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

**英大证券机构版（ 8.2.9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 | 英大证券机构版 |
| 版本 | 8.2.9 |
| 包名 | com.yingda.app |
| 域名线索 | 84条 |
| URL线索 | 43条 |
| APP图标 |  |
| 分析日期 | 2025年6月16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 | 英大证券机构版\_2024年11月12日10点04分.apk |
| 文件大小 | 29.74MB |
| MD5值 | 7cbea8b9ab0a77aa3ae397be1b25e55f |
| SHA1值 | 01362aa5155da9182df96b8c4eeda540228a3773 |
| SHA256值 | e7d127511ab7c584e876b80a37da08d7dfeeb9acd75143d8e71154fb0788710d |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 英大证券机构版 |
| 包名 | com.yingda.app |
| 主活动Activity | io.dcloud.PandoraEntry |
| 安卓版本名称 | 8.2.9 |
| 安卓版本 | 829 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| ask.dcloud.net.cn | IP: 220.194.123.111 所属国家: China 地区: Tianjin 城市: Tianjin  |
| www.64lines.com | 没有服务器地理信息.  |
| www.jpeg.org | IP: 176.58.118.251 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: London  |
| en.wikipedia.org | IP: 103.102.166.224 所属国家: United States of America 地区: Indiana 城市: Francisco  |
| er.dcloud.io | 没有服务器地理信息.  |
| debugx5.qq.com | IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin  |
| tbsrecovery.imtt.qq.com | IP: 61.181.204.91 所属国家: China 地区: Tianjin 城市: Tianjin  |
| rumkin.com | IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| developer.yahoo.com | IP: 69.147.80.12 所属国家: United States of America 地区: New York 城市: New York City  |
| log.tbs.qq.com | IP: 124.95.224.248 所属国家: China 地区: Liaoning 城市: Shenyang  |
| api.next.bspapp.com | IP: 203.107.60.33 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| code.google.com | IP: 142.251.33.110 所属国家: Canada 地区: Ontario 城市: Toronto  |
| ns.adobe.com | 没有服务器地理信息.  |
| www.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.libpng.org | IP: 216.105.38.10 所属国家: United States of America 地区: California 城市: San Diego  |
| www.adobe.com | IP: 60.210.22.232 所属国家: China 地区: Shandong 城市: Zibo  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| push2his.eastmoney.com | IP: 114.55.106.209 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| eligrey.com | IP: 104.236.163.66 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.ietf.org | IP: 104.16.45.99 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| tbs.imtt.qq.com | IP: 42.231.138.59 所属国家: China 地区: Henan 城市: Nanyang  |
| labs.rampinteractive.co.uk | IP: 52.92.36.52 所属国家: Ireland 地区: Dublin 城市: Dublin  |
| dev.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| cdn.liqunonline.cn | IP: 156.250.19.39 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| images.xyduo.com | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| animate.style | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| myapph.requestcatcher.com | IP: 104.248.184.153 所属国家: United States of America 地区: California 城市: Santa Clara  |
| yingda2-fef196566a068882.elb.ap-east-1.amazonaws.com | IP: 18.166.16.103 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| www.github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| debugtbs.qq.com | IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin  |
