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

**Tixcash Institutional Wallet（ 5.0.0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 | Tixcash Institutional Wallet |
| 版本 | 5.0.0 |
| 包名 | com.wallet.institutionalwallet |
| 域名线索 | 64条 |
| URL线索 | 29条 |
| APP图标 |  |
| 分析日期 | 2025年5月22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 | app-release.apk |
| 文件大小 | 184.38MB |
| MD5值 | afa04f60e58a9b0c73fac18444f41561 |
| SHA1值 | 68ca5fe0a0d9d00ba0f51c2835666c279004e4af |
| SHA256值 | fb7b55940b17f3cd96b6d9e6ef2ad61e713fc4552c8678c4c2356936f0802049 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | Tixcash Institutional Wallet |
| 包名 | com.wallet.institutionalwallet |
| 主活动Activity | com.wallet.institutionalwallet.MainActivity |
| 安卓版本名称 | 5.0.0 |
| 安卓版本 | 5 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| tixcash.org | IP: 172.66.43.164 所属国家: United States of America 地区: California 城市: San Francisco  |
| ns.adobe.com | 没有服务器地理信息.  |
| staking.tixcash.org | IP: 172.66.40.92 所属国家: United States of America 地区: California 城市: San Francisco  |
| stakingapi.tixcash.org | IP: 172.66.43.164 所属国家: United States of America 地区: California 城市: San Francisco  |
| default.url | 没有服务器地理信息.  |
| bscscan.com | IP: 104.26.13.158 所属国家: United States of America 地区: California 城市: San Francisco  |
| developer.mozilla.org | IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| play.google.com | IP: 93.46.8.90 所属国家: Italy 地区: Lombardia 城市: Milan  |
| upload.wikimedia.org | IP: 103.102.166.240 所属国家: United States of America 地区: Indiana 城市: Francisco  |
| legacy.tixcash.org | IP: 172.66.40.92 所属国家: United States of America 地区: California 城市: San Francisco  |
| purl.org | IP: 207.241.225.157 所属国家: United States of America 地区: California 城市: San Francisco  |
| etherscan.io | IP: 128.242.245.212 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| fcm.googleapis.com | IP: 216.239.38.57 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| miningpool.tixcash.org | IP: 172.66.43.164 所属国家: United States of America 地区: California 城市: San Francisco  |
| redenvelope.tixcash.org | IP: 172.66.43.164 所属国家: United States of America 地区: California 城市: San Francisco  |
| curve.fi | IP: 108.160.170.33 所属国家: United States of America 地区: California 城市: San Francisco  |
| icons.veryicon.com | IP: 172.67.165.22 所属国家: United States of America 地区: California 城市: San Francisco  |
| schemas.microsoft.com | IP: 13.107.246.73 所属国家: United States of America 地区: Washington 城市: Redmond  |
| donate.tixcash.org | IP: 172.66.40.92 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.youtube.com | IP: 31.13.112.9 所属国家: Ireland 地区: Dublin 城市: Dublin  |
| developer.apple.com | IP: 17.253.85.203 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| xrpscan.com | IP: 104.21.5.97 所属国家: United States of America 地区: California 城市: San Francisco  |
| api.polygonscan.com | IP: 199.167.149.50 所属国家: United States of America 地区: Florida 城市: Tampa  |
| yearn.fi | IP: 76.76.21.21 所属国家: United States of America 地区: California 城市: Walnut  |
| cdn0.iconfinder.com | IP: 172.66.41.45 所属国家: United States of America 地区: California 城市: San Francisco  |
| pancakeswap.finance | IP: 108.160.170.33 所属国家: United States of America 地区: California 城市: San Francisco  |
| in.tradingview.com | IP: 157.240.17.14 所属国家: Switzerland 地区: Zurich 城市: Zurich  |
| streams.videolan.org | IP: 213.36.253.119 所属国家: France 地区: Ile-de-France 城市: Paris  |
| explorer.tixcash.org | IP: 172.66.40.92 所属国家: United States of America 地区: California 城市: San Francisco  |
| api.currencyapi.com | IP: 104.21.9.50 所属国家: United States of America 地区: California 城市: San Francisco  |
| solscan.io | IP: 172.67.43.41 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.jsdelivr.com | IP: 104.21.23.24 所属国家: United States of America 地区: California 城市: San Francisco  |
