uniapp.dcloud.net.cn | IP: 220.194.123.111 所属国家: China 地区: Tianjin 城市: Tianjin  |
| www.google.com | IP: 31.13.94.36 所属国家: Argentina 地区: Ciudad Autonoma de Buenos Aires 城市: Buenos Aires  |
| zxid-m.mobileservice.cn | IP: 101.69.207.69 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| apis.map.qq.com | IP: 116.130.224.140 所属国家: China 地区: Beijing 城市: Beijing  |
| aid.mobileservice.cn | IP: 101.69.207.68 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| schemas.android.com | 没有服务器地理信息.  |
| sdk-im-1252463788.file.myqcloud.com | IP: 116.196.150.249 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| apikr.my-imcloud.com | IP: 124.64.207.114 所属国家: China 地区: Beijing 城市: Beijing  |
| www.tencentcloud.com | IP: 43.174.76.28 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| b-gtc.getui.nethttps | 没有服务器地理信息.  |
| 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.  |
| apisgp.my-imcloud.com | IP: 123.123.191.101 所属国家: China 地区: Beijing 城市: Beijing  |
| apiidn.my-imcloud.com | IP: 124.64.207.114 所属国家: China 地区: Beijing 城市: Beijing  |
| api.next.bspapp.com | IP: 203.107.60.33 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| demos.trtc.tencent-cloud.com | IP: 124.163.195.89 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| api.my-imcloud.com | IP: 60.29.232.36 所属国家: China 地区: Tianjin 城市: Tianjin  |
| c-gtc.getui.nethttps | 没有服务器地理信息.  |
| app.wqr88.com | IP: 61.48.83.224 所属国家: China 地区: Beijing 城市: Beijing  |
| marked.js.org | IP: 66.33.60.35 所属国家: Canada 地区: Ontario 城市: Etobicoke  |
| apiusa.my-imcloud.com | IP: 124.64.207.114 所属国家: China 地区: Beijing 城市: Beijing  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| cloud.tencent.com | IP: 60.28.220.193 所属国家: China 地区: Tianjin 城市: Tianjin  |
| events.im.qcloud.com | IP: 123.125.0.180 所属国家: China 地区: Beijing 城市: Beijing  |
| service.dcloud.net.cn | IP: 111.229.199.57 所属国家: China 地区: Beijing 城市: Beijing  |
| nisportal.10010.com | IP: 124.64.196.20 所属国家: China 地区: Beijing 城市: Beijing  |
| zhiliao.qq.com | IP: 116.196.151.115 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| momentjs.com | IP: 104.17.63.214 所属国家: United States of America 地区: California 城市: San Francisco  |
| er.dcloud.net.cn | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| openjsf.org | IP: 76.76.21.21 所属国家: United States of America 地区: California 城市: Walnut  |
| at.alicdn.com | IP: 101.72.238.65 所属国家: China 地区: Hebei 城市: Langfang  |
| sdk-im-1252463788.cos.ap-hongkong.myqcloud.com | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| er.dcloud.io | 没有服务器地理信息.  |
| sdk-open-phone.getui.com | IP: 101.68.218.175 所属国家: China 地区: Zhejiang 城市: Jiaxing  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://c-gtc.getui.net,https://c-gtc.gepush.com  | com/getui/gtc/c/b.java  |
| https://gtc.getui.net,https://gtc.gepush.com  | com/getui/gtc/c/b.java  |
| https://b-gtc.getui.net,https://b-gtc.gepush.com  | com/getui/gtc/c/b.java  |
| https://sdk-open-phone.getui.com/  | com/getui/gtc/i/d/b.java  |
| https://sdk-open-phone.getui.com/api.php  | com/igexin/push/a.java  |
| https://c-hzgt2.getui.com/api.php  | com/igexin/push/a.java  |
| https://d-gt.getui.com/api.htm  | com/igexin/push/a.java  |
| https://bi.  | com/igexin/push/config/h.java  |
| https://config.  | com/igexin/push/config/h.java  |
| https://bi.  | com/igexin/push/config/b.java  |
| https://config.  | com/igexin/push/config/b.java  |
| http://schemas.android.com/apk/res/android  | com/hjq/permissions/AndroidManifestParser.java  |
| https://im.sdk.qcloud.com/download/plus/8.5.6864/  | com/tencent/imsdk/manager/LibraryDownloader.java  |
| https://sdk-im-1252463788.cos.accelerate.myqcloud.com/download/plus/8.5.6864/  | com/tencent/imsdk/manager/LibraryDownloader.java  |
| https://sdk-im-1252463788.file.myqcloud.com/download/plus/8.5.6864/  | com/tencent/imsdk/manager/LibraryDownloader.java  |
