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

**TOKENBUFF（ 1.0.1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 | TOKENBUFF |
| 版本 | 1.0.1 |
| 包名 | com.tokenbuff.wallet |
| 域名线索 | 58条 |
| URL线索 | 41条 |
| APP图标 |  |
| 分析日期 | 2025年7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 | TOKENBUFF1.0.1.apk |
| 文件大小 | 81.84MB |
| MD5值 | 89e31c232d3b7bf324c08f82c3916e7e |
| SHA1值 | c140c16cc7d55596e58d983f2b3899e23139428b |
| SHA256值 | e0cede65a5f01bf6f727460fafe1131d5f6cd0b5c0f23059b5c4f76517bf3e40 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | TOKENBUFF |
| 包名 | com.tokenbuff.wallet |
| 主活动Activity | com.tokenbuff.wallet.MainActivity |
| 安卓版本名称 | 1.0.1 |
| 安卓版本 | 2 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| grs.dbankcloud.com | IP: 60.28.193.195 所属国家: China 地区: Tianjin 城市: Tianjin  |
| cn.register.xmpush.xiaomi.com | IP: 123.125.102.39 所属国家: China 地区: Beijing 城市: Beijing  |
| issuetracker.google.com | IP: 142.250.217.78 所属国家: United States of America 地区: California 城市: Mountain View  |
| 10.38.162.35 | IP: 10.38.162.35 所属国家: - 地区: - 城市: -  |
| api.etherscan.io | IP: 199.59.148.247 所属国家: United States of America 地区: California 城市: San Francisco  |
| api-push.in.meizu.com | IP: 206.161.233.191 所属国家: United States of America 地区: Virginia 城市: Herndon  |
| crbug.com | IP: 216.239.32.29 所属国家: United States of America 地区: California 城市: Mountain View  |
| api.testnet.solana.com | IP: 103.56.16.112 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| www.webrtc.org | IP: 142.250.217.110 所属国家: United States of America 地区: California 城市: Mountain View  |
| journeyapps.com | IP: 18.155.68.86 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| infura.io | IP: 65.9.42.46 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| resolver.msg.xiaomi.net | IP: 110.43.0.169 所属国家: China 地区: Beijing 城市: Beijing  |
| metrics5.dt.dbankcloud.ru | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| developer.android.com | IP: 142.250.217.78 所属国家: United States of America 地区: California 城市: Mountain View  |
| api.flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| aomediacodec.github.io | IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| feross.org | IP: 50.116.11.184 所属国家: United States of America 地区: California 城市: Fremont  |
| data-drru.push.dbankcloud.com | IP: 159.138.202.31 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| www.jsdelivr.com | IP: 172.67.208.113 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| play.google.com | IP: 93.46.8.90 所属国家: Italy 地区: Lombardia 城市: Milan  |
| xml.org | IP: 104.239.240.11 所属国家: United States of America 地区: Texas 城市: Windcrest  |
| grs.dbankcloud.eu | 没有服务器地理信息.  |
| www.unicode.org | IP: 64.182.27.164 所属国家: United States of America 地区: Texas 城市: Dallas  |
| api-kovan.etherscan.io | IP: 103.214.168.106 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| dartbug.com | IP: 216.239.32.21 所属国家: United States of America 地区: California 城市: Mountain View  |
| docs.flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| web3.gastracker.io | 没有服务器地理信息.  |
| www.ietf.org | IP: 104.16.44.99 所属国家: United States of America 地区: California 城市: San Francisco  |
| links.ethers.org | IP: 13.35.238.59 所属国家: India 地区: Telangana 城市: Hyderabad  |
| grs.platform.dbankcloud.ru | 没有服务器地理信息.  |
| api-push.meizu.com | IP: 221.5.93.66 所属国家: China 地区: Guangdong 城市: Foshan  |
| grs.dbankcloud.cn | IP: 49.4.35.251 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| developer.apple.com | IP: 17.253.87.198 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| g.co | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| api.mainnet-beta.solana.com | IP: 162.125.32.12 所属国家: United States of America 地区: California 城市: San Francisco  |
| grs.dbankcloud.asia | IP: 121.36.117.149 所属国家: China 地区: Beijing 城市: Beijing  |