| btcscan.org | IP: 172.67.170.115 所属国家: United States of America 地区: California 城市: San Francisco  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| dartbug.com | IP: 216.239.34.21 所属国家: United States of America 地区: California 城市: Mountain View  |
| app.uniswap.org | IP: 202.160.130.52 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| developer.android.com | IP: 142.251.33.78 所属国家: Canada 地区: Ontario 城市: Toronto  |
| www.unicode.org | IP: 64.182.27.164 所属国家: United States of America 地区: Texas 城市: Dallas  |
| health.tixcash.org | IP: 172.66.43.164 所属国家: United States of America 地区: California 城市: San Francisco  |
| polygonscan.com | IP: 172.67.71.154 所属国家: United States of America 地区: California 城市: San Francisco  |
| vote.tixcash.org | IP: 172.66.40.92 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.sushi.com | IP: 76.76.21.164 所属国家: United States of America 地区: California 城市: Walnut  |
| coinmarketcap.com | IP: 69.63.178.13 所属国家: United States of America 地区: Utah 城市: Salt Lake City  |
| api.coingecko.com | IP: 199.193.116.105 所属国家: United States of America 地区: Florida 城市: Tampa  |
| api.bscscan.com | IP: 23.92.68.154 所属国家: United States of America 地区: Florida 城市: Tampa  |
| x.com | IP: 104.244.42.1 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.google.com | IP: 31.13.73.9 所属国家: Ireland 地区: Dublin 城市: Dublin  |
| flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| aomedia.org | IP: 202.160.130.117 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| www.tixcash.org | IP: 172.66.40.92 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.example.com | IP: 93.184.215.14 所属国家: United States of America 地区: California 城市: Los Angeles  |
| tyv.community | 没有服务器地理信息.  |
| app.1inch.io | IP: 128.242.240.91 所属国家: United States of America 地区: Washington 城市: Redmond  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| dashif.org | IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| www.tensorflow.org | IP: 142.251.211.238 所属国家: United States of America 地区: California 城市: Mountain View  |
| cdn-icons-png.flaticon.com | IP: 23.41.187.35 所属国家: Italy 地区: Lombardia 城市: Milan  |
| api.flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| pagead2.googlesyndication.com | IP: 114.250.70.38 所属国家: China 地区: Beijing 城市: Beijing  |
| fonts.gstatic.com | IP: 203.208.50.162 所属国家: China 地区: Beijing 城市: Beijing  |
| android.googlesource.com | IP: 74.125.135.82 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  |
| www.ffmpeg.org | IP: 79.124.17.100 所属国家: Bulgaria 地区: Sofia (stolitsa) 城市: Sofia  |
| www.facebook.com | IP: 108.160.172.1 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://www.example.com  | com/pichillilorenzo/flutter\_inappwebview\_android/chrome\_custom\_tabs/CustomTabsHelper.java  |
| https://developer.android.com/guide/topics/media/issues/cleartext-not-permitted  | f5/x.java  |
| https://developer.android.com/guide/topics/permissions/overview  | io/flutter/plugin/platform/g.java  |
| https://developer.android.com/guide/topics/media/issues/player-accessed-on-wrong-thread  | j3/y0.java  |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense  | n3/i0.java  |
| https://x</LA\_URL>  | n3/h0.java  |
| https://default.url  | n3/h0.java  |
| http://dashif.org/guidelines/last-segment-number  | p4/d.java  |
| http://dashif.org/guidelines/trickmode  | p4/d.java  |
| http://dashif.org/thumbnail\_tile  | p4/d.java  |
| http://dashif.org/guidelines/thumbnail\_tile  | p4/d.java  |
| https://github.com/Baseflow/flutter-permission-handler/issues  | u1/q.java  |
| https://github.com/bluefireteam/audioplayers/blob/main/troubleshooting.md  | td/d.java  |
| https://pagead2.googlesyndication.com/pagead/gen\_204?id=gmob-apps  | j5/b.java  |
| http://ns.adobe.com/xap/1.0/  | t3/a.java  |
