MoGua

姐姐 8.1.7.APK 分析报告

APP名称: 姐姐

包名:	com.l4c23403e9.f341d597df
域名线索:	11条
URL线索:	14条
邮箱线索:	2条
分析日期:	2025年7月31日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: jjfhrh_0ow1PwwjOx_0.apk
文件大小: 78.86MB
MD5值: 1f9399a3bc7a112fa87149f0e17cf79f
SHA1值: 9b34db3cc5400965ecbc3e3f4d58008deb282443
SHA256值: 857f863e67c7cc0da3b33725361979938ad54e0f477d6b1dd29fdf19a08ba65f

APP 信息

App名称: 姐姐
包名: com.l4c23403e9.f341d597df
主活动Activity: com.l4c23403e9.f341d597df.MainActivity
安卓版本名称: 8.1.7
安卓版本: 1

域名线索

域名	服务器信息
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
da.dun.163.com	**IP**: 59.111.248.82 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
schemas.android.com	没有服务器地理信息.
	IP: 1.95.21.111

ac.dun.163yun.com	**所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
www.example.com	IP: 23.55.51.197 **所属国家**: Australia **地区**: New South Wales **城市**: Sydney **纬度**: -33.867779 **经度**: 151.207047
crash.163.com	IP: 45.254.50.146 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
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
developer.android.com	IP: 142.250.73.78 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
10.0.2.2	IP: 10.0.2.2 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000

ac.dun.163.com	**IP**: 220.197.32.187 **所属国家**: China **地区**: Sichuan **城市**: Mianyang **纬度**: 31.459375 **经度**: 104.753128
docs.sentry.io	**IP**: 76.76.21.164 **所属国家**: United States of America **地区**: California **城市**: Walnut **纬度**: 34.015400 **经度**: -117.858223

URL线索

URL信息	Url所在文件
http://schemas.android.com/apk/res/android	com/humrousz/sequence/AnimationImageView.java
https://crash.163.com/uploadCrashLogInfo.do	com/netease/htprotect/necrash/nis/crashreport/O8oO888.java
https://crash.163.com/client/api/uploadStartUpInfo.do	com/netease/htprotect/necrash/nis/crashreport/O8oO888.java
https://crash.163.com/uploadCrashLogInfo.do	com/netease/htprotect/necrash/nis/p010O8oO888/p011O8oO888/O8oO888.java
https://crash.163.com/client/api/uploadStartUpInfo.do	com/netease/htprotect/necrash/nis/p010O8oO888/p011O8oO888/O8oO888.java
https://ac.dun.163yun.com	com/netease/mobsec/c/a.java
https://ac.dun.163.com	com/netease/mobsec/c/a.java

https://ac.dun.163.com/v2/config/android?	com/netease/mobsec/f/f.java
https://ac.dun.163yun.com/v2/config/android?	com/netease/mobsec/f/f.java
https://ac.dun.163yun.com/v2/m/d	com/netease/mobsec/f/f.java
https://ac.dun.163.com/v2/m/d	com/netease/mobsec/f/f.java
https://ac.dun.163yun.com/v2/m/b	com/netease/mobsec/f/f.java
https://ac.dun.163.com/v2/m/b	com/netease/mobsec/f/f.java
https://crash.163.com/uploadCrashLogInfo.do	com/netease/nis/basesdk/crash/BaseJavaCrashHandler.java
https://crash.163.com/client/api/uploadStartUpInfo.do	com/netease/nis/basesdk/crash/BaseJavaCrashHandler.java
https://da.dun.163.com/sn.gif?d=	com/netease/nis/captcha/i.java
http://www.example.com	com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/CustomTabsHelper.java
https://docs.flutter.dev/deployment/android	io/flutter/embedding/engine/loader/FlutterLoader.java
https://developer.android.com/guide/topics/permissions/overview	io/flutter/plugin/platform/PlatformPlugin.java
http://10.0.2.2:8969/stream	io/sentry/SpotlightIntegration.java
https://docs.sentry.io/platforms/android/troubleshooting/mixed-versions	io/sentry/util/n.java
https://docs.sentry.io/platforms/java/troubleshooting/mixed-versions	io/sentry/util/n.java
https://github.com/Baseflow/flutter-permission-handler/issues	n/q.java
https://github.com/yyued/SVGAPlayer-Android	y4/g.java

邮箱线索

邮箱地址	所在文件
xxx@email.elided	com/tencent/liteav/base/PiiElider.java
u0013android@android.com0 u0013android@android.com	y1/r.java

手机线索

手机号	所在文件
17512775099	k3/a.java

签名证书

APK已签名
v1 签名: False
v2 签名: True
v3 签名: False
找到 1 个唯一证书
主题: C=CN, ST=Beijing, L=Beijing, O=uXkdzQlm, OU=gJxSiBNZ, CN=aCwgEaXm
签名算法: dsa
有效期自: 2025-07-17 03:21:24+00:00
有效期至: 2029-10-12 03:21:24+00:00
发行人: C=CN, ST=Beijing, L=Beijing, O=uXkdzQlm, OU=gJxSiBNZ, CN=aCwgEaXm
序列号: 0x7d126442
哈希算法: sha256
md5值: 742c27eac401e0ebae9c578cb1b164b7
sha1值: f6ab01202fee5303dad94d6f758eceb3a75db083

sha256值: 511ba0350ba8783ec83d5669b387d8fb079038e24c53e49c271da342f0e079e4
sha512值: 6d5a0704dc81ff7d0f6d4c43cbcd987a59dedef53fc574d93f5c909c9ab49ed69b819b12d56d9b366c1e1a49ae0dc061e3635d168482f512c2504ed9307e6d5d
公钥算法: dsa
密钥长度: 2048
指纹: 94363feca9fc07635737cfe4f6fea868f76177ed75e2bd6c4b65077bc51ee0ab

硬编码敏感信息

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_MEDIA_VISUAL_USER_SELECTED	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.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_AUDIO	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.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.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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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
		允许应用程序广泛	

android.permission.MANAGE_EXTERNAL_STORAGE	危险	访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
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.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.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息
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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.PACKAGE_USAGE_STATS	合法	更新组件使用统计	允许修改收集的组件使用统计。不供普通应用程序使用
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.POST_NOTIFICATIONS	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_PLAYBACK	未知	Unknown permission	Unknown permission from android reference
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.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
Manifest.permission.CAPTURE_AUDIO_OUTPUT	未知	Unknown permission	Unknown permission from android reference
com.l4c23403e9.f341d597df.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference
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.READ_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference
com.google.android.gms.permission.AD_ID	未知	Unknown permission	Unknown permission from android reference
com.asus.permission.READ_SDID_PROVIDER	未知	Unknown permission	Unknown permission from android reference
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference

freemme.permission.msa	未知	Unknown permission	Unknown permission from android reference
freemme.permission.msa.SECURITY_ACCESS	未知	Unknown permission	Unknown permission from android reference

应用内通信
