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

**TokBuy（ 1.2.2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 | TokBuy |
| 版本 | 1.2.2 |
| 包名 | com.hykj.nhwj |
| 域名线索 | 27条 |
| URL线索 | 50条 |
| APP图标 |  |
| 分析日期 | 2025年6月5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 | TokBuy.apk |
| 文件大小 | 25.98MB |
| MD5值 | 5c14f2d01cbb2079767e33b9fee54a02 |
| SHA1值 | 80e06a8d21ec4396953b0c8aeedef43ff69d8db9 |
| SHA256值 | 641febdda3220f5af0cff5422a56b332a458a07e60b035209aff01c284b28672 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | TokBuy |
| 包名 | com.hykj.nhwj |
| 主活动Activity | com.hykj.nhwj.SpalshActivity |
| 安卓版本名称 | 1.2.2 |
| 安卓版本 | 23 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| web.sdk.qcloud.com | IP: 124.163.195.101 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| h5.silkswap.io | IP: 18.65.168.32 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| cloud.tencent.com | IP: 60.28.220.199 所属国家: China 地区: Tianjin 城市: Tianjin  |
| api.tokbuy.io | IP: 8.222.90.112 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| monitor.geetest.com | IP: 47.95.165.133 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| connect.tencentcloud.com | IP: 43.175.132.103 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| www.tencentcloud.com | IP: 43.175.93.11 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| static.geetest.com | IP: 202.108.29.158 所属国家: China 地区: Beijing 城市: Beijing  |
| 119.29.29.99 | IP: 119.29.29.99 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| im.sdk.qcloud.com | IP: 221.204.15.87 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| 162.14.19.114 | IP: 162.14.19.114 所属国家: China 地区: Beijing 城市: Beijing  |
| www.geetest.com | IP: 60.28.220.199 所属国家: China 地区: Tianjin 城市: Tianjin  |
| buy.cloud.tencent.com | IP: 123.125.244.81 所属国家: China 地区: Beijing 城市: Beijing  |
| xml.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| zhiliao.qq.com | IP: 221.204.15.89 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| 119.29.29.98 | IP: 119.29.29.98 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  |
| wwww.baidu.com | IP: 110.242.68.66 所属国家: China 地区: Hebei 城市: Baoding  |
| 162.14.13.170 | IP: 162.14.13.170 所属国家: China 地区: Beijing 城市: Beijing  |
| static.tokbuy.io | IP: 3.166.205.11 所属国家: United States of America 地区: Washington 城市: Seattle  |
| demos.trtc.tencent-cloud.com | IP: 116.136.188.184 所属国家: China 地区: Nei Mongol 城市: Hohhot  |
| 162.14.3.250 | IP: 162.14.3.250 所属国家: China 地区: Beijing 城市: Beijing  |
| h5.tokbuy.io | IP: 18.65.168.56 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| intl.cloud.tencent.com | IP: 60.28.220.199 所属国家: China 地区: Tianjin 城市: Tianjin  |
| privacy.qq.com | IP: 221.204.16.62 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| download.nanheshop.com | IP: 121.37.200.153 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| nh-fix.oss-accelerate.aliyuncs.com | IP: 39.107.134.114 所属国家: China 地区: Zhejiang 城市: Hangzhou  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://xml.apache.org/xslt  | com/blankj/utilcode/util/LogUtils.java  |
| https://monitor.geetest.com/monitor/send  | com/geetest/sdk/p0.java  |
| http://www.geetest.com/first\_page  | com/geetest/sdk/views/GT3GeetestButton.java  |
| https://static.geetest.com/static/appweb/app3-index.html  | com/geetest/sdk/dialog/views/a.java  |
| https://api.tokbuy.io  | com/hykj/nhwj/NhwjApplication.java  |
| https://wwww.baidu.com  | com/hykj/nhwj/SpalshActivity.java  |
| https://nh-fix.oss-accelerate.aliyuncs.com/fix/fix-prod.json  | com/hykj/nhwj/SpalshActivity.java  |
| https://api.tokbuy.io/file/attach/download?path=  | com/hykj/nhwj/constants/Urls.java  |
