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

**众腾（ 2.1.0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 | 众腾 |
| 版本 | 2.1.0 |
| 包名 | plus.H5E1611EE |
| 域名线索 | 77条 |
| URL线索 | 32条 |
| APP图标 |  |
| 分析日期 | 2025年1月24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 | Zhongteng.apk |
| 文件大小 | 17.39MB |
| MD5值 | 75f742e5033b51b12eabe7bf469f22e9 |
| SHA1值 | 2d0eb231890d3ae1c56526372949a4e36ff3d089 |
| SHA256值 | 942087f8b87f3c3d77d3995f2f0d467192e6edd833c487bd6de119ebfa9b3556 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 众腾 |
| 包名 | plus.H5E1611EE |
| 主活动Activity | io.dcloud.PandoraEntry |
| 安卓版本名称 | 2.1.0 |
| 安卓版本 | 210 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| socket.zt82.vip | 没有服务器地理信息. |
| npms.io | IP: 104.21.64.1  所属国家: United States of America  地区: California  城市: San Francisco |
| g.alicdn.com | IP: 125.38.11.59  所属国家: China  地区: Tianjin  城市: Tianjin |
| socket.zt66.org | IP: 104.21.27.59  所属国家: United States of America  地区: California  城市: San Francisco |
| m3w.cn | IP: 124.163.195.101  所属国家: China  地区: Shanxi  城市: Taiyuan |
| momentjs.com | IP: 104.16.32.155  所属国家: United States of America  地区: California  城市: San Francisco |
| login.greenjade88.com | IP: 113.212.181.210  所属国家: Philippines  地区: National Capital Region  城市: Manila |
| www.gamblingtherapy.org | IP: 80.82.114.233  所属国家: United Kingdom of Great Britain and Northern Ireland  地区: England  城市: Manchester |
| android.googlesource.com | IP: 74.125.135.82  所属国家: United States of America  地区: California  城市: Mountain View |
| cube.meituan.com | IP: 101.236.69.20  所属国家: China  地区: Beijing  城市: Beijing |
| api.zt66.org | IP: 172.67.169.6  所属国家: United States of America  地区: California  城市: San Francisco |
| data-api.binance.vision | IP: 57.180.121.33  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| zt.cdn.84dns.com | 没有服务器地理信息. |
| edgedl.me.gvt1.com | IP: 34.104.35.123  所属国家: United States of America  地区: California  城市: Mountain View |
| img01.yzcdn.cn | IP: 27.221.54.107  所属国家: China  地区: Shandong  城市: Qingdao |
| underscorejs.org | IP: 172.67.134.18  所属国家: United States of America  地区: California  城市: San Francisco |
| en.wikipedia.org | IP: 103.102.166.224  所属国家: United States of America  地区: Indiana  城市: Francisco |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| lodash.com | IP: 52.76.120.174  所属国家: Singapore  地区: Singapore  城市: Singapore |
| schemas.android.com | 没有服务器地理信息. |
| acjs.aliyun.com | IP: 203.119.145.38  所属国家: China  地区: Beijing  城市: Beijing |
| wikipredia.net | IP: 104.21.6.223  所属国家: United States of America  地区: California  城市: San Francisco |
| feross.org | IP: 50.116.11.184  所属国家: United States of America  地区: California  城市: Fremont |
| t1.dcloud.net.cn | IP: 101.34.244.49  所属国家: China  地区: Beijing  城市: Beijing |
| static.sanbanye.com | IP: 83.229.44.135  所属国家: Singapore  地区: Singapore  城市: Singapore |
| api.zt82.vip | IP: 61.147.96.188  所属国家: China  地区: Jiangsu  城市: Yangzhou |