| https://aomedia.org/emsg/ID3  | d4/a.java  |
| https://developer.apple.com/streaming/emsg-id3  | d4/a.java  |
| https://github.com/bluefireteam/audioplayers/blob/main/troubleshooting.md  | ud/o.java  |
| 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  |
| https://tyv.community  | lib/arm64-v8a/libapp.so  |
| https://www.tensorflow.org/lite/guide/ops\_select  | lib/arm64-v8a/libbarhopper\_v3.so  |
| http://http  | lib/arm64-v8a/libbarhopper\_v3.so  |
| https://www.tensorflow.org/lite/guide/ops\_custom  | lib/arm64-v8a/libbarhopper\_v3.so  |
| http://www.ffmpeg.org/schema/ffprobe  | lib/arm64-v8a/libffmpegkit.so  |
| https://streams.videolan.org/upload/  | lib/arm64-v8a/libffmpegkit.so  |
| https://android.googlesource.com/toolchain/llvm-project  | lib/arm64-v8a/libffmpegkit.so  |
| http://www.unicode.org/copyright.html  | 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://health.tixcash.org/api/account/uploadfile  | lib/armeabi-v7a/libapp.so  |
| https://stakingapi.tixcash.org/api/account/GetHolderList  | lib/armeabi-v7a/libapp.so  |
| https://stakingapi.tixcash.org/api/account/FundTransferaccount  | lib/armeabi-v7a/libapp.so  |
| https://redenvelope.tixcash.org/api/account/createredenvelopereward  | lib/armeabi-v7a/libapp.so  |
| https://github.com/DavBfr/dart\_pdf  | lib/armeabi-v7a/libapp.so  |
| https://etherscan.io/tx/  | lib/armeabi-v7a/libapp.so  |
| https://redenvelope.tixcash.org/api/account/getredenvelopepackagelist  | lib/armeabi-v7a/libapp.so  |
| https://stakingapi.tixcash.org/api/account/getnetwork  | lib/armeabi-v7a/libapp.so  |
| https://redenvelope.tixcash.org/api/account/claimredenvelopereward  | lib/armeabi-v7a/libapp.so  |
| https://legacy.tixcash.org/api/User/renewalpackage  | lib/armeabi-v7a/libapp.so  |
| https://stakingapi.tixcash.org/api/account/getmarketstatic  | lib/armeabi-v7a/libapp.so  |
| https://staking.tixcash.org/api/account/getservicenamebycountry/China  | lib/armeabi-v7a/libapp.so  |
| https://health.tixcash.org/api/account/uploaduser  | lib/armeabi-v7a/libapp.so  |
| https://stakingapi.tixcash.org  | lib/armeabi-v7a/libapp.so  |
| http://ns.adobe.com/xfdf/  | lib/armeabi-v7a/libapp.so  |
| https://stakingapi.tixcash.org/api/account/getactivestakinglist  | lib/armeabi-v7a/libapp.so  |
| https://cdn-icons-png.flaticon.com/512/25/25231.png  | lib/armeabi-v7a/libapp.so  |
| https://stakingapi.tixcash.org/api/account/UpdateBackupPharse  | lib/armeabi-v7a/libapp.so  |
| http://purl.org/dc/elements/1.1/  | lib/armeabi-v7a/libapp.so  |
| https://stakingapi.tixcash.org/api/account/Swap  | lib/armeabi-v7a/libapp.so  |
| https://stakingapi.tixcash.org/api/account/getuniverslanotification  | lib/armeabi-v7a/libapp.so  |
| https://github.com/dart-lang/language/issues/3488  | lib/armeabi-v7a/libapp.so  |
| https://donate.tixcash.org/api  | lib/armeabi-v7a/libapp.so  |
| https://upload.wikimedia.org/wikipedia/commons/5/57/X\_logo\_2023\_%28white%29.png  | lib/armeabi-v7a/libapp.so  |
| https://yearn.fi/vaults  | lib/armeabi-v7a/libapp.so  |
| https://staking.tixcash.org/api  | lib/armeabi-v7a/libapp.so  |
| https://legacy.tixcash.org/api/User/uploadidfile  | lib/armeabi-v7a/libapp.so  |
| https://bscscan.com/tx/  | lib/armeabi-v7a/libapp.so  |
| https://polygonscan.com/tx/  | lib/armeabi-v7a/libapp.so  |
| https://curve.fi/  | lib/armeabi-v7a/libapp.so  |
| https://explorer.tixcash.org/Transaction/  | lib/armeabi-v7a/libapp.so  |
| https://api.currencyapi.com/v3/latest?apikey=cur\_live\_lo2iAXWa8VwcQFwXWI0IfgX7LeTSsCGtoeWGjxmp  | lib/armeabi-v7a/libapp.so  |
| https://cdn0.iconfinder.com/data/icons/most-usable-logos/150/you\_Tube-512.png  | lib/armeabi-v7a/libapp.so  |
| https://www.google.com  | lib/armeabi-v7a/libapp.so  |
| https://donate.tixcash.org/api/account/getactivedonation  | lib/armeabi-v7a/libapp.so  |