| https://sdk-im-1252463788.cos.ap-hongkong.myqcloud.com/download/plus/8.5.6864/  | com/tencent/imsdk/manager/LibraryDownloader.java  |
| https://zhiliao.qq.com/  | com/tencent/qcloud/tuicore/TUIConstants.java  |
| https://cloud.tencent.com/document/product/269/32458  | com/tencent/qcloud/tuicore/TUIConstants.java  |
| https://intl.cloud.tencent.com/document/product/1047/36021?lang=en&pg=  | com/tencent/qcloud/tuicore/TUIConstants.java  |
| https://buy.cloud.tencent.com/avc?activeId=plugin&regionId=1  | com/tencent/qcloud/tuicore/TUIConstants.java  |
| https://cloud.tencent.com/document/product/269/11673?from=17219  | com/tencent/qcloud/tuicore/TUIConstants.java  |
| https://www.tencentcloud.com/document/product/1047/34349  | com/tencent/qcloud/tuicore/TUIConstants.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/conversation-backgroundImage/backgroundImage\_%s.png  | com/tencent/qcloud/tuicore/TUIConstants.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/conversation-backgroundImage/backgroundImage\_%s\_full.png  | com/tencent/qcloud/tuicore/TUIConstants.java  |
| https://demos.trtc.tencent-cloud.com/prod/base/v1/events/stat  | com/tencent/qcloud/tuicore/TUIConfig.java  |
| https://en.wikipedia.org/wiki/Blend\_modes\n//  | com/tencent/ugc/videoprocessor/transitions/StereoViewerFilter.java  |
| https://aid.mobileservice.cn/  | com/zx/a/I8b7/j3.java  |
| https://zxid-m.mobileservice.cn/sdk/config/v2/init  | com/zx/a/I8b7/n.java  |
| https://nisportal.10010.com:9001  | com/zx/a/I8b7/f1.java  |
| https://zxid-m.mobileservice.cn/sdk/config/init  | com/zx/a/I8b7/l.java  |
| https://zxid-m.mobileservice.cn/sdk/app/depAnalysis  | com/zx/a/I8b7/d1.java  |
| https://zxid-m.mobileservice.cn/sdk/module/getCoreModule  | com/zx/a/I8b7/f0.java  |
| https://zxid-m.mobileservice.cn/sdk/uaid/reportAuthToken  | com/zx/a/I8b7/v1.java  |
| https://zxid-m.mobileservice.cn/sdk/uaid/get  | com/zx/a/I8b7/w1.java  |
| https://zxid-m.mobileservice.cn/sdk/extend/tag  | com/zx/a/I8b7/b2.java  |
| https://zxid-m.mobileservice.cn/sdk/ext/pconfig  | com/zx/a/I8b7/f.java  |
| https://zxid-m.mobileservice.cn/sdk/channel/report  | com/zx/a/I8b7/p1.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://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/35058  | io/dcloud/feature/audio/AudioRecorderMgr.java  |
| https://ask.dcloud.net.cn/article/283  | io/dcloud/feature/utsplugin/ProxyModule.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://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://ask.dcloud.net.cn/article/283  | io/dcloud/g/b.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://service.dcloud.net.cn/uniapp/feedback.html  | 摸瓜V2引擎  |
| https://web.sdk.qcloud.com/component/TUIKit/assets/avatar\_21.png'  | 摸瓜V2引擎  |
| https://web.sdk.qcloud.com/im/demo/TUIkit/web/img/constomer.svg'  | 摸瓜V2引擎  |
| https://at.alicdn.com/t/font\_2225171\_8kdcwk4po24.ttf)  | 摸瓜V2引擎  |
| https://web.sdk.qcloud.com/component/TUIKit/assets/avatar\_21.png  | 摸瓜V2引擎  |
| https://web.sdk.qcloud.com/im/assets/emoji-plugin/  | 摸瓜V2引擎  |
| https://web.sdk.qcloud.com/im/assets/face-elem/  | 摸瓜V2引擎  |
| http://feross.org>  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/c1181d2cab0d4a68a90a42919fa8108d.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/1a7feb6b99ef4ba7a9abcfca01ef3894.PNG  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/b5b63e2c8f524d65adb6134fc7ecded4.JPG  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/2a06898947a3436c973baab949cb2fc3.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/c1181fc4deee440a859b72a4e4d7b804.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/47bbb136341e44ac9457c81090cd1d7c.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/04a798219cce4337950c355477865542.