



MoGua

Yiqixun 12.2.7.APK 分析报告



APP名称:

Yiqixun

包名: com.yiqixunim906.chat

域名线索: 13条

URL线索: 6条

邮箱线索: 5条

分析日期: 2025年6月17日

分析平台: [摸瓜APK反编译平台](#)

文件名: yqx.apk
文件大小: 75.99MB
MD5值: c606ddff2c7a4a9f91ab1bc0387877ff
SHA1值: 5e0ee6d99e1254d2683387a6991b9e2ce5def00b
SHA256值: d9fc17c122cbbbbb5d7656d08a6b2c90def6336a111fd3d240378d59d15515df

i 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: 12.2.7
安卓版本: 225

🔍 域名线索

域名	服务器信息
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
grs.dbankcloud.cn	IP: 124.70.116.153 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
www.w3.org	IP: 104.18.22.19 所属国家: United States of America 地区: California

	城市: San Francisco 纬度: 37.775700 经度: -122.395203
developer.mozilla.org	IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568
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: 142.251.33.78 所属国家: Canada 地区: Ontario 城市: Toronto 纬度: 43.653660 经度: -79.382927
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
	IP: 18.65.168.24

journeyapps.com	所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
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
grs.dbankcloud.eu	没有服务器地理信息.
grs.dbankcloud.asia	IP: 49.4.40.185 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
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

 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://grs.dbankcloud.com	摸瓜V2引擎
https://grs.dbankcloud.cn	摸瓜V2引擎
https://grs.dbankcloud.eu	摸瓜V2引擎
https://grs.dbankcloud.asia	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://yqtx-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=U1UaM, ST=WfSq9, L=RfaEG, O=oh1750054392461, OU=wi1750054392461, CN=efae
签名算法: rsassa_pkcs1v15
有效期自: 2025-06-16 06:13:13+00:00
有效期至: 2075-06-04 06:13:13+00:00
发行人: C=U1UaM, ST=WfSq9, L=RfaEG, O=oh1750054392461, OU=wi1750054392461, CN=efae
序列号: 0x6c5379a5
哈希算法: sha512

md5值: 392500d8f5e466d56eea329e6941dc1c
sha1值: b468b6900690c4e77d6a950646affdac52fe4e10
sha256值: d4032f22a7a8d789530631b3aad15a7b59af521b221f3b7472d0f82f6bc7dab5
sha512值: a8044831e935a072fba36932d57755a293018ce77c006daa03edb18081cac3a7296287e1aabaf33285eaa0a474f73b31b5809dbed657731d2752f78db8f81c72
公钥算法: rsa
密钥长度: 4096
指纹: e31db9286872247647d2da93a16d04452801d1aa4189c7121223bbf1abaf677b

 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.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.FOREGROUND_SERVICE	正		允许常规应用程序使用 Service.startForeground。

	常		
android.permission.FOREGROUND_SERVICE_CAMERA	未知	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE_MICROPHONE	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.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.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_MEDIA_PROJECTION	未知	Unknown permission	Unknown permission from android reference
com.yiqixunim906.chat.permission.JPUSH_MESSAGE	未	Unknown	Unknown permission from android reference

	知	permission	
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

应用内通信