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

**AIX（ 1.2.1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 | AIX |
| 版本 | 1.2.1 |
| 包名 | app.aix |
| 域名线索 | 141条 |
| URL线索 | 45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 | AIX1.2.1.apk |
| 文件大小 | 52.47MB |
| MD5值 | f0d700250b25b84ebf34bf8fa27d5922 |
| SHA1值 | 0a9c2c7368d4e9849854e166c3f3b96fdf1e3eae |
| SHA256值 | b5c26bff9245b85f57a93b10011fecac3df199e11af384f15b73185a1d1d2b55 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | AIX |
| 包名 | app.aix |
| 主活动Activity | io.dcloud.PandoraEntry |
| 安卓版本名称 | 1.2.1 |
| 安卓版本 | 121 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| api.etherscan.io | IP: 31.13.112.4 所属国家: Ireland 地区: Dublin 城市: Dublin  |
| m3w.cn | IP: 116.196.150.251 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| undetectable.ai | IP: 104.18.31.149 所属国家: United States of America 地区: California 城市: San Francisco  |
| api-optimistic.etherscan.io | IP: 103.42.176.244 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| api.bscscan.com | IP: 91.191.210.250 所属国家: United States of America 地区: Florida 城市: Tampa  |
| ns.adobe.com | 没有服务器地理信息.  |
| www.arterys.com | IP: 3.168.86.26 所属国家: United States of America 地区: Washington 城市: Seattle  |
| arxiv.org | IP: 151.101.67.42 所属国家: United States of America 地区: California 城市: San Francisco  |
| gateway.ipfs.io | IP: 199.96.59.61 所属国家: United States of America 地区: California 城市: San Francisco  |
| waymo.com | IP: 142.250.217.110 所属国家: United States of America 地区: California 城市: Mountain View  |
| www.anthropic.com | IP: 160.79.104.10 所属国家: United States of America 地区: New Jersey 城市: Hackensack  |
| ai.meta.com | IP: 31.13.95.33 所属国家: Ireland 地区: Dublin 城市: Dublin  |
| aixwallet.net | IP: 104.26.2.7 所属国家: United States of America 地区: California 城市: San Francisco  |
| api-goerli.arbiscan.io | 没有服务器地理信息.  |
| api.polygonscan.com | IP: 199.167.149.50 所属国家: United States of America 地区: Florida 城市: Tampa  |
| www.cognitivescale.com | IP: 194.42.63.167 所属国家: Finland 地区: Uusimaa 城市: Helsinki  |
| www.butterflynetwork.com | IP: 3.166.228.54 所属国家: United States of America 地区: Washington 城市: Seattle  |
| huggingface.co | IP: 108.160.163.106 所属国家: United States of America 地区: California 城市: San Francisco  |
| vulcansphere.com | IP: 206.189.42.180 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| www.mindfoundry.ai | IP: 199.60.103.225 所属国家: United States of America 地区: Massachusetts 城市: Cambridge  |
| sodipodi.sourceforge.net | IP: 104.18.12.149 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.visteon.com | IP: 162.159.129.11 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.vicarious.com | 没有服务器地理信息.  |
| www.bluerivertechnology.com | IP: 52.203.97.246 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| gasstation.polygon.technology | IP: 172.64.146.146 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.inkscape.org | IP: 140.211.9.79 所属国家: United States of America 地区: Oregon 城市: Eugene  |
| www.caper.ai | IP: 57.180.160.60 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| lame.sf.net | IP: 104.18.20.237 所属国家: United States of America 地区: California 城市: San Francisco  |
| bscscan.com | IP: 104.26.13.158 所属国家: United States of America 地区: California 城市: San Francisco  |