| jquery.com | IP: 104.18.155.119 所属国家: United States of America 地区: California 城市: San Francisco  |
| cdn.rawgit.com | IP: 65.49.26.98 所属国家: United States of America 地区: Missouri 城市: Saint Louis  |
| cdnjs.cloudflare.com | IP: 104.17.25.14 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.phpied.com | IP: 75.119.204.26 所属国家: United States of America 地区: California 城市: Brea  |
| purl.eligrey.com | IP: 104.236.163.66 所属国家: United States of America 地区: California 城市: San Francisco  |
| jsperf.com | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| mgran.blogspot.com | IP: 104.244.46.244 所属国家: United States of America 地区: California 城市: San Francisco  |
| brett-zamir.me | IP: 143.95.253.117 所属国家: United States of America 地区: Florida 城市: Jacksonville  |
| qiniu.zdbty.net | IP: 101.69.128.55 所属国家: China 地区: Zhejiang 城市: Ningbo  |
| opensource.zealink.com | 没有服务器地理信息.  |
| kevin.vanzonneveld.net | IP: 52.55.160.175 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| m3w.cn | IP: 101.72.233.67 所属国家: China 地区: Hebei 城市: Langfang  |
| www.poynton.com | IP: 23.180.104.34 所属国家: - 地区: - 城市: -  |
| quilljs.com | IP: 172.66.43.93 所属国家: United States of America 地区: California 城市: San Francisco  |
| brandon.aaron.sh | IP: 104.21.29.184 所属国家: United States of America 地区: California 城市: San Francisco  |
| example.com | IP: 93.184.215.14 所属国家: United States of America 地区: California 城市: Los Angeles  |
| html2canvas.hertzen.com | IP: 172.67.140.170 所属国家: United States of America 地区: California 城市: San Francisco  |
| jspdf.default.namespaceuri | 没有服务器地理信息.  |
| www.loicminghetti.net | IP: 213.186.33.3 所属国家: France 地区: Ile-de-France 城市: Paris  |
| opensource.org | IP: 172.67.197.41 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.google.com | IP: 31.13.94.36 所属国家: Argentina 地区: Ciudad Autonoma de Buenos Aires 城市: Buenos Aires  |
| 106.75.213.118 | IP: 106.75.213.118 所属国家: China 地区: Shanghai 城市: Shanghai  |
| hangzhou-2.zos.ctyun.cn | IP: 60.190.235.243 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| crbug.com | IP: 216.239.32.29 所属国家: United States of America 地区: California 城市: Mountain View  |
| hertzen.com | IP: 172.67.140.170 所属国家: United States of America 地区: California 城市: San Francisco  |
| dojofoundation.org | IP: 104.18.4.155 所属国家: United States of America 地区: California 城市: San Francisco  |
| bugzilla.mozilla.org | IP: 34.110.178.183 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| pms.mb.qq.com | IP: 60.28.172.238 所属国家: China 地区: Tianjin 城市: Tianjin  |
| apis.map.qq.com | IP: 116.130.223.114 所属国家: China 地区: Beijing 城市: Beijing  |
| www.color.org | IP: 104.26.4.216 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.math.ubc.ca | IP: 137.82.155.105 所属国家: Canada 地区: British Columbia 城市: Vancouver  |
| uniapp.dcloud.net.cn | IP: 221.204.43.106 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| tools.ietf.org | IP: 104.16.44.99 所属国家: United States of America 地区: California 城市: San Francisco  |