| h5.zt66.win | IP: 156.59.152.141  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| solscan.io | IP: 104.22.53.159  所属国家: United States of America  地区: California  城市: San Francisco |
| raydium.io | IP: 93.179.102.140  所属国家: United States of America  地区: California  城市: Los Angeles |
| www.galottery.com | IP: 151.101.91.52  所属国家: United States of America  地区: California  城市: San Francisco |
| baike.baidu.com | IP: 111.206.208.229  所属国家: China  地区: Beijing  城市: Beijing |
| s.tradingview.com | IP: 128.242.240.157  所属国家: United States of America  地区: Washington  城市: Redmond |
| api.zt88.win | IP: 180.178.32.2  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| etherscan.io | IP: 154.83.14.134  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| service.hshsin.com | IP: 104.21.112.1  所属国家: United States of America  地区: California  城市: San Francisco |
| www.taiwanlottery.com | IP: 104.244.43.6  所属国家: United States of America  地区: California  城市: San Francisco |
| gac1.dcloud.net.cn | IP: 124.223.210.113  所属国家: China  地区: Beijing  城市: Beijing |
| www.zt88888.com | IP: 104.21.17.13  所属国家: United States of America  地区: California  城市: San Francisco |
| zh.wikipedia.org | IP: 103.102.166.224  所属国家: United States of America  地区: Indiana  城市: Francisco |
| sdk.api.oaid.wocloud.cn | 没有服务器地理信息. |
| tronscan.org | IP: 172.66.43.46  所属国家: United States of America  地区: California  城市: San Francisco |
| bscscan.com | IP: 172.67.72.93  所属国家: United States of America  地区: California  城市: San Francisco |
| g.alicdn.com.danuoyi.alicdn.com | IP: 125.38.11.59  所属国家: China  地区: Tianjin  城市: Tianjin |
| f.m.suning.com | IP: 202.108.15.155  所属国家: China  地区: Beijing  城市: Beijing |
| na61-na62.wagbridge.alibaba.aliyun.com.gds.alibabadns.com | IP: 203.119.145.38  所属国家: China  地区: Beijing  城市: Beijing |
| api.zt66.win | IP: 156.59.152.141  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| st-tw.maitoo998.com | 没有服务器地理信息. |
| api.m.taobao.com | 没有服务器地理信息. |
| ask.dcloud.net.cn | IP: 220.194.123.111  所属国家: China  地区: Tianjin  城市: Tianjin |
| m1.openfpcdn.io | IP: 99.84.55.31  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| popular.gitbook.io | IP: 172.64.147.209  所属国家: United States of America  地区: California  城市: San Francisco |
| xg-def-cn.xcdn.global | IP: 89.187.160.82  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| api.zt00.win | IP: 104.233.161.49  所属国家: United States of America  地区: California  城市: San Jose |
| www.opap.gr | IP: 184.29.238.153  所属国家: United Arab Emirates  地区: Dubayy  城市: Dubai |
| www.xarg.org | IP: 185.244.195.154  所属国家: Germany  地区: Baden-Wurttemberg  城市: Karlsruhe |
| m.baidu.com | IP: 110.242.71.103  所属国家: China  地区: Hebei  城市: Baoding |
| guoneia.starlinkdp.top | 没有服务器地理信息. |
| images.b728484.com | IP: 216.225.165.167  所属国家: United States of America  地区: California  城市: Westlake Village |