| upload.kp.io | IP: 3.139.159.151 所属国家: United States of America 地区: Ohio 城市: Columbus  |
| api.map.baidu.com | IP: 111.206.208.72 所属国家: China 地区: Beijing 城市: Beijing  |
| www.clarifai.com | IP: 199.60.103.2 所属国家: United States of America 地区: Massachusetts 城市: Cambridge  |
| fontshare.com | IP: 108.139.10.52 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.salesforce.com | IP: 23.210.26.145 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| api.arbiscan.io | IP: 104.26.14.203 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.freenome.com | IP: 23.185.0.2 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.synthesia.io | IP: 54.238.67.66 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| www.google.com | IP: 31.13.106.4 所属国家: Ireland 地区: Dublin 城市: Dublin  |
| api-sepolia.etherscan.io | IP: 108.160.166.137 所属国家: United States of America 地区: California 城市: San Francisco  |
| rpc-amoy.polygon.technology | IP: 104.18.41.110 所属国家: United States of America 地区: California 城市: San Francisco  |
| api-testnet.polygonscan.com | IP: 172.67.71.154 所属国家: United States of America 地区: California 城市: San Francisco  |
| service.dcloud.net.cn | IP: 111.229.199.57 所属国家: China 地区: Beijing 城市: Beijing  |
| 127.0.0.1 | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| www.artisse.ai | IP: 43.198.6.96 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| benevolent.com | IP: 167.99.200.154 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: London  |
| opencv.ai | IP: 75.2.70.75 所属国家: United States of America 地区: Washington 城市: Seattle  |
| www.art-recognition.com | IP: 217.26.55.75 所属国家: Switzerland 地区: Zurich 城市: Zurich  |
| developer.mozilla.org | IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| peak.ai | IP: 46.101.67.35 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: London  |
| x.com | IP: 162.159.140.229 所属国家: United States of America 地区: California 城市: San Francisco  |
| bsc-dataseed.bnbchain.org | IP: 54.199.224.107 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| www.facebook.com | IP: 31.13.95.37 所属国家: Ireland 地区: Dublin 城市: Dublin  |
| www.respeecher.com | IP: 199.60.103.30 所属国家: United States of America 地区: Massachusetts 城市: Cambridge  |
| feross.org | IP: 50.116.11.184 所属国家: United States of America 地区: California 城市: Fremont  |
| www.uipath.com | IP: 104.18.174.91 所属国家: United States of America 地区: California 城市: San Francisco  |
| stability.ai | IP: 198.49.23.144 所属国家: United States of America 地区: New York 城市: New York City  |
| openai.com | IP: 104.18.33.45 所属国家: United States of America 地区: California 城市: San Francisco  |
| runwayml.com | IP: 76.76.21.21 所属国家: United States of America 地区: California 城市: Walnut  |
| code.google.com | IP: 142.251.188.102 所属国家: United States of America 地区: California 城市: Mountain View  |
| aws.amazon.com | IP: 18.65.168.66 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| er.dcloud.io | 没有服务器地理信息.  |
| tronscan.io | IP: 104.18.14.18 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.shadertoy.com | IP: 54.187.128.7 所属国家: United States of America 地区: Oregon 城市: Portland  |
| map.qq.com | IP: 116.130.224.82 所属国家: China 地区: Beijing 城市: Beijing  |
