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

**土豆密聊（ 1.1.1.1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 | 土豆密聊 |
| 版本 | 1.1.1.1 |
| 包名 | com.tudou.im |
| 域名线索 | 19条 |
| URL线索 | 6条 |
| APP图标 |  |
| 分析日期 | 2025年6月21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 | 土豆密聊.apk |
| 文件大小 | 88.05MB |
| MD5值 | 941f7d25a1ab0a60dfdced8007d5a622 |
| SHA1值 | 1bca613cf17a18ce60f43ae7366025a5034a8dad |
| SHA256值 | 4092399f427a8bf51786422ca8170d72096bbac2974a7edafd4a26871864b18d |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 土豆密聊 |
| 包名 | com.tudou.im |
| 主活动Activity | com.hio.client.business.ui.SplashActivity |
| 安卓版本名称 | 1.1.1.1 |
| 安卓版本 | 18 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| data-dre.push.dbankcloud.com | IP: 80.158.49.244 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| grs.dbankcloud.asia | IP: 49.4.35.251 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| confluence.agoralab.co | IP: 123.125.46.42 所属国家: China 地区: Beijing 城市: Beijing  |
| data-drcn.push.dbankcloud.com | IP: 49.4.40.58 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| grs.platform.dbankcloud.ru | 没有服务器地理信息.  |
| data-drru.push.dbankcloud.com | IP: 159.138.202.31 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| metrics5.data.hicloud.com | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| metrics5.dt.dbankcloud.ru | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| journeyapps.com | IP: 18.65.168.3 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| metrics1-drcn.dt.dbankcloud.cn | IP: 111.202.16.252 所属国家: China 地区: Beijing 城市: Beijing  |
| metrics2.data.hicloud.com | IP: 80.158.38.48 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| data-dra.push.dbankcloud.com | IP: 119.8.163.189 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| grs.dbankcloud.com | IP: 60.28.200.159 所属国家: China 地区: Tianjin 城市: Tianjin  |
| metrics-dra.dt.hicloud.com | IP: 94.74.88.100 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| grs.dbankcloud.cn | IP: 121.36.117.149 所属国家: China 地区: Beijing 城市: Beijing  |
| 139.224.238.21 | IP: 139.224.238.21 所属国家: China 地区: Shanghai 城市: Shanghai  |
| www.webrtc.org | IP: 74.125.135.139 所属国家: United States of America 地区: California 城市: Mountain View  |
| grs.dbankcloud.eu | 没有服务器地理信息.  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| 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-drcn.dt.dbankcloud.cn:443  | 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  |
| http://agoratest  | lib/arm64-v8a/libagora-rtc-sdk.so  |
| http://139.224.238.21:9090/udrm/udrmGetLicense  | lib/arm64-v8a/libagora-rtc-sdk.so  |
| https://confluence.agoralab.co/pages/viewpage.action?pageId=  | lib/arm64-v8a/libagora-rtc-sdk.so  |
| https://confluence.agoralab.co/pages/viewpage.action?pageId=1161004477  | lib/arm64-v8a/libagora-rtc-sdk.so  |
| https://confluence.agoralab.co/pages/viewpage.action?pageId=1035862602  | lib/arm64-v8a/libagora-rtc-sdk.so  |
| http://s?  | lib/arm64-v8a/libagora-rtc-sdk.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/generic-frame-descriptor  | lib/arm64-v8a/libagora-rtc-sdk.so  |
| http://agoratest  | lib/armeabi-v7a/libagora-rtc-sdk.so  |
| http://139.224.238.21:9090/udrm/udrmGetLicense  | lib/armeabi-v7a/libagora-rtc-sdk.so  |
| https://confluence.agoralab.co/pages/viewpage.action?pageId=  | lib/armeabi-v7a/libagora-rtc-sdk.so  |
| https://confluence.agoralab.co/pages/viewpage.action?pageId=1161004477  | lib/armeabi-v7a/libagora-rtc-sdk.so  |
| https://confluence.agoralab.co/pages/viewpage.action?pageId=1035862602  | lib/armeabi-v7a/libagora-rtc-sdk.so  |
| http://s  | lib/armeabi-v7a/libagora-rtc-sdk.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/generic-frame-descriptor  | lib/armeabi-v7a/libagora-rtc-sdk.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| appro@openssl.org  | lib/arm64-v8a/libagora-ffmpeg.so  |
| appro@openssl.org  | lib/arm64-v8a/libagora-rtc-sdk.so  |