| 1119378012870022401.zga.globalconnetct.com | IP: 156.59.152.141  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| gac2.dcloud.net.cn | IP: 124.222.75.101  所属国家: China  地区: Beijing  城市: Beijing |
| sgm-m.jd.com | IP: 111.206.227.216  所属国家: China  地区: Beijing  城市: Beijing |
| ns.adobe.com | 没有服务器地理信息. |
| er.dcloud.io | 没有服务器地理信息. |
| bgac.dcloud.net.cn | IP: 43.135.130.85  所属国家: United States of America  地区: California  城市: Santa Clara |
| www.playnow.com | IP: 23.55.107.19  所属国家: United States of America  地区: Florida  城市: Miami |
| fpjs.dev | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| element.eleme.io | IP: 185.199.109.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| openjsf.org | IP: 76.76.21.21  所属国家: United States of America  地区: California  城市: Walnut |
| www.gstatic.com | IP: 203.208.39.194  所属国家: China  地区: Beijing  城市: Beijing |
| er.dcloud.net.cn | IP: 43.142.57.168  所属国家: China  地区: Beijing  城市: Beijing |
| zenorocha.github.io | IP: 185.199.110.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| www.taiwanlottery.com.tw | IP: 34.80.76.78  所属国家: Taiwan (Province of China)  地区: Taipei  城市: Taipei |
| apps.apple.com | IP: 121.22.227.5  所属国家: China  地区: Hebei  城市: Qinhuangdao |
| popular1.blob.core.windows.net | IP: 20.60.200.161  所属国家: Korea (Republic of)  地区: Seoul-teukbyeolsi  城市: Seoul |
| s1.dcloud.net.cn | IP: 122.51.205.36  所属国家: China  地区: Beijing  城市: Beijing |
| www.w3.org | IP: 104.18.23.19  所属国家: United States of America  地区: California  城市: San Francisco |
| atlas-postgraphile.public.main.prod.cldev.sh | 没有服务器地理信息. |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| 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://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://etherscan.io/' | 摸瓜V2引擎 |
| https://etherscan.io/</a> | 摸瓜V2引擎 |
| https://tronscan.org/ | 摸瓜V2引擎 |
| https://bscscan.com/' | 摸瓜V2引擎 |
| https://bscscan.com/</a> | 摸瓜V2引擎 |
| https://www.taiwanlottery.com/lotto/result/bingo\_bingo' | 摸瓜V2引擎 |
| https://www.taiwanlottery.com/lotto/result/bingo\_bingo</a> | 摸瓜V2引擎 |
| https://en.wikipedia.org/wiki/British\_Columbia\_Lottery\_Corporation | 摸瓜V2引擎 |
| https://www.playnow.com/keno/winning-numbers/' | 摸瓜V2引擎 |
| https://www.playnow.com/keno/winning-numbers/</a> | 摸瓜V2引擎 |
| https://www.galottery.com/en-us/games/draw-games/keno.html | 摸瓜V2引擎 |
| https://en.wikipedia.org/wiki/OPAP' | 摸瓜V2引擎 |
| https://en.wikipedia.org/wiki/OPAP</a> | 摸瓜V2引擎 |
| https://www.opap.gr/en/kino-draw-results' | 摸瓜V2引擎 |
| https://www.opap.gr/en/kino-draw-results</a> | 摸瓜V2引擎 |
| https://baike.baidu.com/item/ | 摸瓜V2引擎 |
| https://www.opap.gr/en/super3-draw-results' | 摸瓜V2引擎 |
| https://www.opap.gr/en/super3-draw-results</a> | 摸瓜V2引擎 |
| https://zh.wikipedia.org/zh-hans/%E4%BB%A5%E5%A4%AA%E5%9D%8A | 摸瓜V2引擎 |
| https://zh.wikipedia.org/zh-hans/%E6%B3%A2%E5%A0%B4 | 摸瓜V2引擎 |
| https://zh.wikipedia.org/zh-my/%E5%B9%A3%E5%AE%89 | 摸瓜V2引擎 |
| https://en.wikipedia.org/wiki/Chainlink\_(blockchain) | 摸瓜V2引擎 |