| api-testnet.bscscan.com | IP: 104.26.13.158 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.atomwise.com | IP: 141.193.213.20 所属国家: United States of America 地区: Texas 城市: Austin  |
| creativecommons.org | IP: 172.67.1.191 所属国家: United States of America 地区: California 城市: San Francisco  |
| api.trongrid.io | IP: 52.74.175.233 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| fontello.com | IP: 168.119.169.240 所属国家: Germany 地区: Bayern 城市: Gunzenhausen  |
| android.googlesource.com | IP: 142.251.188.82 所属国家: United States of America 地区: California 城市: Mountain View  |
| t.me | IP: 149.154.167.99 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: Warrington  |
| www.ai21.com | IP: 104.22.15.218 所属国家: United States of America 地区: California 城市: San Francisco  |
| api-sepolia.basescan.org | IP: 104.26.13.113 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.microsoft.com | IP: 221.194.156.64 所属国家: China 地区: Hebei 城市: Langfang  |
| scale.com | IP: 76.76.21.22 所属国家: United States of America 地区: California 城市: Walnut  |
| www.nuro.ai | IP: 52.76.120.174 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| www.glean.com | IP: 57.180.160.60 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| api-goerli-optimistic.etherscan.io | IP: 108.160.167.148 所属国家: United States of America 地区: California 城市: San Francisco  |
| api-amoy.polygonscan.com | IP: 104.26.12.96 所属国家: United States of America 地区: California 城市: San Francisco  |
| api-holesky.etherscan.io | IP: 39.109.122.128 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| www.tempus.com | IP: 146.190.199.140 所属国家: United States of America 地区: New Jersey 城市: North Bergen  |
| gasstation-testnet.polygon.technology | IP: 104.18.41.110 所属国家: United States of America 地区: California 城市: San Francisco  |
| ask.dcloud.net.cn | IP: 123.12.235.54 所属国家: China 地区: Henan 城市: Hebi  |
| www.eleuther.ai | IP: 198.185.159.144 所属国家: United States of America 地区: New York 城市: New York City  |
| er.dcloud.net.cn | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| sift.com | IP: 23.185.0.4 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.recursion.com | IP: 57.180.160.60 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| www.getnexar.com | IP: 3.168.245.2 所属国家: United States of America 地区: Washington 城市: Seattle  |
| covariant.ai | IP: 13.52.115.166 所属国家: United States of America 地区: California 城市: San Jose  |
| cdn.jsdelivr.net | IP: 46.82.174.69 所属国家: Germany 地区: Niedersachsen 城市: Braunschweig  |
| cloudflare-eth.com | IP: 104.18.11.112 所属国家: United States of America 地区: California 城市: San Francisco  |
| polygon-rpc.com | IP: 136.175.126.220 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.darktrace.com | IP: 34.210.109.146 所属国家: United States of America 地区: Oregon 城市: Portland  |
| www.h2o.ai | IP: 151.101.91.10 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  |
| aurora.tech | IP: 75.2.60.5 所属国家: United States of America 地区: Washington 城市: Seattle  |
| indiantypefoundry.comhttps | 没有服务器地理信息.  |
| www.spectre.ai | IP: 172.67.70.22 所属国家: United States of America 地区: California 城市: San Francisco  |
| maps.googleapis.com | IP: 142.250.217.74 所属国家: United States of America 地区: California 城市: Mountain View  |
