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

**全球发展（ 1.0.3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 | 全球发展 |
| 版本 | 1.0.3 |
| 包名 | uni.UNI2C9011F |
| 域名线索 | 37条 |
| URL线索 | 9条 |
| APP图标 |  |
| 分析日期 | 2025年6月17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 | 全球发展传销.apk |
| 文件大小 | 22.8MB |
| MD5值 | 52d210c79673450e8b52d48cc72efe01 |
| SHA1值 | 0e45b0c2902d51991311861d3bde8a5288ac2499 |
| SHA256值 | 52c78f6ff690f0ff2f84c0606608dda063666c47781a0bc7e527710f7c2fac1c |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 全球发展 |
| 包名 | uni.UNI2C9011F |
| 主活动Activity | io.dcloud.PandoraEntry |
| 安卓版本名称 | 1.0.3 |
| 安卓版本 | 103 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| www.puba-interface.com | IP: 156.251.50.182 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| bugs.chromium.org | IP: 74.125.195.121 所属国家: United States of America 地区: California 城市: Mountain View  |
| bonterwj.com | IP: 120.83.145.7 所属国家: China 地区: Guangdong 城市: Foshan  |
| api.bspapp.com | IP: 39.96.249.142 所属国家: China 地区: Beijing 城市: Beijing  |
| mdn.io | IP: 172.67.217.160 所属国家: United States of America 地区: California 城市: San Francisco  |
| bugs.webkit.org | IP: 17.33.194.218 所属国家: United States of America 地区: California 城市: Cupertino  |
| www.particleincell.com | IP: 74.207.242.114 所属国家: United States of America 地区: California 城市: Fremont  |
| egsc.usgs.gov | IP: 137.227.233.178 所属国家: United States of America 地区: Virginia 城市: Reston  |
| hnxsrl.com | IP: 220.249.135.249 所属国家: China 地区: Fujian 城市: Ningde  |
| www.ecma-international.org | IP: 83.166.133.61 所属国家: Switzerland 地区: Geneve 城市: Carouge  |
| geographiclib.sourceforge.net | IP: 104.18.13.149 所属国家: United States of America 地区: California 城市: San Francisco  |
| eev.ee | IP: 45.79.41.207 所属国家: United States of America 地区: Texas 城市: Richardson  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| quilljs.com | IP: 172.66.43.93 所属国家: United States of America 地区: California 城市: San Francisco  |
| api.next.bspapp.com | IP: 203.107.60.33 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| mathworld.wolfram.com | IP: 140.177.8.25 所属国家: United States of America 地区: Illinois 城市: Champaign  |
| math.stackexchange.com | IP: 172.64.144.30 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.jasondavies.com | IP: 130.162.160.161 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: London  |
| hammerjs.github.io | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| www.google.com | IP: 31.13.73.9 所属国家: Ireland 地区: Dublin 城市: Dublin  |
| oli.me.uk | IP: 104.21.64.1 所属国家: United States of America 地区: California 城市: San Francisco  |
| en.wikipedia.org | IP: 31.13.94.10 所属国家: Argentina 地区: Ciudad Autonoma de Buenos Aires 城市: Buenos Aires  |
| mathiasbynens.be | IP: 83.137.145.144 所属国家: Netherlands 地区: Groningen 城市: Groningen  |
| service.dcloud.net.cn | IP: 111.229.199.57 所属国家: China 地区: Beijing 城市: Beijing  |
| d3js.org | IP: 172.67.73.126 所属国家: United States of America 地区: California 城市: San Francisco  |
| ecma-international.org | IP: 83.166.133.61 所属国家: Switzerland 地区: Geneve 城市: Carouge  |
| tykyhkt.com | IP: 202.108.15.155 所属国家: China 地区: Beijing 城市: Beijing  |
| bl.ocks.org | IP: 104.21.32.1 所属国家: United States of America 地区: California 城市: San Francisco  |
| static.mrfeinberg.com | 没有服务器地理信息.  |
| vkceyugu.cdn.bspapp.com | IP: 218.24.90.185 所属国家: China 地区: Liaoning 城市: Shenyang  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| unlicense.org | IP: 172.67.133.50 所属国家: United States of America 地区: California 城市: San Francisco  |
| apis.map.qq.com | IP: 116.130.224.140 所属国家: China 地区: Beijing 城市: Beijing  |
| ask.dcloud.net.cn | IP: 123.125.244.81 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  |
| geoexamples.com | IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| hksjlr.com | IP: 202.108.15.155 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://ask.dcloud.net.cn/article/36199  | 摸瓜V1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://bonterwj.com/virtual-coin/img/video-item-bg.png  | 摸瓜V2引擎  |
| https://vkceyugu.cdn.bspapp.com/VKCEYUGU-6bef1fe3-e3e3-4909-9f0c-6ed9bd11c93b/aae2360a-6628-4c93-b873-ce1600b9a852.apk  | 摸瓜V2引擎  |
| https://tykyhkt.com  | 摸瓜V2引擎  |
| https://hksjlr.com  | 摸瓜V2引擎  |
| https://hnxsrl.com  | 摸瓜V2引擎  |
| https://www.puba-interface.com  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/%E9%9B%86%E5%9B%A2%E4%BB%8B%E7%BB%8D  | 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://bonterwj.com/virtual-coin/img/product-item-des-head-pic  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/product-item-des-cord-bg  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/product-item1.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/product-item2.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/product-item3.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/product-item4.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/product-item5.png  | 摸瓜V2引擎  |