| https://solscan.io/tx/  | lib/armeabi-v7a/libapp.so  |
| https://api.coingecko.com/api/v3/simple/price?ids=okb&vs\_currencies=usd  | lib/armeabi-v7a/libapp.so  |
| https://stakingapi.tixcash.org/api/account/createmultipleaccount  | lib/armeabi-v7a/libapp.so  |
| https://stakingapi.tixcash.org/api/account/addcurrency  | lib/armeabi-v7a/libapp.so  |
| https://staking.tixcash.org/api/account/renewalpackage  | lib/armeabi-v7a/libapp.so  |
| https://api.flutter.dev/flutter/material/Scaffold/of.html  | lib/armeabi-v7a/libapp.so  |
| https://fcm.googleapis.com/fcm/send  | lib/armeabi-v7a/libapp.so  |
| https://stakingapi.tixcash.org/api/account/getAppVersion  | lib/armeabi-v7a/libapp.so  |
| https://redenvelope.tixcash.org/api/account/activateredenvelope  | lib/armeabi-v7a/libapp.so  |
| https://app.uniswap.org  | lib/armeabi-v7a/libapp.so  |
| https://api.polygonscan.com/api  | lib/armeabi-v7a/libapp.so  |
| https://icons.veryicon.com/png/o/miscellaneous/my-icons/my-referral.png  | lib/armeabi-v7a/libapp.so  |
| https://docs.flutter.dev/development/data-and-backend/networking  | lib/armeabi-v7a/libapp.so  |
| https://donate.tixcash.org/api/account/sendamount  | lib/armeabi-v7a/libapp.so  |
| https://play.google.com/store/apps/details?id=com.wallet.line  | lib/armeabi-v7a/libapp.so  |
| https://stakingapi.tixcash.org/api/account/stakpackage  | lib/armeabi-v7a/libapp.so  |
| https://cdn-icons-png.flaticon.com/512/1829/1829589.png  | lib/armeabi-v7a/libapp.so  |
| https://stakingapi.tixcash.org/api/account/createwalletaccount  | lib/armeabi-v7a/libapp.so  |
| https://github.com/flutter/flutter/issues/new.  | lib/armeabi-v7a/libapp.so  |
| https://health.tixcash.org/api/account/updatestepdata  | lib/armeabi-v7a/libapp.so  |
| https://cdn-icons-png.flaticon.com/512/3616/3616929.png  | lib/armeabi-v7a/libapp.so  |
| https://tyv.community  | lib/armeabi-v7a/libapp.so  |
| https://tixcash.org  | lib/armeabi-v7a/libapp.so  |
| https://stakingapi.tixcash.org/api  | lib/armeabi-v7a/libapp.so  |
| https://health.tixcash.org/api  | lib/armeabi-v7a/libapp.so  |
| https://in.tradingview.com/markets/cryptocurrencies/prices-all/  | lib/armeabi-v7a/libapp.so  |
| https://miningpool.tixcash.org/api/account/uploadform  | lib/armeabi-v7a/libapp.so  |
| https://staking.tixcash.org/api/account/getpackagelist  | lib/armeabi-v7a/libapp.so  |
| https://pancakeswap.finance  | lib/armeabi-v7a/libapp.so  |
| https://legacy.tixcash.org/api/User/buywhitelistpackage  | lib/armeabi-v7a/libapp.so  |
| https://www.youtube.com/  | lib/armeabi-v7a/libapp.so  |
| https://miningpool.tixcash.org/api/account/updateserver  | lib/armeabi-v7a/libapp.so  |
| https://miningpool.tixcash.org/api/account/getpackagemonth  | lib/armeabi-v7a/libapp.so  |
| https://health.tixcash.org/api/account/allsonglist  | lib/armeabi-v7a/libapp.so  |
| https://www.tixcash.org/  | lib/armeabi-v7a/libapp.so  |
| https://stakingapi.tixcash.org/api/account/buypackage  | lib/armeabi-v7a/libapp.so  |
| https://developer.mozilla.org/en-US/docs/Web/HTTP/Status  | lib/armeabi-v7a/libapp.so  |
| https://tixcash.org/apk/app-release.apk  | lib/armeabi-v7a/libapp.so  |
| https://coinmarketcap.com/  | lib/armeabi-v7a/libapp.so  |
| https://health.tixcash.org/api/account/updatetarget  | lib/armeabi-v7a/libapp.so  |
| https://github.com/Tixcoin  | lib/armeabi-v7a/libapp.so  |
| https://www.sushi.com/swap  | lib/armeabi-v7a/libapp.so  |
| https://vote.tixcash.org/api/account/uservote  | lib/armeabi-v7a/libapp.so  |
| https://stakingapi.tixcash.org/api/account/getpackagelist  | lib/armeabi-v7a/libapp.so  |
| https://stakingapi.tixcash.org/api/account/DepositFund  | lib/armeabi-v7a/libapp.so  |
| https://legacy.tixcash.org/api/User/getpackagelist  | lib/armeabi-v7a/libapp.so  |
| https://miningpool.tixcash.org/api/account/uploadfile  | lib/armeabi-v7a/libapp.so  |