| www.perplexity.ai | IP: 54.89.135.129 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| vuejs.org | IP: 3.33.186.135 所属国家: United States of America 地区: Washington 城市: Seattle  |
| api.aixinternal.art | IP: 104.26.1.33 所属国家: United States of America 地区: California 城市: San Francisco  |
| fetch.ai | IP: 104.26.14.93 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.preferred.jp | IP: 3.165.102.95 所属国家: United States of America 地区: Washington 城市: Seattle  |
| cohere.ai | IP: 76.76.21.21 所属国家: United States of America 地区: California 城市: Walnut  |
| gemini.google.com | IP: 142.250.217.78 所属国家: United States of America 地区: California 城市: Mountain View  |
| www.jsdelivr.com | IP: 104.21.23.24 所属国家: United States of America 地区: California 城市: San Francisco  |
| mistral.ai | IP: 104.18.23.152 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| pytorch.org | IP: 23.185.0.2 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.openair.com | IP: 141.148.57.163 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| crbug.com | IP: 216.239.32.29 所属国家: United States of America 地区: California 城市: Mountain View  |
| www.palantir.com | IP: 151.101.193.170 所属国家: United States of America 地区: California 城市: San Francisco  |
| x.ai | IP: 128.121.146.235 所属国家: United States of America 地区: California 城市: Sacramento  |
| tfhub.dev | IP: 35.244.233.98 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| www.pathai.com | IP: 104.18.10.32 所属国家: United States of America 地区: California 城市: San Francisco  |
| quilljs.com | IP: 172.66.43.93 所属国家: United States of America 地区: California 城市: San Francisco  |
| lame.sf.net64bits | 没有服务器地理信息.  |
| replit.com | IP: 104.18.35.46 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.ibm.com | IP: 23.35.121.153 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| www.inflection.ai | IP: 104.18.42.219 所属国家: United States of America 地区: California 城市: San Francisco  |
| schemas.android.com | 没有服务器地理信息.  |
| aleph-alpha.com | IP: 91.99.26.32 所属国家: Finland 地区: Uusimaa 城市: Helsinki  |
| insilico.com | IP: 185.215.4.66 所属国家: Russian Federation 地区: Moskva 城市: Moscow  |
| api-goerli.etherscan.io | IP: 118.193.240.37 所属国家: China 地区: Beijing 城市: Beijing  |
| docs.ethers.org | IP: 18.172.31.57 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| api.basescan.org | IP: 172.67.75.129 所属国家: United States of America 地区: California 城市: San Francisco  |
| fontello.comcreated | 没有服务器地理信息.  |
| www.aeye.ai | IP: 35.190.31.54 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| www.descarteslabs.com | IP: 199.60.103.254 所属国家: United States of America 地区: Massachusetts 城市: Cambridge  |
| www.nvidia.com | IP: 23.210.26.154 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| webapi.amap.com | IP: 111.202.5.199 所属国家: China 地区: Beijing 城市: Beijing  |
| encrypted-tbn0.gstatic.com | IP: 142.250.217.78 所属国家: United States of America 地区: California 城市: Mountain View  |
| www.datarobot.com | IP: 23.185.0.2 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  |
| zoox.com | IP: 3.165.102.109 所属国家: United States of America 地区: Washington 城市: Seattle  |
| www.graphcore.ai | IP: 199.60.103.28 所属国家: United States of America 地区: Massachusetts 城市: Cambridge  |