| api-goerli.etherscan.io | IP: 210.56.51.192 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| xmlpull.org | IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| norma-external-collect.meizu.com | IP: 183.60.176.112 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| metrics-dra.dt.hicloud.com | IP: 94.74.88.100 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| metrics2.data.hicloud.com | IP: 80.158.38.48 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| api-ropsten.etherscan.io | IP: 208.31.254.33 所属国家: United States of America 地区: District of Columbia 城市: Washington  |
| default.url | 没有服务器地理信息.  |
| api-rinkeby.etherscan.io | IP: 65.49.26.97 所属国家: United States of America 地区: Missouri 城市: Saint Louis  |
| data-dra.push.dbankcloud.com | IP: 119.8.163.189 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| docs.rs | IP: 13.33.88.114 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| data-drcn.push.dbankcloud.com | IP: 49.4.40.58 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| webrtc.googlesource.com | IP: 74.125.197.82 所属国家: United States of America 地区: California 城市: Mountain View  |
| metrics5.data.hicloud.com | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| schemas.microsoft.com | IP: 13.107.246.73 所属国家: United States of America 地区: Washington 城市: Redmond  |
| metrics1.data.hicloud.com | IP: 111.202.16.252 所属国家: China 地区: Beijing 城市: Beijing  |
| data-dre.push.dbankcloud.com | IP: 80.158.49.244 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| api.devnet.solana.com | IP: 108.160.165.212 所属国家: United States of America 地区: California 城市: San Francisco  |
| goo.gle | IP: 67.199.248.12 所属国家: United States of America 地区: New York 城市: New York City  |
| dashif.org | IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| ns.adobe.com | 没有服务器地理信息.  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://)([\\s\\S]+)  | com/huawei/hms/scankit/p/C0233bd.java  |
| http://xml.org/sax/features/namespaces  | com/huawei/secure/android/common/xml/DocumentBuilderFactorySecurity.java  |
| http://xml.org/sax/features/validation  | com/huawei/secure/android/common/xml/DocumentBuilderFactorySecurity.java  |
| http://xml.org/sax/features/namespaces  | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java  |
| http://xml.org/sax/features/namespace-prefixes  | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java  |
| http://xml.org/sax/features/validation  | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java  |
| http://xml.org/sax/features/external-general-entities  | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java  |
| http://xml.org/sax/features/external-parameter-entities  | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java  |
| http://xml.org/sax/features/string-interning  | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java  |
| http://xmlpull.org/v1/doc/features.html  | com/huawei/secure/android/common/xml/XmlPullParserFactorySecurity.java  |
| https://api-push.meizu.com/garcia/api/server/getPublicKey  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| https://api-push.meizu.com/garcia/api/server/getPushConf  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| https://api-push.in.meizu.com  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| https://api-push.meizu.com  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| https://norma-external-collect.meizu.com/android/exchange/getpublickey.do  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| https://norma-external-collect.meizu.com/push/android/external/add.do  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| https://api-push.meizu.com/garcia/api/client/  | com/meizu/cloud/pushsdk/platform/c/a.java  |
| https://api-push.in.meizu.com/garcia/api/client/  | com/meizu/cloud/pushsdk/platform/c/a.java  |
| https://api-push.meizu.com/garcia/api/client/log/upload  | com/meizu/cloud/pushsdk/platform/c/a.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/fh.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/fw.java  |