| https://zh.wikipedia.org/wiki/%E5%8F%B0%E7%81%A3%E5%BD%A9%E5%88%B8 | 摸瓜V2引擎 |
| https://en.wikipedia.org/wiki/OPAP | 摸瓜V2引擎 |
| https://wikipredia.net/zh/Georgia\_Lottery | 摸瓜V2引擎 |
| https://atlas-postgraphile.public.main.prod.cldev.sh/graphql | 摸瓜V2引擎 |
| https://m.baidu.com/from=1000969a/s?word=%E8%B0%B7%E6%AD%8C%E8%BA%AB%E4%BB%BD%E9%AA%8C%E8%AF%81%E5%99%A8%E4%B8%8B%E8%BD%BD&sa=tb&ts=1542211&t\_kt=0&ie=utf-8&rsv\_t=33e70%252FJVhUh23eFAV799X70L28RJtVITm188tQZFszJDGtxExkUVonzZatCFP3E&rsv\_pq=10879009814157754031&ss=100&tj=1&rqlang=zh&rsv\_sug4=5057&inputT=3529&oq=guge%E8%BA%AB%E4%BB%BD%E9%AA%8C%E8%AF%81%E5%99%A8%E4%B8%8B%E8%BD%BD | 摸瓜V2引擎 |
| https://fpjs.dev/pro | 摸瓜V2引擎 |
| https://m1.openfpcdn.io/fingerprintjs/v | 摸瓜V2引擎 |
| https://api.zt66.win/public/last\_version | 摸瓜V2引擎 |
| https://popular1.blob.core.windows.net/statics/apk/GoogleAuthenticator.apk | 摸瓜V2引擎 |
| https://apps.apple.com/cn/app/google-authenticator/id388497605 | 摸瓜V2引擎 |
| https://fpjs.dev/pro | 摸瓜V2引擎 |
| https://m1.openfpcdn.io/fingerprintjs/v | 摸瓜V2引擎 |
| https://h5.zt66.win | 摸瓜V2引擎 |
| https://www.zt88888.com/ | 摸瓜V2引擎 |
| https://solscan.io/tx/ | 摸瓜V2引擎 |
| https://solscan.io/account/ | 摸瓜V2引擎 |
| https://raydium.io/ | 摸瓜V2引擎 |
| https://cube.meituan.com/ipromotion/cube/toc/component/base/getServerCurrentTime | 摸瓜V2引擎 |
| https://sgm-m.jd.com/h5/ | 摸瓜V2引擎 |
| https://api.m.taobao.com/rest/api3.do?api=mtop.common.getTimestamp | 摸瓜V2引擎 |
| https://f.m.suning.com/api/ct.do | 摸瓜V2引擎 |
| https://www.gamblingtherapy.org | 摸瓜V2引擎 |
| https://service.hshsin.com/chatIndex?ent\_id=14 | 摸瓜V2引擎 |
| https://images.b728484.com:42666/TCG\_GAME\_ICONS/ | 摸瓜V2引擎 |
| https://s.tradingview.com/widgetembed/?frameElementId=tradingview\_b239c&symbol=BINANCE%3ABTCUSDT&interval=5&hidesidetoolbar=0&symboledit=1&saveimage=1&toolbarbg=f1f3f6&studies=%5B%5D&theme=light&style=1&studies\_overrides=%7B%7D&overrides=%7B%7D&enabled\_features=%5B%22header\_fullscreen\_button%22%5D&disabled\_features=%5B%5D&utm\_source=pancakeswap.finance&utm\_medium=widget&utm\_campaign=chart&utm\_term=BINANCE%3ABTCUSDT | 摸瓜V2引擎 |
| https://popular.gitbook.io/popular/prediction | 摸瓜V2引擎 |
| https://popular1.blob.core.windows.net/statics/zhongteng/gameIcon/wap/ | 摸瓜V2引擎 |
| https://popular1.blob.core.windows.net/statics/common/media/dida.mp3 | 摸瓜V2引擎 |
| https://popular1.blob.core.windows.net/statics/common/media/lottery.mp3 | 摸瓜V2引擎 |
| https://etherscan.io/block/ | 摸瓜V2引擎 |
| https://tronscan.org/ | 摸瓜V2引擎 |
| https://bscscan.com/block/ | 摸瓜V2引擎 |
| https://zh.wikipedia.org/wiki/ | 摸瓜V2引擎 |
| https://www.taiwanlottery.com.tw/lotto/BINGOBINGO/drawing.aspx | 摸瓜V2引擎 |
| https://www.taiwanlottery.com.tw/lotto/BINGOBINGO/drawing.aspx</a></p>\n | 摸瓜V2引擎 |
| https://en.wikipedia.org/wiki/British\_Columbia\_Lottery\_Corporation | 摸瓜V2引擎 |
| https://www.playnow.com/keno/winning-numbers/ | 摸瓜V2引擎 |
| https://en.wikipedia.org/wiki/British\_Columbia\_Lottery\_Corporation</a><br>\n | 摸瓜V2引擎 |