| https://github.com/facebook/regenerator/blob/main/LICENSE  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/zjzc-card-list-pic1.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/zjzc-card-list-pic2.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/zjzc-card-list-pic3.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/zjzc-card-list-pic4.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/zjzc-card-list-pic5.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/zjzc-card-list-pic6.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/product-item-bg  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/my-bg2.png);background-size:contain;background-repeat:no-repeat;background-color:  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/develop-history-des-bg2.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/develop-history-des-bg3.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/property-info-bg.png);background-size:contain;background-repeat:no-repeat  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/activity-bg1.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/logo-horizontal1.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/convert-funds-tab-bg.png);box-shadow:0  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/product-order-list-item-bg.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/signin-exchange-head-pic.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/sigin-product-bg.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/signin-exchange-top-item1.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/signin-exchange-top-item2.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/signin-exchange-top-item3.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/signin-exchange-top-item4.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/signin-exchange-top-item5.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/team-bg.png);background-size:contain;background-repeat:no-repeat;background-color:  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/team-header-logo.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/team-header-bg.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/performance-bg.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/total-data-bg.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/invite-bg.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/tab-content-bg.png);background-size:contain;background-repeat:no-repeat  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/tab-content-bg2.png);background-size:contain;background-repeat:no-repeat;overflow:hidden  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/equity-market-banner.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/zjzc-title-bg.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/zjzc-content-bg.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/zjzc-content-title-bg.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/zjzc-title-text.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/zjzc-bottom-list-item-bg.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/equity-market-bg.png);background-size:contain;background-repeat:no-repeat;background-color:  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/property-banner.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/property-banner2.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/property-card-bg1.png)  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/property-card-bg2.png)  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/property-card-bg3.png)  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/property-card-bg4.png)  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/kefu-bg1.png);background-size:contain;background-repeat:no-repeat;background-color:  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/icon-singnin-name-img2.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/my-banner2.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/login-bg2.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/online-bg.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/onlin-bottom-bg.jpg  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/my-bg.png);background-color:  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/my-banner3.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/product-bg.png);background-size:contain;background-repeat:no-repeat;position:relative;overflow:hidden  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/storage-bg.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/storage-chose-days-bg.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/hongkong-bg.png);background-size:contain;background-repeat:no-repeat;background-color:  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/hongkong-total-bg1.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/icon-bank.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/txcash-bottom-bg.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/hongkong-pos-bg1.png);background-size:contain  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/hongkong-pos-title-bg.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/hongkong-pos-bg2.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/hongkong-pos-bg3.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/hongkong-pos-bg4.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/hongkong-pos-content4-item-bg.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/hongkong-pos-bg5.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/hongkong-pos-bg6.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/hongkong-pos-content6-item-pic1.