| www.raiclabs.com | IP: 74.208.236.101 所属国家: United States of America 地区: Pennsylvania 城市: Philadelphia  |
| www.adept.ai | IP: 76.76.21.98 所属国家: United States of America 地区: California 城市: Walnut  |
| writesonic.com | IP: 162.125.34.133 所属国家: United States of America 地区: California 城市: San Francisco  |

### **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  |
| http://ns.adobe.com/xap/1.0/\u0000  | io/dcloud/common/util/ExifInterface.java  |
| https://m3w.cn/s/  | io/dcloud/common/util/ShortCutUtil.java  |
| https://ask.dcloud.net.cn/article/282  | io/dcloud/common/constant/DOMException.java  |
| https://ask.dcloud.net.cn/article/35058  | io/dcloud/feature/audio/AudioRecorderMgr.java  |
| https://ask.dcloud.net.cn/article/283  | io/dcloud/feature/utsplugin/ProxyModule.java  |
| https://er.dcloud.io/sc  | io/dcloud/feature/gg/dcloud/ADHandler.java  |
| https://er.dcloud.net.cn/sc  | io/dcloud/feature/gg/dcloud/ADHandler.java  |
| https://ask.dcloud.net.cn/article/35627  | io/dcloud/p/r.java  |
| https://ask.dcloud.net.cn/article/35877  | io/dcloud/p/r.java  |
| https://ask.dcloud.net.cn/article/283  | io/dcloud/p/g1.java  |
| https://er.dcloud.io/rv  | io/dcloud/p/d0.java  |
| https://er.dcloud.net.cn/rv  | io/dcloud/p/d0.java  |
| https://ask.dcloud.net.cn/article/287  | io/dcloud/share/IFShareApi.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/GifViewUtils.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/GifTextureView.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/GifTextView.java  |
| https://ask.dcloud.net.cn/article/36199  | 摸瓜V1引擎  |
| https://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://tronscan.io/  | 摸瓜V2引擎  |
| https://bscscan.com/tx/0x  | 摸瓜V2引擎  |
| https://openai.com  | 摸瓜V2引擎  |
| https://aixwallet.net  | 摸瓜V2引擎  |
| https://gemini.google.com  | 摸瓜V2引擎  |
| https://www.microsoft.com/en/ai  | 摸瓜V2引擎  |
| https://www.ibm.com/watson  | 摸瓜V2引擎  |
| https://aws.amazon.com/ai/machine-learning/  | 摸瓜V2引擎  |
| https://www.nvidia.com/en-us/  | 摸瓜V2引擎  |
| https://ai.meta.com/  | 摸瓜V2引擎  |
| https://www.salesforce.com/artificial-intelligence/  | 摸瓜V2引擎  |
| https://www.clarifai.com  | 摸瓜V2引擎  |
| https://opencv.ai  | 摸瓜V2引擎  |
| https://stability.ai  | 摸瓜V2引擎  |
| https://www.artisse.ai  | 摸瓜V2引擎  |
| https://www.art-recognition.com  | 摸瓜V2引擎  |
| https://runwayml.com  | 摸瓜V2引擎  |
| https://www.synthesia.io  | 摸瓜V2引擎  |
| https://cohere.ai  | 摸瓜V2引擎  |
| https://huggingface.co  | 摸瓜V2引擎  |
| https://www.perplexity.ai  | 摸瓜V2引擎  |
| https://www.inflection.ai  | 摸瓜V2引擎  |
| https://mistral.ai  | 摸瓜V2引擎  |
| https://aleph-alpha.com  | 摸瓜V2引擎  |
| https://www.eleuther.ai  | 摸瓜V2引擎  |
| https://writesonic.com  | 摸瓜V2引擎  |
| https://undetectable.ai  | 摸瓜V2引擎  |
| https://www.ai21.com  | 摸瓜V2引擎  |
| https://www.respeecher.com  | 摸瓜V2引擎  |
| https://www.uipath.com  | 摸瓜V2引擎  |
| https://www.datarobot.com  | 摸瓜V2引擎  |
| https://www.h2o.ai  | 摸瓜V2引擎  |
| https://www.vicarious.com  | 摸瓜V2引擎  |
| https://www.cognitivescale.com  | 摸瓜V2引擎  |
| https://www.graphcore.ai  | 摸瓜V2引擎  |
| https://www.preferred.jp/en/  | 摸瓜V2引擎  |
| https://www.anthropic.com  | 摸瓜V2引擎  |
| https://x.ai  | 摸瓜V2引擎  |
| https://www.adept.ai  | 摸瓜V2引擎  |
