MoGua

土豆密聊 1.1.1.1.APK 分析报告

APP名称:	土豆密聊

包名:	com.tudou.im
域名线索:	19条
URL线索:	6条
邮箱线索:	2条
分析日期:	2025年6月21日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 土豆密聊.apk
文件大小: 88.05MB
MD5值: 941f7d25a1ab0a60dfdced8007d5a622
SHA1值: 1bca613cf17a18ce60f43ae7366025a5034a8dad
SHA256值: 4092399f427a8bf51786422ca8170d72096bbac2974a7edafd4a26871864b18d

APP 信息

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

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 **纬度**: 54.321358 **经度**: 10.134532
grs.dbankcloud.asia	**IP**: 49.4.35.251 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
confluence.agoralab.co	**IP**: 123.125.46.42 **所属国家**: China **地区**: Beijing

	城市: Beijing **纬度**: 39.907501 **经度**: 116.397102
data-drcn.push.dbankcloud.com	IP: 49.4.40.58 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
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 **纬度**: 56.857498 **经度**: 60.612499
metrics5.data.hicloud.com	IP: 159.138.203.215 **所属国家**: Russian Federation **地区**: Sverdlovskaya oblast' **城市**: Yekaterinburg **纬度**: 56.857498 **经度**: 60.612499
metrics5.dt.dbankcloud.ru	IP: 159.138.203.215 **所属国家**: Russian Federation **地区**: Sverdlovskaya oblast' **城市**: Yekaterinburg **纬度**: 56.857498 **经度**: 60.612499
journeyapps.com	IP: 18.65.168.3 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689499

	经度: 139.692322
metrics1-drcn.dt.dbankcloud.cn	IP: 111.202.16.252 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
metrics2.data.hicloud.com	IP: 80.158.38.48 **所属国家**: Germany **地区**: Schleswig-Holstein **城市**: Kiel **纬度**: 54.321358 **经度**: 10.134532
github.com	IP: 20.205.243.166 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
data-dra.push.dbankcloud.com	IP: 119.8.163.189 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
grs.dbankcloud.com	IP: 60.28.200.159 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
	IP: 94.74.88.100 **所属国家**: Singapore

metrics-dra.dt.hicloud.com	**地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
grs.dbankcloud.cn	**IP**: 121.36.117.149 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
139.224.238.21	**IP**: 139.224.238.21 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
www.webrtc.org	**IP**: 74.125.135.139 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
grs.dbankcloud.eu	没有服务器地理信息.

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

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

手机线索

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

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"

加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

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
		Unknown	

com.tudou.im.permission.MIPUSH_RECEIVE	未知	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	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

		动	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

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://,