| opensourcecache.zealink.com | 没有服务器地理信息.  |
| jsfiddle.net | IP: 104.21.49.15 所属国家: United States of America 地区: California 城市: San Francisco  |
| kjur.github.io | IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| developer.mozilla.org | IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| mathiasbynens.be | IP: 83.137.145.144 所属国家: Netherlands 地区: Groningen 城市: Groningen  |
| mdc.html5.qq.com | IP: 125.39.196.199 所属国家: China 地区: Tianjin 城市: Tianjin  |
| kukawski.pl | IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| developer.apple.com | IP: 17.253.87.200 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| www.wolframalpha.com | IP: 140.177.50.14 所属国家: United States of America 地区: Illinois 城市: Champaign  |
| hansmuller-flex.blogspot.com | IP: 104.244.46.85 所属国家: United States of America 地区: California 城市: San Francisco  |
| er.dcloud.net.cn | IP: 43.142.57.168 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  |
| plugins.jquery.com | IP: 104.131.8.164 所属国家: United States of America 地区: New Jersey 城市: Clifton  |
| www.brucelindbloom.com | IP: 66.175.58.9 所属国家: Canada 地区: Ontario 城市: Waterloo  |
| mqqad.html5.qq.com | IP: 0.0.0.1 所属国家: - 地区: - 城市: -  |
| phpjs.org | IP: 52.55.160.175 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| rjwagner49.com | IP: 67.20.98.29 所属国家: United States of America 地区: Utah 城市: Provo  |
| service.dcloud.net.cn | IP: 111.229.199.57 所属国家: China 地区: Beijing 城市: Beijing  |
| schemas.android.com | 没有服务器地理信息.  |
| cfg.imtt.qq.com | IP: 60.28.172.238 所属国家: China 地区: Tianjin 城市: Tianjin  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| 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=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://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://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/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://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/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://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://myapph.requestcatcher.com/test  | 摸瓜V2引擎  |
| https://opensourcecache.zealink.com/cache/minuteday/day/  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://developer.yahoo.com/yui/license.html  | 摸瓜V2引擎  |
| https://kjur.github.io/jsrsasign/license/  | 摸瓜V2引擎  |
| https://qiniu.zdbty.net/g8LtkTUpJjDh.gif  | 摸瓜V2引擎  |
| https://push2his.eastmoney.com/api  | 摸瓜V2引擎  |
| https://opensource.zealink.com  | 摸瓜V2引擎  |
| https://opensourcecache.zealink.com  | 摸瓜V2引擎  |
| https://opensource.zealink.com/API/StockHistoryDay  | 摸瓜V2引擎  |
| https://opensource.zealink.com/API/FactorTiming  | 摸瓜V2引擎  |
| https://opensource.zealink.com/API/MarketAttention  | 摸瓜V2引擎  |
| https://opensource.zealink.com/API/MarketHeat  | 摸瓜V2引擎  |
| https://opensource.zealink.com/API/QuadrantCalculate  | 摸瓜V2引擎  |
| http://images.xyduo.com  | 摸瓜V2引擎  |
| https://hangzhou-2.zos.ctyun.cn:10443/bucket-d1112/yingda2d1prod1112.json  | 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://github.com/facebook/regenerator/blob/main/LICENSE  | 摸瓜V2引擎  |