| https://h5.tokbuy.io/?inviteCode=  | com/hykj/nhwj/constants/Urls.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/avatar/avatar\_%s.png  | com/hykj/nhwj/im/Constants.java  |
| https://cloud.tencent.com/product/im  | com/hykj/nhwj/im/Constants.java  |
| https://privacy.qq.com/document/preview/c63a48325d0e4a35b93f675205a65a77  | com/hykj/nhwj/im/Constants.java  |
| https://privacy.qq.com/document/preview/1cfe904fb7004b8ab1193a55857f7272  | com/hykj/nhwj/im/Constants.java  |
| https://cloud.tencent.com/act/event/report-platform  | com/hykj/nhwj/im/Constants.java  |
| https://privacy.qq.com/document/preview/45ba982a1ce6493597a00f8c86b52a1e  | com/hykj/nhwj/im/Constants.java  |
| https://privacy.qq.com/document/preview/dea84ac4bb88454794928b77126e9246  | com/hykj/nhwj/im/Constants.java  |
| https://web.sdk.qcloud.com/document/Tencent-IM-User-Agreement.html  | com/hykj/nhwj/im/Constants.java  |
| https://connect.tencentcloud.com/web/im/chat/?webAppId=b793f9edaeae064560e9542b22833ec3&isFromUserGuide=true  | com/hykj/nhwj/ui/mine/HelpCenterActivity.java  |
| https://static.tokbuy.io/html/TokbuyRegistrationAgreement-Contract.html  | com/hykj/nhwj/ui/mine/AccountLogoutActivity.java  |
| https://static.tokbuy.io/html/TokbuyUserAgreement-Contract.html  | com/hykj/nhwj/ui/login/ReloginActivity.java  |
| https://static.tokbuy.io/html/TokbuyUserAgreement-Contract.html  | com/hykj/nhwj/ui/login/RegisterActivity.java  |
| https://download.nanheshop.com/  | com/hykj/nhwj/ui/ecology/EcologyFragment.java  |
| https://h5.silkswap.io/  | com/hykj/nhwj/ui/ecology/EcologyFragment.java  |
| https://github.com/kongzue/DialogX/wiki  | com/kongzue/dialogx/DialogX.java  |
| https://github.com/kongzue/DialogX  | com/kongzue/dialogx/interfaces/BaseDialog.java  |
| https://github.com/kongzue/DialogX  | com/kongzue/dialogx/impl/ActivityLifecycleImpl.java  |
| https://zhiliao.qq.com/  | com/tencent/qcloud/tuicore/TUIConstants.java  |
| https://cloud.tencent.com/document/product/269/32458  | com/tencent/qcloud/tuicore/TUIConstants.java  |
| https://intl.cloud.tencent.com/document/product/1047/36021?lang=en&pg=  | com/tencent/qcloud/tuicore/TUIConstants.java  |
| https://buy.cloud.tencent.com/avc?activeId=plugin&regionId=1  | com/tencent/qcloud/tuicore/TUIConstants.java  |
| https://cloud.tencent.com/document/product/269/11673?from=17219  | com/tencent/qcloud/tuicore/TUIConstants.java  |
| https://www.tencentcloud.com/document/product/1047/34349  | com/tencent/qcloud/tuicore/TUIConstants.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/conversation-backgroundImage/backgroundImage\_%s.png  | com/tencent/qcloud/tuicore/TUIConstants.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/conversation-backgroundImage/backgroundImage\_%s\_full.png  | com/tencent/qcloud/tuicore/TUIConstants.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/group-avatar/group\_avatar\_%s.png  | com/tencent/qcloud/tuicore/TUIConstants.java  |
| https://demos.trtc.tencent-cloud.com/prod/base/v1/events/stat  | com/tencent/qcloud/tuicore/TUIConfig.java  |
| https://cloud.tencent.com/document/product/269/32458  | com/tencent/qcloud/tuikit/tuichat/TUIChatConstants.java  |
| https://intl.cloud.tencent.com/document/product/1047/36021?lang=en&pg=  | com/tencent/qcloud/tuikit/tuichat/TUIChatConstants.java  |
| https://cloud.tencent.com/document/product/269/3794  | com/tencent/qcloud/tuikit/tuichat/bean/CustomHelloMessage.java  |
| https://cloud.tencent.com/product/im  | com/tencent/qcloud/tuikit/tuicontact/TUIContactConstants.java  |
| https://www.tencentcloud.com/products/im?lang=en&pg=  | com/tencent/qcloud/tuikit/tuicontact/TUIContactConstants.java  |
| https://cloud.tencent.com/product/im  | com/tencent/qcloud/tuikit/tuicontact/minimalistui/pages/GroupTypeSelectMinimalistActivity.java  |