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/a49bb957ea61480385e0ddd410ce0431.JPG  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/78a76ae9586c4e39b757ca25db81a43f.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/f066e946dedd4354aab0b04ddf67f39c.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/db042a49b07749e5887d8313b02d3a6b.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/e19c98a0879b42a5a991873b27a4077d.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/c4434138e1b04133bfa95ece8b1962f4.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/c6e5d3bf032a4184a5a42f04b7387a68.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/c326d2a6081b4f7eb9cb23acb24cd8bd.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/efbf0e3c3a9346518580551014ce0735.png  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/860f8bfdef6f4ec78714445e17346277.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/2647ca606b91415f96f98eea8e56727c.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/f776ed0da8e54844961b219812552305.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/63f4544851744a3da69fd008d12b151b.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/711d2c26b3da455d9383f2819d9a25e2.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/1d9cd41d29dc4d86a112f8f39146c2e8.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/b3c6223bc35f4e7d869288875dc73ebf.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/efdaae9229654ae6889dd960af6a8f5e.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/b537d0ec25a446e1bcedce1ac0e6448c.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/86697373fe6440928dcfc7ea1c4d6334.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/423cecf409e944468ac7bd5d006bf7db.png  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/65df103739f04104b80cec6f12d122be.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/ae051b6e9ecf40c0912de24a0dd88233.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/c9b2663b73fd489398449d1d6c48991c.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/3b909c5922644420b2340b47bb6f1b14.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/8da1561797cb4b69a835a1f7589a5543.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/7721fb735225428c99b3556af9ba252a.webp  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/b044291fb95248bf9fc584bc37a612ee.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/4a3c854f3dd34055804609820bce7a45.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/e06e49c21c3a45b2b628585ebb01b1b7.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/817444a96c0847bfbf6ab106ee5d5fdc.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/6fe5a155ab0349b98b5d38286753329e.PNG  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/f4e1ab08f7d04e6fa2fb279f54cf3510.webp  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/1d03b6dfb3b6428fa6d5af339a8cee6c.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/183417c38ed2448f94ac31debe0f1803.JPG  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/14a0ad970a1e4e0992a733bab46b9965.JPG  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/825c26801da8469ebebe4951cfcb1659.png  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/5a44c88f943e44c996d6225a8d777a92.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/aa30291a26f94cec89f8f43951df2851.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/1d698231b2634727aa7ae93de50ee6c7.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/667fcf1ab31f4132a057b88e98bb8da7.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/c91a5a69c3a14b6aa4877e24d45065e8.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/6eed45b557f54663b2738fbc8ee427d0.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/96e0515329d74cfebef5fff940b8c777.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/59e89557635f4d61bd72c0e350135948.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/3a254d58942a4ace92b03256cc8d49ef.jpg  | 摸瓜V2引擎  |