| https://stakingapi.tixcash.org/api/account/renewalpackage  | lib/armeabi-v7a/libapp.so  |
| https://staking.tixcash.org/api/account/applystake  | lib/armeabi-v7a/libapp.so  |
| https://api.bscscan.com/api  | lib/armeabi-v7a/libapp.so  |
| https://stakingapi.tixcash.org/api/account/MarketListuser  | lib/armeabi-v7a/libapp.so  |
| https://staking.tixcash.org/api/account/whitelistapplystake  | lib/armeabi-v7a/libapp.so  |
| https://www.facebook.com/tixcashtxh  | lib/armeabi-v7a/libapp.so  |
| https://health.tixcash.org/api/account/updateuserbanner  | lib/armeabi-v7a/libapp.so  |
| https://stakingapi.tixcash.org/api/account/GetAllTransactionList  | lib/armeabi-v7a/libapp.so  |
| https://stakingapi.tixcash.org/api/account/claimstakingreward  | lib/armeabi-v7a/libapp.so  |
| https://legacy.tixcash.org/api  | lib/armeabi-v7a/libapp.so  |
| https://health.tixcash.org/Documents/  | lib/armeabi-v7a/libapp.so  |
| https://x.com/tixcash?s=09  | lib/armeabi-v7a/libapp.so  |
| https://redenvelope.tixcash.org/api  | lib/armeabi-v7a/libapp.so  |
| https://btcscan.org/tx/  | lib/armeabi-v7a/libapp.so  |
| https://miningpool.tixcash.org/api/account/renewalpremiumpackage  | lib/armeabi-v7a/libapp.so  |
| https://miningpool.tixcash.org/api  | lib/armeabi-v7a/libapp.so  |
| https://github.com/material-foundation/flutter-packages/blob/main/packages/google\_fonts/example/test  | lib/armeabi-v7a/libapp.so  |
| https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android.  | lib/armeabi-v7a/libapp.so  |
| https://staking.tixcash.org/api/account/buywhitelistpackage  | lib/armeabi-v7a/libapp.so  |
| https://legacy.tixcash.org/api/User/whitelistapplystake  | lib/armeabi-v7a/libapp.so  |
| https://fonts.gstatic.com/s/a/  | lib/armeabi-v7a/libapp.so  |
| https://app.1inch.io/  | lib/armeabi-v7a/libapp.so  |
| https://xrpscan.com/tx/  | lib/armeabi-v7a/libapp.so  |
| https://www.tensorflow.org/lite/guide/ops\_select  | lib/armeabi-v7a/libbarhopper\_v3.so  |
| http://http  | lib/armeabi-v7a/libbarhopper\_v3.so  |
| https://www.tensorflow.org/lite/guide/ops\_custom  | lib/armeabi-v7a/libbarhopper\_v3.so  |
| http://www.ffmpeg.org/schema/ffprobe  | lib/armeabi-v7a/libffmpegkit\_armv7a\_neon.so  |
| https://streams.videolan.org/upload/  | lib/armeabi-v7a/libffmpegkit\_armv7a\_neon.so  |
| https://android.googlesource.com/toolchain/llvm-project  | lib/armeabi-v7a/libffmpegkit\_armv7a\_neon.so  |
| http://www.unicode.org/copyright.html  | lib/armeabi-v7a/libflutter.so  |
| https://github.com/flutter/flutter/issues.  | lib/armeabi-v7a/libflutter.so  |
| https://dartbug.com/52121.  | lib/armeabi-v7a/libflutter.so  |
| https://www.tensorflow.org/lite/guide/ops\_select  | lib/x86/libbarhopper\_v3.so  |
| http://http  | lib/x86/libbarhopper\_v3.so  |
| https://www.tensorflow.org/lite/guide/ops\_custom  | lib/x86/libbarhopper\_v3.so  |
| http://www.ffmpeg.org/schema/ffprobe  | lib/x86/libffmpegkit.so  |
| https://streams.videolan.org/upload/  | lib/x86/libffmpegkit.so  |
| https://android.googlesource.com/toolchain/llvm-project  | lib/x86/libffmpegkit.so  |
| https://tyv.community  | lib/x86\_64/libapp.so  |
| https://www.tensorflow.org/lite/guide/ops\_select  | lib/x86\_64/libbarhopper\_v3.so  |
| http://http  | lib/x86\_64/libbarhopper\_v3.so  |
| https://www.tensorflow.org/lite/guide/ops\_custom  | lib/x86\_64/libbarhopper\_v3.so  |
| http://www.ffmpeg.org/schema/ffprobe  | lib/x86\_64/libffmpegkit.so  |
| https://streams.videolan.org/upload/  | lib/x86\_64/libffmpegkit.so  |
| https://android.googlesource.com/toolchain/llvm-project  | lib/x86\_64/libffmpegkit.so  |
| http://www.unicode.org/copyright.html  | lib/x86\_64/libflutter.so  |
| https://github.com/flutter/flutter/issues.  | lib/x86\_64/libflutter.so  |