### **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: False 找到 1 个唯一证书 主题: CN=pure, OU=pure, O=pure, L=sc, ST=cd, C=635000 签名算法: rsassa\_pkcs1v15 有效期自: 2024-10-12 07:29:40+00:00 有效期至: 2124-09-18 07:29:40+00:00 发行人: CN=pure, OU=pure, O=pure, L=sc, ST=cd, C=635000 序列号: 0x1 哈希算法: sha256 md5值: 8c00c2f3f60c87ca65f81573ad909383 sha1值: 88be58213457bc79b596b6bbc4a377e63a16500c sha256值: 7b4f33197f6e8213fc02342c3553e1995d4b1dec7daf09e6017ba7f2d22ea7bf sha512值: 7d5c49a0894590b236c748da777ef14fa8afa4278fd03496a6ca119db79f44fdf8b5442ad9ec060ea78e23e74da8b82b9970c3a2d515ebeb8b62cdf506283731 公钥算法: rsa 密钥长度: 2048 指纹: 45a3a8a3b0da91a0d45eca9f26da784f9653fa4248ba0f282e08dc33be42d617**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "add\_friend\_find\_user" : "找人"  |
| "add\_friend\_search\_user" : "查找人"  |
| "chat\_card\_user" : "个人名片"  |
| "chat\_private\_set" : "聊天设置"  |
| "contact\_auth\_chat" : "仅聊天"  |
| "contact\_auth\_chat\_and\_circle" : "聊天、朋友圈"  |
| "contact\_auth\_circle" : "朋友圈设置"  |
| "contact\_auth\_circle1" : "不让TA看"  |
| "contact\_auth\_circle2" : "不看TA"  |
| "contact\_auth\_friend" : "设置朋友权限"  |
| "digits\_key" : "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ"  |
| "digits\_password" : "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ`¬!£$%^\*()~=#{}[];':,./?/\*-\_+<>@&"  |
| "library\_zxingandroidembedded\_author" : "JourneyApps"  |
| "library\_zxingandroidembedded\_authorWebsite" : "https://journeyapps.com/"  |
| "loading\_go\_auth" : "Go to Alipay for authorization"  |
| "loading\_go\_auth" : "前往支付寶授權"  |
| "loading\_go\_auth" : "去支付寶授權"  |
| "loading\_go\_auth" : "去支付宝授权"  |

## **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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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 |
| android.permission.EXPAND\_STATUS\_BAR | 正常 | 展开/折叠状态栏 | 允许应用程序展开或折叠状态栏 |
| android.permission.ACCESS\_MEDIA\_LOCATION | 危险 | 访问的任何地理位置 | 允许应用程序访问的任何地理位置持久保存在用户的共享集合 |
| android.permission.KILL\_BACKGROUND\_PROCESSES | 正常 | 杀死后台进程 | 允许应用程序杀死其他应用程序的后台进程,即使内存不低 |
| android.permission.FOREGROUND\_SERVICE\_MEDIA\_PLAYBACK | 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.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.CHANGE\_WIFI\_MULTICAST\_STATE | 正常 | 允许Wi-Fi多播接收  | 允许应用程序接收不是直接发送到您设备的数据包。这在发现附近提供的服务时很有用。它比非多播模式使用更多的功率 |
| 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.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.READ\_MEDIA\_IMAGES | 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.READ\_MEDIA\_VIDEO | 未知 | Unknown permission | Unknown permission from android reference |
| 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.REORDER\_TASKS | 正常 | 重新排序正在运行的应用程序 | 允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前 |
| com.tudou.im.permission.MIPUSH\_RECEIVE | 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.ACCESS\_FINE\_LOCATION | 危险 | 精细定位（GPS） | 访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量 |
| android.permission.ACCESS\_COARSE\_LOCATION | 危险 | 粗定位 | 访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置 |
| android.permission.DISABLE\_KEYGUARD | 正常 |  | 如果键盘不安全,允许应用程序禁用它。 |
| android.permission.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| android.permission.CHANGE\_CONFIGURATION | 系统需要 | 更改您的 UI 设置 | 允许应用程序更改当前配置,例如语言环境或整体字体大小 |
| 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.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。 |
| 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.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\_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.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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| com.tudou.im.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 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 |
| com.tudou.im.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| com.tudou.im.permission.PUSH\_PROVIDER | 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 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.hio.client.business.ui.SplashActivity | **Schemes**: tencentminiapp102582855://,  |
| com.tencent.tauth.AuthActivity | **Schemes**: tencent102582855://,  |

**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。**