| https://www.playnow.com/keno/winning-numbe | 摸瓜V2引擎 |
| https://www.playnow.com/keno/winning-numbe</a><br></p>\n | 摸瓜V2引擎 |
| https://wikipredia.net/zh/Georgia\_Lottery | 摸瓜V2引擎 |
| https://www.galottery.com/en-us/games/draw-games/keno.html | 摸瓜V2引擎 |
| https://en.wikipedia.org/wiki/Georgia\_Lottery | 摸瓜V2引擎 |
| https://en.wikipedia.org/wiki/Georgia\_Lottery</a><br>\n | 摸瓜V2引擎 |
| https://en.wikipedia.org/wiki/OPAP | 摸瓜V2引擎 |
| https://www.opap.gr/en/kino-draw-results | 摸瓜V2引擎 |
| https://www.opap.gr/en/kino-draw-results</a></p>\n | 摸瓜V2引擎 |
| https://etherscan.io/ | 摸瓜V2引擎 |
| https://etherscan.io/</a></p>\n | 摸瓜V2引擎 |
| https://tronscan.org/</a></p>\n | 摸瓜V2引擎 |
| https://etherscan.io/</a></p>\n\t\t' | 摸瓜V2引擎 |
| https://en.wikipedia.org/wiki/British\_Columbia\_Lottery\_Corporation</a></p>\n | 摸瓜V2引擎 |
| https://www.playnow.com/keno/winning-numbe</a> | 摸瓜V2引擎 |
| https://en.wikipedia.org/wiki/OPAP</a> | 摸瓜V2引擎 |
| https://www.playnow.com/keno/winning-numbers/</a></p>\n | 摸瓜V2引擎 |
| https://en.wikipedia.org/wiki/OPAP</a></p>\n | 摸瓜V2引擎 |
| https://www.opap.gr/en/super3-draw-results | 摸瓜V2引擎 |
| https://www.opap.gr/en/super3-draw-results</a></p>\n | 摸瓜V2引擎 |
| https://www.playnow.com/keno/winning-numbe</a></p>\n | 摸瓜V2引擎 |
| https://api.zt66.org | 摸瓜V2引擎 |
| https://api.zt66.win | 摸瓜V2引擎 |
| https://api.zt88.win | 摸瓜V2引擎 |
| https://api.zt00.win | 摸瓜V2引擎 |
| https://api.zt82.vip:4435 | 摸瓜V2引擎 |
| https://api.zt66.win/public/last\_version | 摸瓜V2引擎 |
| https://static.sanbanye.com/ | 摸瓜V2引擎 |
| https://st-tw.maitoo998.com/v6/public/GetNewVersion | 摸瓜V2引擎 |
| https://data-api.binance.vision/api/v3/klines?symbol= | 摸瓜V2引擎 |
| https://socket.zt66.org | 摸瓜V2引擎 |
| https://socket.zt82.vip:4435 | 摸瓜V2引擎 |
| https://feross.org> | 摸瓜V2引擎 |
| http://www.xarg.org/2014/03/rational-numbers-in-javascript/ | 摸瓜V2引擎 |
| https://img01.yzcdn.cn/vant/coupon-empty.png | 摸瓜V2引擎 |
| https://img01.yzcdn.cn/vant/empty-image- | 摸瓜V2引擎 |
| https://img01.yzcdn.cn/vant/share-sheet- | 摸瓜V2引擎 |
| https://img01.yzcdn.cn/upload\_files/2020/06/24/FmKWDg0bN9rMcTp9ne8MXiQWGtLn.png | 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 |
| http://momentjs.com/guides/ | 摸瓜V2引擎 |
| https://zenorocha.github.io/clipboard.js | 摸瓜V2引擎 |
| http://element.eleme.io/ | 摸瓜V2引擎 |
| https://github.com/MikeMcl/decimal.js/LICENCE | 摸瓜V2引擎 |
| https://service.hshsin.com/chatIndex?ent\_id=14 | 摸瓜V3引擎 |
| https://api.zt66.win/public/last\_version | 摸瓜V3引擎 |
| g.alicdn.com | 摸瓜V3引擎 |
| https://tronscan.org/ | 摸瓜V3引擎 |
| login.greenjade88.com | 摸瓜V3引擎 |
| https://m3w.cn/s/ | 摸瓜V3引擎 |
| https://www.playnow.com/keno/winning-numbe | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android | 摸瓜V3引擎 |
| api.zt66.org | 摸瓜V3引擎 |
| https://socket.zt66.org | 摸瓜V3引擎 |
| https://f.m.suning.com/api/ct.do | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android00androidx.appcompat.widget.FitWindowsLinearLayout((androi | 摸瓜V3引擎 |