| https://cloud.tencent.com/product/im  | com/tencent/qcloud/tuikit/tuicontact/minimalistui/pages/CreateGroupMinimalistActivity.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/group-avatar/group\_avatar\_%s.png  | com/tencent/qcloud/tuikit/tuicontact/minimalistui/pages/CreateGroupMinimalistActivity.java  |
| https://cloud.tencent.com/product/im  | com/tencent/qcloud/tuikit/tuicontact/classicui/pages/GroupTypeSelectActivity.java  |
| https://cloud.tencent.com/product/im  | com/tencent/qcloud/tuikit/tuicontact/classicui/pages/CreateGroupActivity.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/group-avatar/group\_avatar\_%s.png  | com/tencent/qcloud/tuikit/tuicontact/classicui/pages/CreateGroupActivity.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/group-avatar/group\_avatar\_%s.png  | com/tencent/qcloud/tuikit/tuigroup/TUIGroupConstants.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/group-avatar/group\_avatar\_%s.png  | com/tencent/qcloud/tuikit/tuigroup/classicui/page/GroupInfoFragment.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/group-avatar/group\_avatar\_%s.png  | com/tencent/qcloud/tuikit/tuigroup/minimalistui/page/GroupInfoMinimalistFragment.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/group-avatar/group\_avatar\_%s.png  | com/tencent/qcloud/tuikit/tuicommunity/ui/page/CreateCommunityActivity.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/group-avatar/group\_avatar\_%s.png  | com/tencent/qcloud/tuikit/tuicommunity/ui/page/CommunitySettingsActivity.java  |
| https://cloud.tencent.com/document/product/269/75979  | com/tencent/qcloud/tuikit/tuicommunity/utils/CommunityConstants.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/community-cover/community\_cover\_%s.png  | com/tencent/qcloud/tuikit/tuicommunity/utils/CommunityConstants.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/community-cover/community\_cover\_default.png  | com/tencent/qcloud/tuikit/tuicommunity/utils/CommunityConstants.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/group-avatar/group\_avatar\_default.png  | com/tencent/qcloud/tuikit/tuicommunity/utils/CommunityConstants.java  |
| https://cloud.tencent.com/document/product/269/36852  | com/tencent/qcloud/tuikit/tuicommunity/utils/CommunityConstants.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/group-avatar/group\_avatar\_%s.png  | com/tencent/qcloud/tuikit/tuicommunity/utils/CommunityConstants.java  |
| https://cloud.tencent.com/act/pro/imnew?from=17971  | com/tencent/qcloud/tuikit/tuicommunity/utils/CommunityConstants.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Completable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Single.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Maybe.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Observable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Flowable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/Completable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/Single.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/Maybe.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/Observable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/Flowable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling  | io/reactivex/rxjava3/exceptions/OnErrorNotImplementedException.java  |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0  | io/reactivex/rxjava3/exceptions/UndeliverableException.java  |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling  | io/reactivex/exceptions/OnErrorNotImplementedException.java  |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0  | io/reactivex/exceptions/UndeliverableException.java  |
