MoGua

Yiqixun 12.2.6.APK 分析报告

APP名称: Yiqixun

包名:	com.yiqixunim906.chat
域名线索:	23条
URL线索:	8条
邮箱线索:	5条
分析日期:	2025年8月14日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: yqx.apk
文件大小: 80.21MB
MD5值: c55ec4763e67b30e6a0bcb0f20040cd2
SHA1值: 0bae5885acfd64dcc5cfd1ce40648e8560736f11
SHA256值: 7bb5bee71024cde6980791310c74aee01ef9dede362e2974b6c802973fb7a969

APP 信息

App名称: Yiqixun
包名: com.yiqixunim906.chat
主活动Activity: com.yiqixunim906.chat.MainActivity
安卓版本名称: 12.2.6
安卓版本: 225

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
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
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.platform.dbankcloud.ru	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 **纬度**: 32.814899 **经度**: -96.879204
metrics-dra.dt.hicloud.com	IP: 94.74.88.100 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
dartbug.com	IP: 216.239.32.21 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
www.w3.org	IP: 104.18.23.19 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
journeyapps.com	IP: 18.155.68.69 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987

	经度: 103.850281
docs.flutter.dev	IP: 199.36.158.100 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
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
grs.dbankcloud.com	IP: 60.28.193.195 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
www.webrtc.org	IP: 142.250.69.206 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
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
	IP: 34.111.97.67 **所属国家**: United States of America

developer.mozilla.org	**地区**: Missouri **城市**: Kansas City **纬度**: 39.099731 **经度**: -94.578568
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
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
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.dbankcloud.asia	IP: 121.36.116.8 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
grs.dbankcloud.eu	没有服务器地理信息.
grs.dbankcloud.cn	IP: 49.4.35.251 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361

	经度: 113.264572
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
yqxtx-sh-1327836933.cos.ap-shanghai.myqcloud.com	**IP**: 127.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000

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
https://github.com/richtr/NoSleep.js/issues/15	摸瓜V2引擎
https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released)	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://yqxtx-sh-1327836933.cos.ap-shanghai.myqcloud.com/	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

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
appro@openssl.org	lib/arm64-v8a/libflutter.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

手机线索

签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: True
找到 1 个唯一证书
主题: C=3Nv2H, ST=VlMjP, L=TzSUg, O=nx1746032088792, OU=lm1746032088792, CN=jwyd

签名算法: rsassa_pkcs1v15
有效期自: 2025-04-30 16:54:49+00:00
有效期至: 2075-04-18 16:54:49+00:00
发行人: C=3Nv2H, ST=VlMjP, L=TzSUg, O=nx1746032088792, OU=lm1746032088792, CN=jwyd
序列号: 0x6cc39142
哈希算法: sha512
md5值: eb325bc7eec6afd6f66ec13abc1eed2b
sha1值: b7e13d8a84a3aa4bd02d52262dd9036df0faf640
sha256值: e3d168766dd369625d4fcebade5a7fe06d009c2352cfa7120d8d2e4934ab8456
sha512值: 5f94aca7ff2455f407b8ede37d9ac16e1b1b72744825b11c6958f9af93427e8c40f36251dbcb4a983bb4f00f8da4987abdc69c04935fdccc2c9e12dbacc39dc3
公钥算法: rsa
密钥长度: 4096
指纹: b8d614830816044c1070f1ade369ad2e09b3f282d5167464cd8980e7356d11cf

硬编码敏感信息

可能的敏感信息
"library_zxingandroidembedded_author" : "JourneyApps"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"

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.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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.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.BLUETOOTH_SCAN	未知	Unknown permission	Unknown permission from android reference
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
com.vivo.notification.permission.BADGE_ICON	未知	Unknown permission	Unknown permission from android reference
com.sec.android.provider.badge.permission.READ	正常	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.sec.android.provider.badge.permission.WRITE	正常	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
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.huawei.android.launcher.permission.READ_SETTINGS	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.huawei.android.launcher.permission.WRITE_SETTINGS	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
android.permission.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
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.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.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.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.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.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.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_CONNECT	未知	Unknown permission	Unknown permission from android reference
com.yiqixunim906.chat.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.FOREGROUND_SERVICE_MEDIA_PROJECTION	未知	Unknown permission	Unknown permission from android reference
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.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.yiqixunim906.chat.permission.JPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference
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
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.QUERY_ALL_PACKAGES	正常		允许查询设备上的任何普通应用程序,无论清单声明如何
com.yiqixunim906.chat.permission.PROCESS_PUSH_MSG	未知	Unknown permission	Unknown permission from android reference
com.yiqixunim906.chat.permission.PUSH_PROVIDER	未知	Unknown permission	Unknown permission from android reference
com.yiqixunim906.chat.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.meizu.flyme.permission.PUSH	未知	Unknown permission	Unknown permission from android reference
com.meizu.flyme.push.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.yiqixunim906.chat.push.permission.MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.meizu.c2dm.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.yiqixunim906.chat.permission.C2D_MESSAGE	未	Unknown	Unknown permission from android reference

	知	permission	
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.hihonor.android.launcher.permission.CHANGE_BADGE	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

报告由 **摸瓜**APK**反编译平台** 自动生成，并非包含所有检测结果，有疑问请联系管理员。