| https://dartbug.com/52121.  | lib/x86\_64/libflutter.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| u0013android@android.com0 u0013android@android.com  | n5/u.java  |
| pac@2x.png 0xbtc@2x.png 2give@2x.png aave@2x.png abt@2x.png act@2x.png actn@2x.png ada@2x.png add@2x.png adx@2x.png ae@2x.png aeon@2x.png aeur@2x.png agi@2x.png agrs@2x.png aion@2x.png algo@2x.png amb@2x.png amp@2x.png ampl@2x.png ankr@2x.png ant@2x.png apex@2x.png appc@2x.png ardr@2x.png arg@2x.png ark@2x.png arn@2x.png arnx@2x.png ary@2x.png ast@2x.png atm@2x.png atom@2x.png audr@2x.png auto@2x.png aywa@2x.png bab@2x.png bal@2x.png band@2x.png bat@2x.png bay@2x.png bcbc@2x.png bcc@2x.png bcd@2x.png bch@2x.png bcio@2x.png bcn@2x.png bco@2x.png bcpt@2x.png bdl@2x.png beam@2x.png bela@2x.png bix@2x.png blcn@2x.png blk@2x.png block@2x.png blz@2x.png bnb@2x.png bnt@2x.png bnty@2x.png booty@2x.png bos@2x.png bpt@2x.png bq@2x.png brd@2x.png bsd@2x.png bsv@2x.png btc@2x.png btcd@2x.png btch@2x.png btcp@2x.png btcz@2x.png btdx@2x.png btg@2x.png btm@2x.png bts@2x.png btt@2x.png btx@2x.png burst@2x.png bze@2x.png call@2x.png cc@2x.png cdn@2x.png cdt@2x.png cenz@2x.png chain@2x.png chat@2x.png chips@2x.png chsb@2x.png cix@2x.png clam@2x.png cloak@2x.png cmm@2x.png cmt@2x.png cnd@2x.png cnx@2x.png cny@2x.png cob@2x.png coinxplus@2x.png colx@2x.png comp@2x.png coqui@2x.png cred@2x.png crpt@2x.png crv@2x.png crw@2x.png cs@2x.png ctr@2x.png ctxc@2x.png cvc@2x.png d@2x.png dai@2x.png dash@2x.png dat@2x.png data@2x.png dbc@2x.png dcn@2x.png dcr@2x.png deez@2x.png dent@2x.png dew@2x.png dgb@2x.png dgd@2x.png dlt@2x.png dnt@2x.png dock@2x.png doge@2x.png dot@2x.png drgn@2x.png drop@2x.png dta@2x.png dth@2x.png dtr@2x.png ebst@2x.png eca@2x.png edg@2x.png edo@2x.png edoge@2x.png ela@2x.png elec@2x.png elf@2x.png elix@2x.png ella@2x.png emb@2x.png emc2@2x.png emc@2x.png eng@2x.png enj@2x.png entrp@2x.png eon@2x.png eop@2x.png eos@2x.png eql@2x.png equa@2x.png etc@2x.png eth@2x.png ethos@2x.png etn@2x.png etp@2x.png eur@2x.png evx@2x.png exmo@2x.png exp@2x.png fair@2x.png fct@2x.png fil@2x.png fjc@2x.png fldc@2x.png flo@2x.png flux@2x.png fsn@2x.png ftc@2x.png fuel@2x.png fun@2x.png game@2x.png gas@2x.png gbp@2x.png gbx@2x.png gbyte@2x.png generic@2x.png gin@2x.png glxt@2x.png gmr@2x.png gno@2x.png gnt@2x.png gold@2x.png grc@2x.png grin@2x.png grs@2x.png grt@2x.png gsc@2x.png gto@2x.png gup@2x.png gusd@2x.png gvt@2x.png gxs@2x.png gzr@2x.png hight@2x.png hns@2x.png hodl@2x.png hot@2x.png hpb@2x.png hsr@2x.png ht@2x.png html@2x.png huc@2x.png husd@2x.png hush@2x.png icn@2x.png icp@2x.png icx@2x.png ignis@2x.png ilk@2x.png ink@2x.png ins@2x.png ion@2x.png iop@2x.png iost@2x.png iotx@2x.png iq@2x.png itc@2x.png jnt@2x.png jpy@2x.png kcs@2x.png kin@2x.png klown@2x.png kmd@2x.png knc@2x.png krb@2x.png ksm@2x.png lbc@2x.png lend@2x.png leo@2x.png link@2x.png lkk@2x.png loom@2x.png lpt@2x.png lrc@2x.png lsk@2x.png ltc@2x.png lun@2x.png maid@2x.png mana@2x.png matic@2x.png max@2x.png mcap@2x.png mco@2x.png mda@2x.png mds@2x.png med@2x.png meetone@2x.png mft@2x.png miota@2x.png mith@2x.png mkr@2x.png mln@2x.png mnx@2x.png mnz@2x.png moac@2x.png mod@2x.png mona@2x.png msr@2x.png mth@2x.png mtl@2x.png music@2x.png mzc@2x.png nano@2x.png nas@2x.png nav@2x.png ncash@2x.png ndz@2x.png nebl@2x.png neo@2x.png neos@2x.png neu@2x.png nexo@2x.png ngc@2x.png nio@2x.png nkn@2x.png nlc2@2x.png nlg@2x.png nmc@2x.png nmr@2x.png npxs@2x.png ntbc@2x.png nuls@2x.png nxs@2x.png nxt@2x.png oax@2x.png ok@2x.png omg@2x.png omni@2x.png one@2x.png ong@2x.png ont@2x.png oot@2x.png ost@2x.png ox@2x.png oxt@2x.png part@2x.png pasc@2x.png pasl@2x.png pax@2x.png paxg@2x.png pay@2x.png payx@2x.png pink@2x.png pirl@2x.png pivx@2x.png plr@2x.png poa@2x.png poe@2x.png polis@2x.png poly@2x.png pot@2x.png powr@2x.png ppc@2x.png ppp@2x.png ppt@2x.png