| https://github.com/Yaffle/EventSource/  | 摸瓜V2引擎  |
| https://animate.style/\r\n  | 摸瓜V2引擎  |
| http://opensource.org/licenses/MIT\r\n  | 摸瓜V2引擎  |
| http://cdn.liqunonline.cn/temp/202274/%E6%B8%90%E5%8F%98%E8%83%8C%E6%99%AF@2x.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  |
| http://yingda2-fef196566a068882.elb.ap-east-1.amazonaws.com  | 摸瓜V2引擎  |
| http://106.75.213.118:8022  | 摸瓜V2引擎  |
| https://html2canvas.hertzen.com>  | 摸瓜V2引擎  |
| https://hertzen.com>  | 摸瓜V2引擎  |
| https://cdnjs.cloudflare.com/ajax/libs/pdfobject/2.1.1/pdfobject.min.js  | 摸瓜V2引擎  |
| http://jspdf.default.namespaceuri/  | 摸瓜V2引擎  |
| http://brandon.aaron.sh)  | 摸瓜V2引擎  |
| https://github.com/timmywil/jquery.panzoom/blob/master/MIT-License.txt  | 摸瓜V2引擎  |
| https://github.com/louisremi/jquery.transform.js)  | 摸瓜V2引擎  |
| https://github.com/florianguenther/zui53  | 摸瓜V2引擎  |
| https://github.com/timmywil/jquery.panzoom/issues/90  | 摸瓜V2引擎  |
| http://www.loicminghetti.net  | 摸瓜V2引擎  |
| https://github.com/loicminghetti/TouchPDF-Jquery-Plugin  | 摸瓜V2引擎  |
| http://plugins.jquery.com/project/touchPDF  | 摸瓜V2引擎  |
| http://jquery.com/).  | 摸瓜V2引擎  |
| http://jquery.com/)  | 摸瓜V2引擎  |
| http://www.github.com/mattbryson  | 摸瓜V2引擎  |
| https://github.com/mattbryson/TouchSwipe-Jquery-Plugin  | 摸瓜V2引擎  |
| http://labs.rampinteractive.co.uk/touchSwipe/  | 摸瓜V2引擎  |
| http://plugins.jquery.com/project/touchSwipe  | 摸瓜V2引擎  |
| http://code.google.com/p/jquery-ui-for-ipad-and-iphone/  | 摸瓜V2引擎  |
| https://github.com/joelhy)  | 摸瓜V2引擎  |
| https://github.com/mattbryson/TouchSwipe-Jquery-Plugin/issues/206  | 摸瓜V2引擎  |
| http://jquery.com/).  | 摸瓜V2引擎  |
| http://jquery.com/)  | 摸瓜V2引擎  |
| https://github.com/MrRio/jsPDF  | 摸瓜V2引擎  |
| https://github.com/acspike  | 摸瓜V2引擎  |
| https://github.com/pablohess  | 摸瓜V2引擎  |
| https://github.com/fjenett  | 摸瓜V2引擎  |
| https://github.com/warrenweckesser  | 摸瓜V2引擎  |
| https://github.com/lifof  | 摸瓜V2引擎  |
| https://github.com/lsdriscoll  | 摸瓜V2引擎  |
| https://github.com/stefslon  | 摸瓜V2引擎  |
| https://github.com/jmorel  | 摸瓜V2引擎  |
| https://github.com/chris-rock  | 摸瓜V2引擎  |
| https://github.com/juanpgaviria  | 摸瓜V2引擎  |
| https://github.com/dollaruw  | 摸瓜V2引擎  |
| https://github.com/diegocr  | 摸瓜V2引擎  |
| https://github.com/Flamenco  | 摸瓜V2引擎  |
| https://github.com/Gavvers  | 摸瓜V2引擎  |
| https://github.com/BiggA94  | 摸瓜V2引擎  |
| http://opensource.org/licenses/mit-license  | 摸瓜V2引擎  |
| https://github.com/niklasvh/html2canvas)  | 摸瓜V2引擎  |
| https://github.com/cburgmer/rasterizeHTML.js)  | 摸瓜V2引擎  |
| https://cdn.rawgit.com/MrRio/jsPDF/master/examples/html2pdf/showcase\_supported\_html.html)  | 摸瓜V2引擎  |
| https://github.com/niklasvh/html2canvas'  | 摸瓜V2引擎  |
| https://github.com/cburgmer/rasterizeHTML.js');  | 摸瓜V2引擎  |
| https://github.com/siefkenj/  | 摸瓜V2引擎  |
| https://github.com/gingerchris  | 摸瓜V2引擎  |
| https://github.com/ineedfat  | 摸瓜V2引擎  |
| https://github.com/eaparango  | 摸瓜V2引擎  |
| https://github.com/burnburnrocket  | 摸瓜V2引擎  |