| https://%1$s/gslb/?ver=5.0  | com/xiaomi/push/ch.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/fx.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/ex.java  |
| http://10.38.162.35:9085  | com/xiaomi/push/service/q.java  |
| https://cn.register.xmpush.xiaomi.com  | com/xiaomi/push/service/q.java  |
| https://resolver.msg.xiaomi.net/psc/?t=a  | com/xiaomi/push/service/ax.java  |
| http://ns.adobe.com/xap/1.0/\u0000  | defpackage/op0.java  |
| https://developer.apple.com/streaming/emsg-id3  | defpackage/to0.java  |
| https://developer.android.com/guide/topics/media/issues/cleartext-not-permitted  | defpackage/b71.java  |
| https://play.google.com/store/apps/details?id=  | defpackage/oe1.java  |
| https://github.com/Baseflow/flutter-permission-handler/issues  | defpackage/c62.java  |
| http://g.co/dev/packagevisibility.  | defpackage/sk2.java  |
| http://ns.adobe.com/xap/1.0/  | defpackage/ld1.java  |
| https://goo.gle/compose-feedback  | defpackage/gw.java  |
| https://x</LA\_URL>  | defpackage/x21.java  |
| https://default.url  | defpackage/x21.java  |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense  | defpackage/i71.java  |
| https://issuetracker.google.com/issues/new?component=907884&template=1466542  | defpackage/u03.java  |
| http://dashif.org/guidelines/last-segment-number  | defpackage/c20.java  |
| http://dashif.org/guidelines/trickmode  | defpackage/c20.java  |
| http://dashif.org/thumbnail\_tile  | defpackage/c20.java  |
| http://dashif.org/guidelines/thumbnail\_tile  | defpackage/c20.java  |
| https://developer.android.com/guide/topics/media/issues/player-accessed-on-wrong-thread  | defpackage/as0.java  |
| https://developer.android.com/guide/topics/permissions/overview  | io/flutter/plugin/platform/PlatformPlugin.java  |
| https://docs.flutter.dev/deployment/android  | io/flutter/embedding/engine/loader/FlutterLoader.java  |
| https://journeyapps.com/  | 摸瓜V1引擎  |
| https://github.com/journeyapps/zxing-android-embedded  | 摸瓜V1引擎  |
| https://data-drcn.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-dra.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-dre.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-drru.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://metrics1.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics-dra.dt.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics2.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics5.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics5.dt.dbankcloud.ru:6447  | 摸瓜V2引擎  |
| https://grs.dbankcloud.com  | 摸瓜V2引擎  |
| https://grs.dbankcloud.cn  | 摸瓜V2引擎  |
| https://grs.dbankcloud.asia  | 摸瓜V2引擎  |
| https://grs.platform.dbankcloud.ru  | 摸瓜V2引擎  |
| https://grs.dbankcloud.eu  | 摸瓜V2引擎  |
| https://api.etherscan.io  | 摸瓜V2引擎  |
| https://api-ropsten.etherscan.io  | 摸瓜V2引擎  |
| https://api-rinkeby.etherscan.io  | 摸瓜V2引擎  |
| https://api-kovan.etherscan.io  | 摸瓜V2引擎  |
| https://api-goerli.etherscan.io  | 摸瓜V2引擎  |
| https://infura.io)  | 摸瓜V2引擎  |
| https://web3.gastracker.io  | 摸瓜V2引擎  |
| https://web3.gastracker.io/morden  | 摸瓜V2引擎  |
| http://feross.org>  | 摸瓜V2引擎  |
| https://feross.org>  | 摸瓜V2引擎  |
| https://github.com/indutny/elliptic/issues  | 摸瓜V2引擎  |
| https://github.com/indutny/elliptic  | 摸瓜V2引擎  |
| https://links.ethers.org/v5-errors-  | 摸瓜V2引擎  |
| http://api.devnet.solana.com  | 摸瓜V2引擎  |
| http://api.testnet.solana.com  | 摸瓜V2引擎  |
| http://api.mainnet-beta.solana.com/  | 摸瓜V2引擎  |
| https://api.devnet.solana.com  | 摸瓜V2引擎  |
| https://api.testnet.solana.com  | 摸瓜V2引擎  |
| https://api.mainnet-beta.solana.com/  | 摸瓜V2引擎  |
| https://github.com/indutny/elliptic/issues  | 摸瓜V2引擎  |
| https://github.com/indutny/elliptic  | 摸瓜V2引擎  |
| https://github.com/uuidjs/uuid  | 摸瓜V2引擎  |
| https://github.com/nodeca/pica  | 摸瓜V2引擎  |
| https://www.jsdelivr.com/using-sri-with-dynamic-files  | 摸瓜V2引擎  |