pre@2x.png prl@2x.png pungo@2x.png pura@2x.png qash@2x.png qiwi@2x.png qlc@2x.png qrl@2x.png qsp@2x.png qtum@2x.png r@2x.png rads@2x.png rap@2x.png rcn@2x.png rdd@2x.png rdn@2x.png ren@2x.png rep@2x.png repv2@2x.png req@2x.png rhoc@2x.png ric@2x.png rise@2x.png rlc@2x.png rpx@2x.png rub@2x.png rvn@2x.png ryo@2x.png safe@2x.png safemoon@2x.png sai@2x.png salt@2x.png san@2x.png sand@2x.png sbd@2x.png sberbank@2x.png sc@2x.png shift@2x.png sib@2x.png sin@2x.png skl@2x.png sky@2x.png slr@2x.png sls@2x.png smart@2x.png sngls@2x.png snm@2x.png snt@2x.png snx@2x.png soc@2x.png sol@2x.png spacehbit@2x.png spank@2x.png sphtx@2x.png srn@2x.png stak@2x.png start@2x.png steem@2x.png storj@2x.png storm@2x.png stox@2x.png stq@2x.png strat@2x.png stx@2x.png sub@2x.png sumo@2x.png sushi@2x.png sys@2x.png taas@2x.png tau@2x.png tbx@2x.png tdc@2x.png tel@2x.png ten@2x.png tern@2x.png tgch@2x.png theta@2x.png tix@2x.png tkn@2x.png tks@2x.png tnb@2x.png tnc@2x.png tnt@2x.png tomo@2x.png tpay@2x.png trig@2x.png tron@2x.png trtl@2x.png trx@2x.png tusd@2x.png tzc@2x.png ubq@2x.png uma@2x.png uni@2x.png unity@2x.png usd@2x.png usdc@2x.png usdt@2x.png utk@2x.png veri@2x.png vet@2x.png via@2x.png vib@2x.png vibe@2x.png vivo@2x.png vrc@2x.png vrsc@2x.png vtc@2x.png vtho@2x.png wabi@2x.png wan@2x.png waves@2x.png wax@2x.png wbtc@2x.png wgr@2x.png wicc@2x.png wings@2x.png wpr@2x.png wtc@2x.png x@2x.png xas@2x.png xbc@2x.png xbp@2x.png xby@2x.png xcp@2x.png xdn@2x.png xem@2x.png xin@2x.png xlm@2x.png xmcc@2x.png xmg@2x.png xmo@2x.png xmr@2x.png xmy@2x.png xp@2x.png xpa@2x.png xpm@2x.png xpr@2x.png xrp@2x.png xsg@2x.png xtz@2x.png xuc@2x.png xvc@2x.png xvg@2x.png xzc@2x.png yfi@2x.png yoyow@2x.png zcl@2x.png zec@2x.png zel@2x.png zen@2x.png zest@2x.png zil@2x.png zilla@2x.png zrx@2x.png  | 摸瓜V2引擎  |
| android-sdk-releaser@vopo7.prod  | lib/arm64-v8a/libbarhopper\_v3.so  |
| ffmpeg-devel@ffmpeg.org  | lib/arm64-v8a/libffmpegkit.so  |
| appro@openssl.org  | lib/arm64-v8a/libflutter.so  |
| \_httpparser@13463476.responsepa \_future@4048458.immediate \_growablelist@0150898.\_literal \_link@14069316.fromrawpat \_growablelist@0150898.withcapaci \_receiveportimpl@1026248.fromrawrec \_growablelist@0150898.\_literal2 \_bigintimpl@0150898.from \_list@0150898.empty reliwellpvtltd@gmail.com \_hashcollisionnode@40137193.fromcollis \_colorfilter@15065589.lineartosr \_growablelist@0150898.\_literal4 \_growablelist@0150898.of \_list@0150898.of \_uri@0150898.http \_list@0150898.generate \_typeerror@0150898.\_create \_list@0150898.\_ofgrowabl \_list@0150898.\_ofefficie \_growablelist@0150898.\_ofarray \_socket@14069316.\_readpipe \_list@0150898.\_ofother \_compressednode@40137193.single \_bytebuffer@7027147.\_new txh@2x.png \_nativesocket@14069316.normal \_filestream@14069316.forstdin \_colorfilter@15065589.srgbtoline line@2x.png \_pointerpanzoomdata@404213599.fromupdate \_growablelist@0150898.\_literal8 \_future@4048458.zonevalue \_double@0150898.fromintege \_growablelist@0150898.\_literal6 \_colorfilter@15065589.mode \_imagefilter@15065589.composed \_list@0150898.\_ofarray \_timer@1026248.periodic \_invocationmirror@0150898.\_withtype \_assetmanifestbin@48287047.fromstanda \_growablelist@0150898.\_literal1 \_uri@0150898.file \_imagefilter@15065589.blur \_growablelist@0150898.\_ofgrowabl \_nativesocket@14069316.pipe authenticationscheme@13463476.fromstring \_growablelist@0150898.\_literal3 \_growablelist@0150898.\_ofother \_timer@1026248.\_internal \_growablelist@0150898.\_literal5 \_rawsocket@14069316.\_readpipe ngstreamsubscription@4048458.zoned \_assertionerror@0150898.\_create \_imagefilter@15065589.fromcolorf \_uri@0150898.directory \_file@14069316.fromrawpat \_growablelist@0150898.generate \_uri@0150898.notsimple \_growablelist@0150898.\_literal7 \_growablelist@0150898.\_ofefficie \_future@4048458.immediatee  | lib/armeabi-v7a/libapp.so  |