| https://covariant.ai  | 摸瓜V2引擎  |
| https://www.openair.com  | 摸瓜V2引擎  |
| https://www.tempus.com  | 摸瓜V2引擎  |
| https://www.butterflynetwork.com  | 摸瓜V2引擎  |
| https://www.arterys.com  | 摸瓜V2引擎  |
| https://www.freenome.com  | 摸瓜V2引擎  |
| https://www.recursion.com  | 摸瓜V2引擎  |
| https://www.atomwise.com  | 摸瓜V2引擎  |
| https://benevolent.com  | 摸瓜V2引擎  |
| https://www.pathai.com  | 摸瓜V2引擎  |
| https://zoox.com  | 摸瓜V2引擎  |
| https://www.nuro.ai  | 摸瓜V2引擎  |
| https://www.aeye.ai  | 摸瓜V2引擎  |
| https://aurora.tech  | 摸瓜V2引擎  |
| https://waymo.com  | 摸瓜V2引擎  |
| https://www.getnexar.com  | 摸瓜V2引擎  |
| https://www.visteon.com  | 摸瓜V2引擎  |
| https://sift.com  | 摸瓜V2引擎  |
| https://www.darktrace.com  | 摸瓜V2引擎  |
| https://www.palantir.com  | 摸瓜V2引擎  |
| https://www.bluerivertechnology.com  | 摸瓜V2引擎  |
| https://www.descarteslabs.com  | 摸瓜V2引擎  |
| https://scale.com  | 摸瓜V2引擎  |
| https://replit.com  | 摸瓜V2引擎  |
| https://fetch.ai  | 摸瓜V2引擎  |
| https://www.raiclabs.com  | 摸瓜V2引擎  |
| https://pytorch.org  | 摸瓜V2引擎  |
| https://www.glean.com  | 摸瓜V2引擎  |
| https://www.mindfoundry.ai  | 摸瓜V2引擎  |
| https://peak.ai  | 摸瓜V2引擎  |
| https://www.caper.ai  | 摸瓜V2引擎  |
| https://www.spectre.ai  | 摸瓜V2引擎  |
| https://insilico.com  | 摸瓜V2引擎  |
| https://gateway.ipfs.io/ipfs/  | 摸瓜V2引擎  |
| https://github.com/ethers-io/ethers.js/issues/4537  | 摸瓜V2引擎  |
| https://gateway.ipfs.io/ipfs/$  | 摸瓜V2引擎  |
| https://gasstation.polygon.technology/v2  | 摸瓜V2引擎  |
| https://gasstation-testnet.polygon.technology/v2  | 摸瓜V2引擎  |
| https://docs.ethers.org/api-keys/  | 摸瓜V2引擎  |
| https://$  | 摸瓜V2引擎  |
| https://cloudflare-eth.com/  | 摸瓜V2引擎  |
| https://api.etherscan.io  | 摸瓜V2引擎  |
| https://api-goerli.etherscan.io  | 摸瓜V2引擎  |
| https://api-sepolia.etherscan.io  | 摸瓜V2引擎  |
| https://api-holesky.etherscan.io  | 摸瓜V2引擎  |
| https://api.arbiscan.io  | 摸瓜V2引擎  |
| https://api-goerli.arbiscan.io  | 摸瓜V2引擎  |
| https://api.basescan.org  | 摸瓜V2引擎  |
| https://api-sepolia.basescan.org  | 摸瓜V2引擎  |
| https://api.bscscan.com  | 摸瓜V2引擎  |
| https://api-testnet.bscscan.com  | 摸瓜V2引擎  |
| https://api.polygonscan.com  | 摸瓜V2引擎  |
| https://api-amoy.polygonscan.com  | 摸瓜V2引擎  |
| https://api-testnet.polygonscan.com  | 摸瓜V2引擎  |
| https://api-optimistic.etherscan.io  | 摸瓜V2引擎  |
| https://api-goerli-optimistic.etherscan.io  | 摸瓜V2引擎  |
| https://polygon-rpc.com/  | 摸瓜V2引擎  |
| https://rpc-amoy.polygon.technology/  | 摸瓜V2引擎  |
| https://feross.org/opensource>  | 摸瓜V2引擎  |
| https://api.trongrid.io  | 摸瓜V2引擎  |
| https://bsc-dataseed.bnbchain.org  | 摸瓜V2引擎  |
| https://t.me/aixwalletgroup  | 摸瓜V2引擎  |
| https://x.com/@AixWallet  | 摸瓜V2引擎  |
| https://www.facebook.com/AixWallet/  | 摸瓜V2引擎  |
| https://api.aixinternal.art  | 摸瓜V2引擎  |
| https://apis.map.qq.com/jsapi?qt=translate&type=1&points=$  | 摸瓜V2引擎  |
| https://github.com/uuidjs/uuid  | 摸瓜V2引擎  |
| https://vuejs.org/error-reference/  | 摸瓜V2引擎  |
| https://service.dcloud.net.cn/uniapp/feedback.html  | 摸瓜V2引擎  |
| https://map.qq.com/api/js?v=2.exp&  | 摸瓜V2引擎  |
| https://maps.googleapis.com/maps/api/js?  | 摸瓜V2引擎  |
| https://webapi.amap.com/maps?v=2.0&  | 摸瓜V2引擎  |
| https://api.map.baidu.com/api?type=webgl&v=1.0&  | 摸瓜V2引擎  |
| https://quilljs.com/  | 摸瓜V2引擎  |