| https://github.com/apvarun/toastify-js  | 摸瓜V2引擎  |
| http://agoratest  | lib/arm64-v8a/libagora-rtc-sdk.so  |
| http://s?  | lib/arm64-v8a/libagora-rtc-sdk.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/abs-capture-time  | lib/arm64-v8a/libagora-rtc-sdk.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/generic-frame-descriptor  | lib/arm64-v8a/libagora-rtc-sdk.so  |
| https://api.flutter.dev/flutter/material/Scaffold/of.html  | lib/arm64-v8a/libapp.so  |
| http://www.unicode.org/copyright.html  | lib/arm64-v8a/libflutter.so  |
| https://docs.flutter.dev/release/breaking-changes/android-surface-plugins  | lib/arm64-v8a/libflutter.so  |
| https://github.com/flutter/flutter/issues.  | lib/arm64-v8a/libflutter.so  |
| https://dartbug.com/52121.  | lib/arm64-v8a/libflutter.so  |
| https://crbug.com/1053756  | lib/arm64-v8a/libjingle\_peerconnection\_so.so  |
| https://webrtc.googlesource.com/src/+/refs/heads/main/docs/native-code/rtp-hdrext/playout-delay/,  | lib/arm64-v8a/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/transport-wide-cc-02  | lib/arm64-v8a/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/generic-frame-descriptor-00  | lib/arm64-v8a/libjingle\_peerconnection\_so.so  |
| https://aomediacodec.github.io/av1-rtp-spec/  | lib/arm64-v8a/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/abs-capture-time  | lib/arm64-v8a/libjingle\_peerconnection\_so.so  |
| http://www.ietf.org/id/draft-holmer-rmcat-transport-wide-cc-extensions-01  | lib/arm64-v8a/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/abs-send-time  | lib/arm64-v8a/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/video-content-type  | lib/arm64-v8a/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/video-timing  | lib/arm64-v8a/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/video-layers-allocation00  | lib/arm64-v8a/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/playout-delay  | lib/arm64-v8a/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/color-space  | lib/arm64-v8a/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/video-frame-tracking-id  | lib/arm64-v8a/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/inband-cn  | lib/arm64-v8a/libjingle\_peerconnection\_so.so  |
| https://docs.rs/getrandom  | lib/arm64-v8a/librust\_bdk\_ffi.so  |
| http://scheme  | lib/arm64-v8a/librust\_bdk\_ffi.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| feross@feross.org git@github.com fedor@indutny.com  | 摸瓜V2引擎  |
| git@github.com fedor@indutny.com superstruct@0.11  | 摸瓜V2引擎  |
| appro@openssl.org  | lib/arm64-v8a/libagora-ffmpeg.so  |
| appro@openssl.org  | lib/arm64-v8a/libagora-rtc-sdk.so  |
| appro@openssl.org  | lib/arm64-v8a/libagora\_face\_capture\_extension.so  |
| appro@openssl.org  | lib/arm64-v8a/libagora\_lip\_sync\_extension.so  |
| appro@openssl.org  | lib/arm64-v8a/libagora\_video\_av1\_decoder\_extension.so  |
| appro@openssl.org  | lib/arm64-v8a/libagora\_video\_av1\_encoder\_extension.so  |
| appro@openssl.org  | lib/arm64-v8a/libagora\_video\_decoder\_extension.so  |
| appro@openssl.org  | lib/arm64-v8a/libagora\_video\_encoder\_extension.so  |
| appro@openssl.org  | lib/arm64-v8a/libflutter.so  |
| appro@openssl.org  | lib/arm64-v8a/libjingle\_peerconnection\_so.so  |
| appro@openssl.org  | lib/arm64-v8a/librust\_bdk\_ffi.so  |
| nf@xpfr6ktsre6gbytuwtg.tgmq6k3flf dshu7immlpkc@mbst14hc.dwicgkl  | lib/arm64-v8a/libvideo\_dec.so  |
| nf@xpfr6ktsre6gbytuwtg.tgmq6k3flf dshu7immlpkc@mbst14hc.dwicgkl  | lib/arm64-v8a/libvideo\_enc.so  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 19919152923  | 摸瓜V2引擎  |
| 19919152923  | 摸瓜V2引擎  |