| https://github.com/jamesbrobb  | 摸瓜V2引擎  |
| https://en.wikipedia.org/wiki/List\_of\_file\_signatures  | 摸瓜V2引擎  |
| http://jsperf.com/encoding-xhr-image-data/31  | 摸瓜V2引擎  |
| http://www.64lines.com/jpeg-width-height  | 摸瓜V2引擎  |
| http://mgran.blogspot.com]  | 摸瓜V2引擎  |
| https://github.com/Rob--W/pdf.js/commit/c676ecb5a0f54677b9f3340c3ef2cf42225453bb  | 摸瓜V2引擎  |
| http://hansmuller-flex.blogspot.com/2011/10/more-about-approximating-circular-arcs.html  | 摸瓜V2引擎  |
| https://github.com/danielhusar  | 摸瓜V2引擎  |
| https://github.com/woolfg  | 摸瓜V2引擎  |
| https://github.com/flamenco  | 摸瓜V2引擎  |
| http://www.libpng.org/pub/png/book/chapter09.html  | 摸瓜V2引擎  |
| http://www.ietf.org/rfc/rfc1950.txt  | 摸瓜V2引擎  |
| http://jspdf.default.namespaceuri/  | 摸瓜V2引擎  |
| http://eligrey.com  | 摸瓜V2引擎  |
| https://github.com/dsamarin  | 摸瓜V2引擎  |
| https://github.com/eligrey/Blob.js/blob/master/LICENSE.md  | 摸瓜V2引擎  |
| http://purl.eligrey.com/github/Blob.js/blob/master/Blob.js  | 摸瓜V2引擎  |
| https://github.com/eligrey/FileSaver.js/blob/master/LICENSE.md  | 摸瓜V2引擎  |
| http://purl.eligrey.com/github/FileSaver.js/blob/master/FileSaver.js  | 摸瓜V2引擎  |
| https://developer.apple.com/library/safari/documentation/Tools/Conceptual/SafariExtensionGuide/WorkingwithWindowsandTabs/WorkingwithWindowsandTabs.html  | 摸瓜V2引擎  |
| https://github.com/deanm/omggif  | 摸瓜V2引擎  |
| http://www.phpied.com/rgb-color-parser-in-javascript/  | 摸瓜V2引擎  |
| http://html2canvas.hertzen.com>  | 摸瓜V2引擎  |
| http://mathiasbynens.be/notes/javascript-encoding>  | 摸瓜V2引擎  |
| http://tools.ietf.org/html/rfc3492  | 摸瓜V2引擎  |
| https://developer.mozilla.org/docs/Web/CSS/angle  | 摸瓜V2引擎  |
| http://jsfiddle.net/niklasvh/2e48b/  | 摸瓜V2引擎  |
| https://github.com/niklasvh/base64-arraybuffer  | 摸瓜V2引擎  |
| https://github.com/andreasgal/pdf.js  | 摸瓜V2引擎  |
| https://github.com/paulmillr/console-polyfill  | 摸瓜V2引擎  |
| http://phpjs.org/functions/base64\_encode/  | 摸瓜V2引擎  |
| http://rumkin.com)  | 摸瓜V2引擎  |
| http://kevin.vanzonneveld.net)  | 摸瓜V2引擎  |
| http://kukawski.pl)  | 摸瓜V2引擎  |
| http://phpjs.org/functions/base64\_decode/  | 摸瓜V2引擎  |
| http://brett-zamir.me)  | 摸瓜V2引擎  |
| https://github.com/MrRio/jsPDF  | 摸瓜V2引擎  |
| http://dojofoundation.org/license  | 摸瓜V2引擎  |
| https://github.com/siefkenj/  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| https://github.com/davidchambers/Base64.js  | 摸瓜V2引擎  |
| https://github.com/mozilla/pdf.js/issues/3260  | 摸瓜V2引擎  |
| https://github.com/mozilla/pdf.js/issues/3381.  | 摸瓜V2引擎  |
| https://crbug.com/442318  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://tools.ietf.org/html/rfc3986  | 摸瓜V2引擎  |
| https://bugzilla.mozilla.org/show\_bug.cgi?id=810490  | 摸瓜V2引擎  |
| https://bugzilla.mozilla.org/show\_bug.cgi?id=683280  | 摸瓜V2引擎  |
| http://www.wolframalpha.com/input/?  | 摸瓜V2引擎  |
| https://bugzilla.mozilla.org/show\_bug.cgi?id=726227  | 摸瓜V2引擎  |
| https://bugzilla.mozilla.org/show\_bug.cgi?id=664884  | 摸瓜V2引擎  |