| https://quilljs.com  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://code.google.com/p/dat-gui  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| https://upload.kp.io/api/fileDirect/v1/uploadCommonFile',  | 摸瓜V2引擎  |
| http://127.0.0.1:8807/api/fileDirect/v1/uploadCommonFile',  | 摸瓜V2引擎  |
| https://cdn.jsdelivr.net/npm/@tensorflow/tfjs-backend-wasm@$  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| https://developer.mozilla.org/en-US/docs/Web/API/Fetch\_API)  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| https://tfhub.dev/mediapipe/tfjs-model/face\_detection/short/1  | 摸瓜V2引擎  |
| https://tfhub.dev/mediapipe/tfjs-model/face\_detection/full/1  | 摸瓜V2引擎  |
| https://tfhub.dev  | 摸瓜V2引擎  |
| https://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| https://github.com/tensorflow/tfjs/issues  | 摸瓜V2引擎  |
| https://www.jsdelivr.com/using-sri-with-dynamic-files  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| https://www.shadertoy.com/view/4djSRW\n  | 摸瓜V2引擎  |
| https://github.com/tensorflow/tfjs/issues/1735\n  | 摸瓜V2引擎  |
| https://github.com/tensorflow/tfjs/issues/5447\n  | 摸瓜V2引擎  |
| https://arxiv.org/abs/1706.02515\n  | 摸瓜V2引擎  |
| https://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| https://developer.mozilla.org/en-US/docs/Web/API/Fetch\_API)  | 摸瓜V2引擎  |
| https://vulcansphere.com  | 摸瓜V3引擎  |
| https://developer.mozilla.org/en-US/docs/Web/API/Fetch\_API  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res-auto00androidx.appcompat.widget.ActionBarOverlayLayout  | 摸瓜V3引擎  |
| https://ask.dcloud.net.cn/article/282  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/android00androidx.appcompat.widget.FitWindowsLinearLayout((androi  | 摸瓜V3引擎  |
| https://er.dcloud.net.cn/rv  | 摸瓜V3引擎  |
| http://www.inkscape.org/namespaces/inkscape  | 摸瓜V3引擎  |
| http://creativecommons.org/ns#  | 摸瓜V3引擎  |
| https://ask.dcloud.net.cn/article/35627  | 摸瓜V3引擎  |
| http://fontello.com  | 摸瓜V3引擎  |
| https://android.googlesource.com/toolchain/llvm  | 摸瓜V3引擎  |
| https://indiantypefoundry.comhttps://www.indiantypefoundry.comThis  | 摸瓜V3引擎  |
| https://er.dcloud.io/sc  | 摸瓜V3引擎  |
| http://www.inkscape.org/  | 摸瓜V3引擎  |
| http://fontello.comCreated  | 摸瓜V3引擎  |
| http://lame.sf.net  | 摸瓜V3引擎  |
| https://android.googlesource.com/toolchain/llvm-project  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/android//com.taobao.weex.ui.view.listview.WXRecyclerView  | 摸瓜V3引擎  |
| https://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V3引擎  |
| https://ask.dcloud.net.cn/article/35058  | 摸瓜V3引擎  |
| https://ask.dcloud.net.cn/article/35877  | 摸瓜V3引擎  |
| http://lame.sf.net64bits  | 摸瓜V3引擎  |
| discover-pa.googleapis.com  | 摸瓜V3引擎  |
| https://er.dcloud.io/rv  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res-auto  | 摸瓜V3引擎  |
| https://m3w.cn/s/  | 摸瓜V3引擎  |
| https://fontshare.com/termsAlternate  | 摸瓜V3引擎  |
| https://android.googlesource.com/toolchain/clang  | 摸瓜V3引擎  |
| http://sodipodi.sourceforge.net/DTD/sodipodi-0.dtd  | 摸瓜V3引擎  |
| https://ask.dcloud.net.cn/article/287  | 摸瓜V3引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V3引擎  |
| https://ask.dcloud.net.cn/article/283  | 摸瓜V3引擎  |