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/hongkong-pos-content6-item-pic2.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/hongkong-pos-bg7.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/icon-smrz.png);background-size:280rpx  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/smrz-card-item-info.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/bottom-bg.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/signin-exchange-head-bg.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/signin-exchange-head-info-bg.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/signin-exchange-days-card-bg.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/nodata-bg.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/partners-title-bg.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/partners-bg1.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/partners-des-item-bg.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/product-introduce-bg5.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/partners-bottom-item-bg.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/property-transfer-bg.png);background-size:contain;background-repeat:no-repeat;background-color:  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/hongkong-total-bg2.png)  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/signin-bg.png);background-size:contain;background-repeat:no-repeat;background-color:  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/signin-head-bg.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/signin-plan-coupon-bg.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/signin-money-card-bg.png);background-repeat:no-repeat;background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/activity-bg0.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/partners-bg2.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/partners-bg-logo.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/partners-bottom-item-pic1.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/partners-bottom-item-pic2.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/partners-bottom-item-pic3.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/partners-bottom-item-pic4.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/hongkong-pos-content1-bg.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/hongkong-pos-content2-pic.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/hongkong-pos-content4-item-pic.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/hongkong-pos-content4-item-pic2.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/hongkong-pos-content4-item-pic3.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/hongkong-pos-content4-item-pic4.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/hongkong-pos-content4-item-pic5.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/hongkong-pos-content4-item-pic6.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/hongkong-pos-content6-item-pic3.png)  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/securityCenter-bg.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/talent-bg1.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/talent-bg2.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/active-talent-bg5.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/talent-bg4.png);background-size:contain  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/talent-card-tab.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/talent-card-bg.png);background-size:contain;background-repeat:no-repeat  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/item-banner.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/develop-history-bg1.png);background-size:contain;background-repeat:no-repeat;background-color:  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/develop-history-bg2.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/develop-history-btn-bg.png);background-size:contain;font-size:40rpx;font-weight:700;color:  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/changepassword-bg.png);background-size:contain;background-repeat:no-repeat  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/zjzc-title-logo.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/des-list-item-pic1.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/des-list-item-pic2.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/des-list-item-pic3.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/popup-bg.png);background-size:contain;background-repeat:no-repeat  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/menu-bg.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/menu-card-bg.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/video-bg.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/bottom-content-head-bg.png);background-size:cover  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/company-registration-certificate.jpg  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/order-list-item-bg.png);background-size:cover;box-shadow:0  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/kefu-bg.png);background-size:contain;background-repeat:no-repeat;background-color:  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/group-bg.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/product-item-des-head-bg.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/product-item-des-cards-bg.