## **5. 签名证书**

**APK已签名 v1 签名: False v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown 签名算法: rsassa\_pkcs1v15 有效期自: 2024-12-19 16:22:28+00:00 有效期至: 2124-11-25 16:22:28+00:00 发行人: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown 序列号: 0x1c1f1e8e 哈希算法: sha256 md5值: 4f399aa03366630029494df4ff9f3bd5 sha1值: e7b91643b6cecb8fa58e0fa8e6a90e0c511817c1 sha256值: f80e368e946c8d24c8f5ff194264d5d3f96fe89ea1105d2d4f30f72570213fc5 sha512值: bfdbc392a4aab081c0149a876d137611612cd2ad31000a12b405758b7719568783ab957bf05a1642034275792775997a7e6b6b10a3323621bf56cf6fd0c3c7fe 公钥算法: rsa 密钥长度: 2048 指纹: 9f2e58413555b3d756aea8714bc711ce5c583aa3005a95a097b33823d190237c**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "ENGAGELAB\_PRIVATES\_CHANNEL\_high" : "HIGH"  |
| "ENGAGELAB\_PRIVATES\_CHANNEL\_low" : "LOW"  |
| "ENGAGELAB\_PRIVATES\_CHANNEL\_normal" : "NORMAL"  |
| "ENGAGELAB\_PRIVATES\_CHANNEL\_silence" : "SILENCE"  |
| "library\_zxingandroidembedded\_author" : "JourneyApps"  |
| "library\_zxingandroidembedded\_authorWebsite" : "https://journeyapps.com/"  |
| "ENGAGELAB\_PRIVATES\_CHANNEL\_high" : "重要"  |
| "ENGAGELAB\_PRIVATES\_CHANNEL\_low" : "不重要"  |
| "ENGAGELAB\_PRIVATES\_CHANNEL\_normal" : "普通"  |
| "ENGAGELAB\_PRIVATES\_CHANNEL\_silence" : "静默"  |

## **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.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.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.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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| android.permission.USE\_BIOMETRIC | 正常 |  | 允许应用使用设备支持的生物识别模式。 |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.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.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.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.RECEIVE\_BOOT\_COMPLETED | 正常 | 开机时自动启动 | 允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度 |
| 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.BLUETOOTH | 正常 | 创建蓝牙连接 | 允许应用程序连接到配对的蓝牙设备 |
| android.permission.BLUETOOTH\_ADMIN | 正常 | 蓝牙管理 | 允许应用程序发现和配对蓝牙设备。  |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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 |
| com.google.android.c2dm.permission.RECEIVE | 合法 | C2DM 权限 | 云到设备消息传递的权限 |
| 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.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.tokenbuff.wallet.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| com.tokenbuff.wallet.permission.PUSH\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| com.huawei.appmarket.service.commondata.permission.GET\_COMMON\_DATA | 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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| com.meizu.flyme.permission.PUSH | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |
| com.meizu.flyme.push.permission.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.tokenbuff.wallet.push.permission.MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.coloros.mcs.permission.RECIEVE\_MCS\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.heytap.mcs.permission.RECIEVE\_MCS\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.push.permission.UPSTAGESERVICE | 未知 | Unknown permission | Unknown permission from android reference |
| com.hihonor.android.launcher.permission.CHANGE\_BADGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BLUETOOTH\_CONNECT | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_AUDIO | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.USE\_FINGERPRINT | 正常 | allow use of指纹 | 该常量在 API 级别 28 中已被弃用。应用程序应改为请求 USE\_BIOMETRIC |
| com.tokenbuff.wallet.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| com.hihonor.push.permission.READ\_PUSH\_NOTIFICATION\_INFO | 未知 | Unknown permission | Unknown permission from android reference |
| com.tokenbuff.wallet.permission.MIPUSH\_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.meizu.c2dm.permission.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.tokenbuff.wallet.permission.C2D\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.facebook.CustomTabActivity | **Schemes**: @string/fb\_login\_protocol\_scheme://,  |

**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。**