| encrypted-tbn0.gstatic.com  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/android  | 摸瓜V3引擎  |
| https://er.dcloud.net.cn/sc  | 摸瓜V3引擎  |
| https://%https://ask.dcloud.net.cn/article/283%https://ask.dcloud.net.cn/article/287  | 摸瓜V3引擎  |
| https://crbug.com/v8/8520  | lib/armeabi-v7a/libweexjss.so  |
| http://lame.sf.net  | lib/armeabi-v7a/liblamemp3.so  |
| http://ns.adobe.com/xap/1.0/  | lib/armeabi-v7a/libnative-imagetranscoder.so  |
| http://ns.adobe.com/xap/1.0/  | lib/armeabi-v7a/libstatic-webp.so  |
| https://crbug.com/v8/8520  | lib/x86/libweexjss.so  |
| http://lame.sf.net  | lib/x86/liblamemp3.so  |
| https://crbug.com/v8/8520  | lib/arm64-v8a/libweexjss.so  |
| http://lame.sf.net  | lib/arm64-v8a/liblamemp3.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| rfe@rm.rs 0bje@bm.bwayc me@ricmoo.com official@aixwallets.com  | 摸瓜V2引擎  |
| ghcs@cnma.ilr  | 摸瓜V2引擎  |
| official@aixwallets.com  | 摸瓜V2引擎  |
| jhruby.web@gmail.com  | 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: CN=appxx, OU=appxx, O=appxx, L=newyork, ST=newyork, C=aa 签名算法: rsassa\_pkcs1v15 有效期自: 2025-01-29 02:42:57+00:00 有效期至: 2075-01-17 02:42:57+00:00 发行人: CN=appxx, OU=appxx, O=appxx, L=newyork, ST=newyork, C=aa 序列号: 0x1 哈希算法: sha256 md5值: 38ec8fd7dc66de72e1d69d4427187b26 sha1值: 3406ff9c0de6605cab1bfefb4b8663869d59653b sha256值: acd1940e938f126d60e4b1ab2ff37596082e9c76e5f870bfd0270bfb7a51058e sha512值: 3018d665908ef1b0659e710d349bfe28ae6ca23ce645b93ed2d524974f2c0c4d1fa726f119f10009881294b905399b94a76b58ea3d2c2519a5caa53d896a1e9c 公钥算法: rsa 密钥长度: 2048 指纹: c23319c139cc1d06c6d733ce0d96fddff66be8a0878f644e1db846b8cc976729**

## **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\_feature\_confusion\_exception\_no\_private\_key\_input" : "no private key input"  |
| "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\_feature\_confusion\_exception\_no\_private\_key\_input" : "私钥数据为空"  |
| "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.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 |
| app.aix.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ACCESS\_WIFI\_STATE | 正常 | 查看Wi-Fi状态 | 允许应用程序查看有关 Wi-Fi 状态的信息 |
| android.permission.INSTALL\_PACKAGES | 系统需要 | 直接安装应用程序 | 允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序 |
| android.permission.REQUEST\_INSTALL\_PACKAGES | 危险 | 允许应用程序请求安装包。 | 恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。 |
| android.permission.CAPTURE\_AUDIO\_OUTPUT | 系统需要 |  | 允许应用程序捕获音频输出。 |
| android.permission.CAPTURE\_SECURE\_VIDEO\_OUTPUT | 正常 |  | 允许应用程序捕获安全视频输出 |
| android.permission.CAPTURE\_VIDEO\_OUTPUT | 正常 |  | 允许应用程序捕获视频输出 |
| 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.CLEAR\_APP\_CACHE | 系统需要 | 删除所有应用程序缓存数据 | 允许应用程序通过删除应用程序缓存目录中的文件来释放手机存储空间。访问通常非常受限于系统进程。  |
| android.permission.CLEAR\_APP\_USER\_DATA | 合法 | 删除其他应用程序数据 | 允许应用程序清除用户数据 |
| android.permission.DELETE\_CACHE\_FILES | 系统需要 | 删除其他应用程序缓存 | 允许应用程序删除缓存文件 |
| android.permission.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| android.permission.GET\_ACCOUNTS | 危险 | 列出帐户 | 允许访问账户服务中的账户列表 |
| android.permission.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.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。 |

## **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。**