| http://miliaoyuyin.oss-cn-hongkong.aliyuncs.com/image/749ad122f6064bb4ae95e1e5dd6dcc5e.jpg  | 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://web.sdk.qcloud.com/im/assets/images/Public.svg  | 摸瓜V2引擎  |
| https://web.sdk.qcloud.com/component/TUIKit/assets/file-  | 摸瓜V2引擎  |
| https://web.sdk.qcloud.com/component/TUIKit/assets/message-search.svg  | 摸瓜V2引擎  |
| https://web.sdk.qcloud.com/im/demo/TUIkit/web/img/constomer.svg  | 摸瓜V2引擎  |
| https://cloud.tencent.com/document/product/269/1499  | 摸瓜V2引擎  |
| https://web.sdk.qcloud.com/im/doc/zh-cn/SDK.html  | 摸瓜V2引擎  |
| https://cloud.tencent.com/apply/p/xc3oaubi98g  | 摸瓜V2引擎  |
| https://cloud.tencent.com/document/product/269/79861  | 摸瓜V2引擎  |
| https://cloud.tencent.com/document/product/1640/79968  | 摸瓜V2引擎  |
| https://web.sdk.qcloud.com/component/TUIKit/assets/avatar\_16.png  | 摸瓜V2引擎  |
| https://web.sdk.qcloud.com/im/demo/TUIkit/web/img/constomer.png  | 摸瓜V2引擎  |
| https://web.sdk.qcloud.com/component/TUIKit/assets/group\_avatar.png  | 摸瓜V2引擎  |
| https://map.qq.com/?type=marker&isopeninfowin=1&markertype=1&  | 摸瓜V2引擎  |
| https://apis.map.qq.com/ws/staticmap/v2/?  | 摸瓜V2引擎  |
| https://events.im.qcloud.com  | 摸瓜V2引擎  |
| https://api.my-imcloud.com  | 摸瓜V2引擎  |
| https://apisgp.my-imcloud.com  | 摸瓜V2引擎  |
| https://apikr.my-imcloud.com  | 摸瓜V2引擎  |
| https://apiger.my-imcloud.com  | 摸瓜V2引擎  |
| https://apiind.my-imcloud.com  | 摸瓜V2引擎  |
| https://apijpn.my-imcloud.com  | 摸瓜V2引擎  |
| https://apiusa.my-imcloud.com  | 摸瓜V2引擎  |
| https://apiidn.my-imcloud.com  | 摸瓜V2引擎  |
| https://boce-cdn.my-imcloud.com/v3/netcheck/getconninfo?  | 摸瓜V2引擎  |
| https://web.sdk.qcloud.com/im/download/error-message/v3/0.0.7/tim-error-message.txt  | 摸瓜V2引擎  |
| https://web.sdk.qcloud.com/im/doc/v3/zh-cn/SDK.html  | 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  |
| http://momentjs.com/guides/  | 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://web.sdk.qcloud.com/component/TUIKit/assets/has\_risk\_default.png  | 摸瓜V2引擎  |
| https://web.sdk.qcloud.com/im/assets/images/Meeting.svg  | 摸瓜V2引擎  |
| https://web.sdk.qcloud.com/im/assets/images/Work.svg  | 摸瓜V2引擎  |
| https://web.sdk.qcloud.com/im/assets/images/AVChatroom.svg  | 摸瓜V2引擎  |
| https://web.sdk.qcloud.com/im/assets/images/Community.png  | 摸瓜V2引擎  |
| https://app.zdr19.com/app/renzheng/saveshipin  | 摸瓜V2引擎  |
| https://marked.js.org/  | 摸瓜V2引擎  |
| https://github.com/markedjs/marked.  | 摸瓜V2引擎  |
| https://web.sdk.qcloud.com/im/assets/images/at.svg  | 摸瓜V2引擎  |
| https://app.wqr88.com  | 摸瓜V2引擎  |
| https://web.sdk.qcloud.com/im/assets/images/  | 摸瓜V2引擎  |
| https://quilljs.com/  | 摸瓜V2引擎  |
| https://quilljs.com  | 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://apis.map.qq.com/jsapi?qt=translate&type=1&points=  | 摸瓜V2引擎  |
| https://github.com/facebook/regenerator/blob/main/LICENSE  | 摸瓜V2引擎  |
| https://at.alicdn.com/t/font\_2225171\_8kdcwk4po24.ttf  | 摸瓜V2引擎  |
| https://app.wqr88.com  | 摸瓜V2引擎  |
| https://github.com/facebook/regenerator/blob/main/LICENSE  | 摸瓜V2引擎  |
| https://at.alicdn.com/t/font\_2225171\_8kdcwk4po24.ttf  | 摸瓜V2引擎  |
| https://app.wqr88.com  | 摸瓜V2引擎  |
| https://at.alicdn.com/t/font\_2225171\_8kdcwk4po24.ttf  | 摸瓜V2引擎  |
| https://github.com/facebook/regenerator/blob/main/LICENSE  | 摸瓜V2引擎  |
| https://at.alicdn.com/t/font\_2225171\_8kdcwk4po24.ttf  | 摸瓜V2引擎  |
| https://app.wqr88.com  | 摸瓜V2引擎  |
| https://at.alicdn.com/t/font\_2225171\_8kdcwk4po24.ttf  | 摸瓜V2引擎  |
| https://zxid-m.mobileservice.cn/sdk/said/ping  | lib/arm64-v8a/libzxprotect.so  |
| https://id6.me/gw/preuniq.do  | lib/arm64-v8a/libzxprotect.so  |