| zt.cdn.84dns.com | 摸瓜V3引擎 |
| edgedl.me.gvt1.com | 摸瓜V3引擎 |
| https://www.galottery.com/en-us/games/draw-games/keno.html#tab-winningNumbers | 摸瓜V3引擎 |
| https://socket.zt82.vip:4435 | 摸瓜V3引擎 |
| acjs.aliyun.com | 摸瓜V3引擎 |
| t1.dcloud.net.cn | 摸瓜V3引擎 |
| api.zt82.vip | 摸瓜V3引擎 |
| firebaseinstallations.googleapis.com | 摸瓜V3引擎 |
| https://solscan.io/account/ | 摸瓜V3引擎 |
| api.zt88.win | 摸瓜V3引擎 |
| https://api.zt88.win | 摸瓜V3引擎 |
| https://sgm-m.jd.com/h5/ | 摸瓜V3引擎 |
| gac1.dcloud.net.cn | 摸瓜V3引擎 |
| https://bscscan.com/ | 摸瓜V3引擎 |
| https://baike.baidu.com/item/ | 摸瓜V3引擎 |
| https://ask.dcloud.net.cn/article/35877 | 摸瓜V3引擎 |
| sdk.api.oaid.wocloud.cn | 摸瓜V3引擎 |
| https://www.opap.gr/en/super3-draw-results | 摸瓜V3引擎 |
| https://solscan.io/tx/ | 摸瓜V3引擎 |
| https://static.sanbanye.com/shengtu/common/images/loading.gif | 摸瓜V3引擎 |
| https://android.googlesource.com/toolchain/llvm-project | 摸瓜V3引擎 |
| https://android.googlesource.com/toolchain/clang | 摸瓜V3引擎 |
| g.alicdn.com.danuoyi.alicdn.com | 摸瓜V3引擎 |
| https://api.zt82.vip:4435 | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res-auto | 摸瓜V3引擎 |
| update.googleapis.com | 摸瓜V3引擎 |
| https://er.dcloud.net.cn/rv | 摸瓜V3引擎 |
| https://cube.meituan.com/ipromotion/cube/toc/component/base/getServerCurrentTime | 摸瓜V3引擎 |
| https://login.greenjade88.com/jswrapper/integration.js.php?casino=greenjade88 | 摸瓜V3引擎 |
| https://www.taiwanlottery.com.tw/lotto/BINGOBINGO/drawing.aspx | 摸瓜V3引擎 |
| infinitedata-pa.googleapis.com | 摸瓜V3引擎 |
| na61-na62.wagbridge.alibaba.aliyun.com.gds.alibabadns.com | 摸瓜V3引擎 |
| api.zt66.win | 摸瓜V3引擎 |
| https://wikipredia.net/zh/Georgia\_Lottery | 摸瓜V3引擎 |
| https://etherscan.io/ | 摸瓜V3引擎 |
| https://ask.dcloud.net.cn/article/35627 | 摸瓜V3引擎 |
| https://api.zt66.org | 摸瓜V3引擎 |
| https://api.zt00.win | 摸瓜V3引擎 |
| https://atlas-postgraphile.public.main.prod.cldev.sh/graphql | 摸瓜V3引擎 |
| xg-def-cn.xcdn.global | 摸瓜V3引擎 |
| api.zt00.win | 摸瓜V3引擎 |
| https://data-api.binance.vision/api/v3/klines?symbol= | 摸瓜V3引擎 |
| https://er.dcloud.net.cn/sc | 摸瓜V3引擎 |
| https://api.m.taobao.com/rest/api3.do?api=mtop.common.getTimestamp | 摸瓜V3引擎 |
| https://tronscan.org/#/ | 摸瓜V3引擎 |
| https://raydium.io/ | 摸瓜V3引擎 |
| guoneia.starlinkdp.top | 摸瓜V3引擎 |
| https://static.sanbanye.com/shengtu/common/images/loading.png); | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res-auto00androidx.appcompat.widget.ActionBarOverlayLayout | 摸瓜V3引擎 |
| 1119378012870022401.zga.globalconnetct.com | 摸瓜V3引擎 |
| https://ask.dcloud.net.cn/article/35058 | 摸瓜V3引擎 |
| https://g.alicdn.com/AWSC/AWSC/awsc.js | 摸瓜V3引擎 |
| https://er.dcloud.io/sc | 摸瓜V3引擎 |
| gac2.dcloud.net.cn | 摸瓜V3引擎 |
| bgac.dcloud.net.cn | 摸瓜V3引擎 |
| clientservices.googleapis.com | 摸瓜V3引擎 |
| https://android.googlesource.com/toolchain/llvm | 摸瓜V3引擎 |
| www.gstatic.com | 摸瓜V3引擎 |
| er.dcloud.net.cn | 摸瓜V3引擎 |
| https://ask.dcloud.net.cn/article/283 | 摸瓜V3引擎 |