| https://bugzilla.mozilla.org/show\_bug.cgi?id=972126  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://tools.ietf.org/html/rfc3986  | 摸瓜V2引擎  |
| https://bugzilla.mozilla.org/show\_bug.cgi?id=810490  | 摸瓜V2引擎  |
| https://bugzilla.mozilla.org/show\_bug.cgi?id=707484  | 摸瓜V2引擎  |
| https://example.com');  | 摸瓜V2引擎  |
| https://github.com/mozilla/pdf.js/issues/6179.  | 摸瓜V2引擎  |
| http://'  | 摸瓜V2引擎  |
| http://rjwagner49.com/Mathematics/Interpolation.pdf  | 摸瓜V2引擎  |
| http://www.poynton.com/notes/colour\_and\_gamma/ColorFAQ.html,  | 摸瓜V2引擎  |
| http://www.brucelindbloom.com/index.html?Eqn\_ChromAdapt.html  | 摸瓜V2引擎  |
| http://www.brucelindbloom.com/index.html?Eqn\_RGB\_XYZ\_Matrix.html.  | 摸瓜V2引擎  |
| http://en.wikipedia.org/wiki/SRGB.  | 摸瓜V2引擎  |
| http://www.adobe.com/content/dam/Adobe/en/devnet/photoshop/sdk/  | 摸瓜V2引擎  |
| http://www.color.org/srgb.pdf  | 摸瓜V2引擎  |
| https://developer.apple.com/fonts/TTRefMan/RM05/Chap5.html  | 摸瓜V2引擎  |
| https://github.com/mozilla/pdf.js/pull/2127  | 摸瓜V2引擎  |
| http://www.math.ubc.ca/  | 摸瓜V2引擎  |
| http://code.google.com/p/chromium/issues/detail?id=122465  | 摸瓜V2引擎  |
| https://github.com/mozilla/pdf.js/issues/1689  | 摸瓜V2引擎  |
| http://www.jpeg.org/public/fcd15444-1.pdf  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| kenji.urushima@gmail.com  | 摸瓜V2引擎  |
| af@2x.png  | 摸瓜V2引擎  |
| james@parall.ax steven@twelvetone.tv youssef.beddad@gmail.com eduardo.morais@usp.br u-jussi@suomi24.fi chick307@gmail.com dean@gmail.com jloup@gzip.org madler@alumni.caltech sstoo@gmail.com gal@mozilla.com cjones@mozilla.com shaon.barman@gmail.com 21@vingtetun.org justindarc@gmail.com  | 摸瓜V2引擎  |
| james@snapshotmedia.co ddotsenko@willowsystems.com dante@dojotoolkit.org  | 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  |
| 15695978492  | 摸瓜V2引擎  |
| 16563550634  | 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=91af0e57, ST=91af0e57, L=91af0e57, O=91af0e57, OU=91af0e57, CN=91af0e57 签名算法: rsassa\_pkcs1v15 有效期自: 2024-09-05 15:18:26+00:00 有效期至: 2124-08-12 15:18:26+00:00 发行人: C=91af0e57, ST=91af0e57, L=91af0e57, O=91af0e57, OU=91af0e57, CN=91af0e57 序列号: 0x2b3f9ccd 哈希算法: sha256 md5值: 4d1853127b29028e9205772df0fc7fed sha1值: 4ea0ca7cb3bf93c70d8bc1e947a8633394c24ba5 sha256值: 6742a7ad7d1856545a7e0e1c5c4aa4970c551f9ed5068721a907ceede22759f5 sha512值: 0e45353c1b0c82ce8fd9e0411c84313e1a97c4374ec78e25fddf677887f1f7d574f894995468de8cc87370573cecd300580332ba0d3d5ca1f1efa02c4dcd5a20 公钥算法: rsa 密钥长度: 1024 指纹: 60a45df526e813183a6504b21b0c52febc49a24b6caadcfaba7ac3eefe183a51**

## **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.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.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.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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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.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.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.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。 |

## **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。**