| android-sdk-releaser@vopo7.prod  | lib/armeabi-v7a/libbarhopper\_v3.so  |
| ffmpeg-devel@ffmpeg.org  | lib/armeabi-v7a/libffmpegkit\_armv7a\_neon.so  |
| android-sdk-releaser@vopo7.prod  | lib/x86/libbarhopper\_v3.so  |
| ffmpeg-devel@ffmpeg.org  | lib/x86/libffmpegkit.so  |
| 6h@fo.lwft w9oi\_2nhels4u@dlilycclglhl.5jlcg\_bqh yay@y.u5vcghyy  | lib/x86\_64/libavcodec.so  |
| 6h@fo.lwft w9oi\_2nhels4u@dlilycclglhl.5jlcg\_bqh yay@y.u5vcghyy  | lib/x86\_64/libavformat.so  |
| android-sdk-releaser@vopo7.prod  | lib/x86\_64/libbarhopper\_v3.so  |
| ffmpeg-devel@ffmpeg.org  | lib/x86\_64/libffmpegkit.so  |
| appro@openssl.org  | lib/x86\_64/libflutter.so  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17512775099  | o7/a.java  |
| 18222222222  | u3/e.java  |
| 15123456789  | lib/armeabi-v7a/libapp.so  |
| 13123456789  | lib/armeabi-v7a/libapp.so  |

## **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: CN=Android Debug, O=Android, C=US 签名算法: rsassa\_pkcs1v15 有效期自: 2023-11-03 15:23:20+00:00 有效期至: 2053-10-26 15:23:20+00:00 发行人: CN=Android Debug, O=Android, C=US 序列号: 0x1 哈希算法: sha1 md5值: 54d2140cfdad349ea7cc6745cb7c22fc sha1值: 7a4f165d5633d8fdd275a6b9195148f176da0f18 sha256值: 99c349fd2ed35507df5acb1e54a76dd76139c3bc215cb8297458922420ea56fa sha512值: 365d0356f3cfbc7d3de63f5c90e46e98a73be2a98aaa7568398a80a3c9b1e7fa2b8ba7f702b48344f235aede77b0676a70b41b757dce1afd7f859e62f052fd46 公钥算法: rsa 密钥长度: 2048 指纹: 5597ecc8719bf759167c871366f45d3b863a1a9ebb6fb8bf171d28043b6a7b8f**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "google\_api\_key" : "AIzaSyBVqK5kA2sdZ-6IPUq0Yhlh1gtm5BR-YOg"  |
| "google\_crash\_reporting\_api\_key" : "AIzaSyBVqK5kA2sdZ-6IPUq0Yhlh1gtm5BR-YOg"  |

## **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.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 |
| 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.GALLERY | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ACTIVITY\_RECOGNITION | 危险 | 允许应用程序识别身体活动 | 允许应用程序识别身体活动 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS | 正常 |  | 应用程序必须持有的权限才能使用 Settings.ACTION\_REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS。 |
| 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.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.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.ACCESS\_NOTIFICATION\_POLICY | 正常 |  | 希望访问通知策略的应用程序的标记权限。 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.USE\_EXACT\_ALARM | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FOREGROUND\_SERVICE\_MEDIA\_PLAYBACK | 未知 | Unknown permission | Unknown permission from android reference |
| 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.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| 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\_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.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\_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.USE\_FULL\_SCREEN\_INTENT | 正常 |  | 针对想要使用通知全屏意图的 Build.VERSION\_CODES.Q 的应用程序是必需的 |
| 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.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 |
| com.google.android.c2dm.permission.RECEIVE | 合法 | C2DM 权限 | 云到设备消息传递的权限 |
| com.google.android.gms.permission.AD\_ID | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ACCESS\_ADSERVICES\_ATTRIBUTION | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ACCESS\_ADSERVICES\_AD\_ID | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.finsky.permission.BIND\_GET\_INSTALL\_REFERRER\_SERVICE | 未知 | Unknown permission | Unknown permission from android reference |
| com.wallet.institutionalwallet.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |

## **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。**