| https://er.dcloud.io/rv | 摸瓜V3引擎 |
| instantmessaging-pa.googleapis.com | 摸瓜V3引擎 |
| s1.dcloud.net.cn | 摸瓜V3引擎 |
| https://ask.dcloud.net.cn/article/282 | 摸瓜V3引擎 |
| https://api.zt66.win | 摸瓜V3引擎 |
| https://www.playnow.com/keno/winning-numbers/ | 摸瓜V3引擎 |
| https://www.taiwanlottery.com/lotto/result/bingo\_bingo | 摸瓜V3引擎 |
| https://www.opap.gr/en/kino-draw-results | 摸瓜V3引擎 |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| robert@xarg.org | 摸瓜V2引擎 |

### **4.4 手机号线索**

## **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=BJ, L=HD, O=Android, OU=Android, CN=Android Debug 签名算法: rsassa\_pkcs1v15 有效期自: 2021-04-12 08:27:53+00:00 有效期至: 2121-03-19 08:27:53+00:00 发行人: C=CN, ST=BJ, L=HD, O=Android, OU=Android, CN=Android Debug 序列号: 0x363bc393 哈希算法: sha256 md5值: 06838cc840093b9d4689fc419ba1a3f3 sha1值: 97c84101b9141c130dd75d7428a2922518c36dcd sha256值: b01d06180d003e79c7b9088993b8e5ae7a19b0da1161aa097c7f398a6f514fa7 sha512值: 67720eb20639d1f5f9c8b7b201b185ea4364f6a89bedd35aa1d273002c16d65a7739f59679510d3b96c1f2c3dd3136d9a34451cb679251a86ff4cafdc18314bf 公钥算法: rsa 密钥长度: 2048 指纹: b27ac6d7a4586417c251be6e44179616262379e57da2d1e19db0995be0ddf509**

## **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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| android.permission.WRITE\_EXTERNAL\_STORAGE | 危险 | 读取/修改/删除外部存储内容 | 允许应用程序写入外部存储 |
| android.permission.ACCESS\_NETWORK\_STATE | 正常 | 查看网络状态 | 允许应用程序查看所有网络的状态 |
| android.permission.ACCESS\_WIFI\_STATE | 正常 | 查看Wi-Fi状态 | 允许应用程序查看有关 Wi-Fi 状态的信息 |
| android.permission.INSTALL\_PACKAGES | 系统需要 | 直接安装应用程序 | 允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序 |
| android.permission.REQUEST\_INSTALL\_PACKAGES | 危险 | 允许应用程序请求安装包。 | 恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。 |
| android.permission.ACCESS\_COARSE\_LOCATION | 危险 | 粗定位 | 访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置 |
| android.permission.ACCESS\_FINE\_LOCATION | 危险 | 精细定位（GPS） | 访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量 |
| android.permission.CALL\_PHONE | 危险 | 直接拨打电话号码 | 允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码 |
| android.permission.CAMERA | 危险 | 拍照和录像 | 允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像 |
| android.permission.CHANGE\_NETWORK\_STATE | 正常 | 更改网络连接 | 允许应用程序更改网络连接状态。 |
| android.permission.CHANGE\_WIFI\_STATE | 正常 | 更改Wi-Fi状态 | 允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改 |
| android.permission.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| android.permission.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.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.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.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.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 |
| com.asus.msa.SupplementaryDID.ACCESS | 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**: h5e1611ee://, |

**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。**