| https://msg.cmpassport.com/h5/getMobile  | lib/arm64-v8a/libzxprotect.so  |
| https://nisportal.10010.com:9001  | lib/arm64-v8a/libzxprotect.so  |
| https://crbug.com/v8/8520  | lib/arm64-v8a/libweexjss.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| xxx@email.elided  | com/tencent/liteav/base/PiiElider.java  |
| emoji\_0@2x.png 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 jhruby.web@gmail.com  | 摸瓜V2引擎  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 14159265358  | com/tencent/ugc/videoprocessor/transitions/BounceFilter.java  |
| 17179869184  | tv/danmaku/ijk/media/player/IjkMediaMeta.java  |

## **5. 签名证书**

**APK已签名 v1 签名: False v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: C=CN, ST=Beijing, L=Beijing, O=LCsIIoeJ, OU=RuoCldoc, CN=wcbHqnjo 签名算法: dsa 有效期自: 2025-06-24 12:36:25+00:00 有效期至: 2030-09-28 12:36:25+00:00 发行人: C=CN, ST=Beijing, L=Beijing, O=LCsIIoeJ, OU=RuoCldoc, CN=wcbHqnjo 序列号: 0x7e2777fe 哈希算法: sha256 md5值: 9c80d2245265f15844f4de67db8f68e0 sha1值: 762081eddaae5f68670cd15ca0837cb06c68bc88 sha256值: 367e230e8856f76f774edc51bf014e6906a6630d19736708e7c5853058fab8ae sha512值: 6fa2b2c38f247784dcf113a6d86ccc3bb779e2816701fecba48406c9d118bd03a0094cde0d28d9c6b66def1106496769fa6778a1b83bfa3940082b7a8a29e136 公钥算法: dsa 密钥长度: 2048 指纹: 51b1f0419604c44cd004ebfd504e8bc849dd81649860749f1651dcc620df26ed**

## **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 |
| getui.permission.GetuiService.uni.UNI8B381C5 | 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 |
| 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 |
| 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 |
| com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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.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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.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.BLUETOOTH | 正常 | 创建蓝牙连接 | 允许应用程序连接到配对的蓝牙设备 |
| android.permission.BLUETOOTH\_ADMIN | 正常 | 蓝牙管理 | 允许应用程序发现和配对蓝牙设备。  |
| android.permission.BLUETOOTH\_CONNECT | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FOREGROUND\_SERVICE\_CAMERA | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FOREGROUND\_SERVICE\_MICROPHONE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FOREGROUND\_SERVICE\_MEDIA\_PLAYBACK | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.GET\_TASKS | 危险 | 检索正在运行的应用程序 | 允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息 |
| android.permission.SCHEDULE\_EXACT\_ALARM | 正常 |  | 允许应用程序使用精确的警报调度 API 来执行对时间敏感的后台工作 |
| 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.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\_BACKGROUND\_LOCATION | 危险 | 后台访问位置 | 允许应用程序在后台访问位置 |
| 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.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.GET\_ACCOUNTS | 危险 | 列出帐户 | 允许访问账户服务中的账户列表 |
| 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.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.READ\_SMS | 危险 | 阅读短信或彩信 | 允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息 |
| android.permission.READ\_CALL\_LOG | 危险 |  | 允许应用程序读取用户的通话日志 |
| android.permission.WRITE\_CALL\_LOG | 危险 |  | 允许应用程序写入（但不读取）用户号召日志数据。 |
| 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.ACCESS\_NOTIFICATION\_POLICY | 正常 |  | 希望访问通知策略的应用程序的标记权限。 |
| android.permission.WRITE\_CONTACTS | 危险 | 写入联系人数据 | 允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可以使用它来删除或修改您的联系人数据 |
| android.permission.READ\_CONTACTS | 危险 | 读取联系人数据 | 允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人 |
| android.permission.FOREGROUND\_SERVICE\_MEDIA\_PROJECTION | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| io.dcloud.PandoraEntry | **Schemes**: unipush://, **Hosts:** io.dcloud.unipush, **Paths:** /,  |

**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。**