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/balance-chose-bg.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/balance-chose-bg1.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/product-introduce-logo.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/product-introduce-banner.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/product-introduce-bg6.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/develop-history-des-bg1.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/jiaoyi-item-bg1.png)  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/jiaoyi-item-bg2.png)  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/jiaoyi-item-bg3.png)  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/jiaoyi-item-bg4.png)  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/jiaoyi-bg1.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/jiaoyi-bg2.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/product-introduce-bg1.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/product-introduce-bg2.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/product-introduce-bg3.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/product-introduce-bg4.png);background-size:100%  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/invite-title-bg.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/invite-bottom-bg.png  | 摸瓜V2引擎  |
| https://bonterwj.com/virtual-coin/img/product-item-bg.png);background-size:contain;background-repeat:no-repeat;background-color:  | 摸瓜V2引擎  |
| https://service.dcloud.net.cn/uniapp/feedback.html  | 摸瓜V2引擎  |
| https://github.com/developit/dlv/blob/master/index.js  | 摸瓜V2引擎  |
| https://d3js.org/d3-array/  | 摸瓜V2引擎  |
| https://github.com/python/cpython/blob/a74eea238f5baba15797e2e8b570d153bc8690a7/Modules/mathmodule.c  | 摸瓜V2引擎  |
| https://github.com/mourner/quickselect  | 摸瓜V2引擎  |
| https://d3js.org/d3-collection/  | 摸瓜V2引擎  |
| http://geoexamples.com/d3-composite-projections/  | 摸瓜V2引擎  |
| http://egsc.usgs.gov/isb/pubs/MapProjections/projections.html  | 摸瓜V2引擎  |
| https://bl.ocks.org/mbostock/5629120  | 摸瓜V2引擎  |
| https://d3js.org/d3-dsv/  | 摸瓜V2引擎  |
| https://github.com/d3/d3-dsv/issues/45  | 摸瓜V2引擎  |
| https://d3js.org/d3-geo-projection/  | 摸瓜V2引擎  |
| https://github.com/OSUCartography/JMapProjLib/blob/master/src/com/jhlabs/map/proj/PattersonProjection.java  | 摸瓜V2引擎  |
| https://github.com/d3/d3/issues/1558  | 摸瓜V2引擎  |
| https://d3js.org/d3-geo/  | 摸瓜V2引擎  |
| http://geographiclib.sourceforge.net/  | 摸瓜V2引擎  |
| https://d3js.org/d3-hierarchy/  | 摸瓜V2引擎  |
| https://d3js.org/d3-path/  | 摸瓜V2引擎  |
| https://github.com/d3/d3-sankey  | 摸瓜V2引擎  |
| https://d3js.org/d3-shape/  | 摸瓜V2引擎  |
| http://mathworld.wolfram.com/Circle-LineIntersection.html  | 摸瓜V2引擎  |
| https://en.wikipedia.org/wiki/Cubic\_Hermite\_spline  | 摸瓜V2引擎  |
| https://www.particleincell.com/2012/bezier-splines/  | 摸瓜V2引擎  |
| https://d3js.org/d3-voronoi/  | 摸瓜V2引擎  |
| http://math.stackexchange.com/questions/108113/find-edge-between-two-boxes  | 摸瓜V2引擎  |
| http://ecma-international.org/ecma-262/7.0/  | 摸瓜V2引擎  |
| https://bugs.webkit.org/show\_bug.cgi?id=156034  | 摸瓜V2引擎  |
| https://github.com/jashkenas/underscore/pull/1247  | 摸瓜V2引擎  |
| https://bugs.chromium.org/p/v8/issues/detail?id=90  | 摸瓜V2引擎  |
| http://www.ecma-international.org/ecma-262/7.0/  | 摸瓜V2引擎  |
| http://eev.ee/blog/2015/09/12/dark-corners-of-unicode/).  | 摸瓜V2引擎  |
| https://mathiasbynens.be/notes/javascript-unicode).  | 摸瓜V2引擎  |
| https://mdn.io/Structured\_clone\_algorithm)  | 摸瓜V2引擎  |
| https://github.com/topojson/topojson-client  | 摸瓜V2引擎  |
| http://unlicense.org/  | 摸瓜V2引擎  |
| https://oli.me.uk/  | 摸瓜V2引擎  |
| https://github.com/Planeshifter/kernel-smooth/blob/master/lib/index.js  | 摸瓜V2引擎  |
| https://github.com/jasondavies/science.js/blob/master/src/stats/kernel.js  | 摸瓜V2引擎  |
| https://www.jasondavies.com/wordcloud/  | 摸瓜V2引擎  |
| http://static.mrfeinberg.com/bv\_ch03.pdf  | 摸瓜V2引擎  |
| http://hammerjs.github.io/  | 摸瓜V2引擎  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| jhruby.web@gmail.com  | 摸瓜V2引擎  |
| \_d3-array@2.11 \_d3-geo@1.12 \_lodash@4.17 \_webpack@4.46  | 摸瓜V2引擎  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 18811699200  | 摸瓜V2引擎  |

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: True 找到 1 个唯一证书 主题: C=cn, ST=beijing, L=beijng, O=qqfz, OU=world, CN=anna 签名算法: rsassa\_pkcs1v15 有效期自: 2025-06-08 06:51:41+00:00 有效期至: 2125-05-15 06:51:41+00:00 发行人: C=cn, ST=beijing, L=beijng, O=qqfz, OU=world, CN=anna 序列号: 0x35804877 哈希算法: sha256 md5值: 7cc3aeb3908b2321811126db9c4be074 sha1值: a1b6cfdcdc7528f4d910cb992b02a28f577dbb47 sha256值: b9e5c5838fd1b33ea24e8f9cd28b3989798d99574d24453c9270afcc1c73f89b sha512值: 1416835edd8623c5910c7d305d884206a230c944805e91c3b34b520822991cf31381a43a3f855d0a84eb1d089b76c0306e6c3c9e7773902a7ff27f5e63e21baa 公钥算法: rsa 密钥长度: 2048 指纹: bcc180baf7cd69f71c2e65b2c6831e4d8201152e480da4e665ffacc1d07b0f47**

## **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.UNI2C9011F | 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.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.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.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**

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