MoGua

MD 8.0.8.APK 分析报告

APP名称:	MD
包名:	a8nai.k6bg3.a4zg7
域名线索:	13条
URL线索:	13条
邮箱线索:	2条
分析日期:	2025年4月8日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: mdn.apk
文件大小: 77.38MB
MD5值: 3f8acee0a2d8619ce86d3a21c7382fd5
SHA1值: 1277ec27dc528a46c8a240881697dabd63bf0b83
SHA256值: 8f267aec16b3753f4e4935157da5c023288c2a3dc50244dd76d5cfa73a2f528c

APP 信息

App名称: MD
包名: a8nai.k6bg3.a4zg7
主活动Activity: a8nai.k6bg3.a4zg7.MainActivity
安卓版本名称: 8.0.8
安卓版本: 1

域名线索

域名	服务器信息
www.example.com	**IP**: 92.122.244.51 **所属国家**: Germany **地区**: Hessen **城市**: Frankfurt am Main **纬度**: 50.110882 **经度**: 8.681996
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

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
ac.dun.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
cloud.tencent.com	**IP**: 60.28.220.199 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
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
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
developer.android.com	**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
ac.dun.163yun.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
playvideo.qcloud.com	**IP**: 115.56.90.192 **所属国家**: China **地区**: Henan **城市**: Jiaozuo **纬度**: 35.239719 **经度**: 113.233063
	IP: 221.204.15.52 **所属国家**: China **地区**: Shanxi

1255566655.vod2.myqcloud.com	**城市**: Taiyuan **纬度**: 37.869438 **经度**: 112.561508
schemas.android.com	没有服务器地理信息.
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

URL线索

URL信息	Url所在文件
http://schemas.android.com/apk/res/android	com/humrousz/sequence/AnimationImageView.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/g.java
http://www.example.com	com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/CustomTabsHelper.java
https://cloud.tencent.com/act/event/License	com/tencent/liteav/a.java
http://playvideo.qcloud.com/getplayinfo/v2	com/tencent/liteav/txcvodplayer/b/d.java
https://playvideo.qcloud.com/getplayinfo/v2	com/tencent/liteav/txcvodplayer/b/d.java
http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff1456497281851960244 7/coverBySnapshot/1513156403_1311093072.100_0.jpg?t=5c08d9fa&us=someus&sign=95f34beb353fe32cfe7f8b5e79cc28b1\	com/tencent/liteav/txcvodplayer/b/d.java

http://1255566655.vod2.myqcloud.com/ca754badvodgzp1255566655/8f5fbff1456497281851960244 7/imageSprite/1513156058_533711271_00001.jpg?t=5c08d9fa&us=someus&sign=79449db4e1fb05a3becfa096613659c3\	com/tencent/liteav/txcvodplayer/b/d.java
http://1255566655.vod2.myqcloud.com/ca754badvodgzp1255566655/8f5fbff1456497281851960244 7/imageSprite/1513156058_533711271.vtt?t=5c08d9fa&us=someus&sign=79449db4e1fb05a3becfa096613659c3\	com/tencent/liteav/txcvodplayer/b/d.java
http://1255566655.vod2.myqcloud.com/ca754badvodgzp1255566655/8f5fbff1456497281851960244 7/uAnXX0OMLSAA.wmv?t=5c08d9fa&us=someus&sign=659af5dd3f27eb92dc4ed74eb561daa4\	com/tencent/liteav/txcvodplayer/b/d.java
http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff1456497281851960244 7/master_playlist.m3u8?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d\	com/tencent/liteav/txcvodplayer/b/d.java
http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff1456497281851960244 7/v.f220.m3u8?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d\	com/tencent/liteav/txcvodplayer/b/d.java
http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff1456497281851960244 7/v.f230.m3u8?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d\	com/tencent/liteav/txcvodplayer/b/d.java
http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff1456497281851960244 7/v.f240.m3u8?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d\	com/tencent/liteav/txcvodplayer/b/d.java
http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff1456497281851960244 7/v.f210.m3u8?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d\	com/tencent/liteav/txcvodplayer/b/d.java
http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff1456497281851960244 7/v.f10.mp4?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d\	com/tencent/liteav/txcvodplayer/b/d.java
http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff1456497281851960244 7/v.f20.mp4?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d\	com/tencent/liteav/txcvodplayer/b/d.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://github.com/Baseflow/flutter-permission-handler/issues	l/p.java
https://github.com/yyued/SVGAPlayer-Android	t5/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	w2/q.java

手机线索

手机号	所在文件
17512775099	i4/a.java

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=adminuf9jme, ST=adminuf9jme, L=adminuf9jme, O=adminuf9jme, OU=adminuf9jme, CN=adminuf9jme
签名算法: rsassa_pkcs1v15
有效期自: 2025-04-07 08:25:21+00:00
有效期至: 2125-03-14 08:25:21+00:00
发行人: C=adminuf9jme, ST=adminuf9jme, L=adminuf9jme, O=adminuf9jme, OU=adminuf9jme, CN=adminuf9jme
序列号: 0x6e0f24c
哈希算法: sha256
md5值: a5019fd498a1ad99824eecaefe51537b
sha1值: f9fd9ec8b1c1314d4565cec5b068d17478dcaf8f
sha256值: 868025c7b3aab960b49d6c1845daf41179c11ac4c380448e354d74896aaab372
sha512值: ac6be2fc75dc1982c5e242ae6b61c9cc80c38b7fefc00c6b9b4dd9270f3aa419213df6d52fcbcb80471e941bcb060f55018111f9bae8fa6b7190f13bf9e336a1
公钥算法: rsa
密钥长度: 1024
指纹: 7ba5ac9954c1db7b2aac4c18fea14cc33f87faeebbd0c15063522b257ff2ae56

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.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛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
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
a8nai.k6bg3.a4zg7.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

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。