| https://cloud.tencent.com/document/product/269/37059  | 摸瓜V1引擎  |
| https://www.tencentcloud.com/document/product/1047/34286  | 摸瓜V1引擎  |
| https://162.14.13.170/v4/ConfigGetSvc/GetOpenSSOIPList  | lib/arm64-v8a/libImSDK.so  |
| http://162.14.3.250/v4/ConfigGetSvc/GetOpenSSOIPList  | lib/arm64-v8a/libImSDK.so  |
| https://119.29.29.99/d?token=353599313  | lib/arm64-v8a/libImSDK.so  |
| http://119.29.29.98/d?id=39662  | lib/arm64-v8a/libImSDK.so  |
| http://162.14.19.114/  | lib/arm64-v8a/libImSDK.so  |

### **4.3 邮箱线索**

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 15778800000  | org/joda/time/chrono/BasicFixedMonthChronology.java  |
| 15778476000  | org/joda/time/chrono/GregorianChronology.java  |
| 15778800000  | org/joda/time/chrono/JulianChronology.java  |
| 15308640144  | org/joda/time/chrono/IslamicChronology.java  |

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: CN=sf, OU=gg, O=ghd, L=vs, ST=vhbd, C=965852 签名算法: rsassa\_pkcs1v15 有效期自: 2024-09-19 02:46:44+00:00 有效期至: 2049-09-13 02:46:44+00:00 发行人: CN=sf, OU=gg, O=ghd, L=vs, ST=vhbd, C=965852 序列号: 0x1 哈希算法: sha256 md5值: 4232974ff0f1d8985277286b18328f69 sha1值: 1bc333908aad86a8e3261959aad2255abcc16cc3 sha256值: bb9dee9591bb6e058d10376929470b15521680b78a6141e3539e6b3cd710ed41 sha512值: 44ecee0708bbc8aa313a3c688cbc6ac70bb2d8c8f7419233470ff4ebe89cf099b0bcbf8b915c57136938cd0ec8beabcfa9edf0e2e8c1939b1a4d94bdf7607c14 公钥算法: rsa 密钥长度: 2048 指纹: 325211680eb4847aabf26f4430d9b63ad6653dd215b3e28c1ad90d00515090e1**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "common\_input\_pwd\_title" : "请输入支付密码"  |
| "congratulations\_becoming\_a\_node\_user" : "恭喜您升级为节点人！"  |
| "contact\_no\_such\_user" : "该用户不存在"  |
| "private\_group" : "讨论组"  |
| "reset\_password" : "重置登录密码"  |
| "common\_input\_pwd\_title" : "Please enter your payment password"  |
| "congratulations\_becoming\_a\_node\_user" : "Congratulations on becoming a node user ！"  |
| "reset\_password" : "Reset login password"  |
| "contact\_no\_such\_user" : "هذا المستخدم غير موجود"  |
| "private\_group" : "محادثة فردية"  |
| "contact\_no\_such\_user" : "该用户不存在"  |
| "private\_group" : "讨论组"  |
| "common\_input\_pwd\_title" : "請輸入支付密碼"  |
| "congratulations\_becoming\_a\_node\_user" : "恭喜您升级为节点人！"  |
| "contact\_no\_such\_user" : "該用戶不存在"  |
| "private\_group" : "讨论组"  |
| "reset\_password" : "重置登錄密碼"  |
| "common\_input\_pwd\_title" : "请输入支付密码"  |
| "congratulations\_becoming\_a\_node\_user" : "恭喜您升级为节点人！"  |
| "reset\_password" : "重置登录密码"  |
| "contact\_no\_such\_user" : "This user does not exist."  |
| "private\_group" : "Discussion Group"  |

## **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\_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.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_PRIVILEGED\_PHONE\_STATE | 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 |
| 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.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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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.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.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.CALL\_PHONE | 危险 | 直接拨打电话号码 | 允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码 |
| android.permission.DISABLE\_KEYGUARD | 正常 |  | 如果键盘不安全,允许应用程序禁用它。 |
| 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.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.USE\_BIOMETRIC | 正常 |  | 允许应用使用设备支持的生物识别模式。 |
| android.permission.SYSTEM\_ALERT\_WINDOW | 危险 | 显示系统级警报 | 允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕 |
| com.hykj.nhwj.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。**