MoGua

喜马拉雅儿童 4.0.0.APK 分析报告

APP名称: 喜马拉雅儿童

包名:	com.ximalaya.ting.android.carkids
域名线索:	23条
URL线索:	22条
邮箱线索:	0条
分析日期:	2025年1月24日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: TingCarKids_SVW_MOS_ID4_0_2023-04-04_v4.0.0_c150_proguard.apk
文件大小: 14.64MB
MD5值: 9af4bf9ff7c24bc99b3602fd8ea0d2ca
SHA1值: 3a26caa1f92fc6150551b6ea1bd544b7a386d1cd
SHA256值: 89cdb0b8ff72605e50e6778822ac9bb1a8066cbfefc726c2cedba915da323837

APP 信息

App名称: 喜马拉雅儿童
包名: com.ximalaya.ting.android.carkids
主活动Activity: com.ximalaya.ting.android.carkids.business.module.splash.WelActivity
安卓版本名称: 4.0.0
安卓版本: 150

域名线索

域名	服务器信息
mpay.ximalaya.com	**IP**: 140.249.85.79 **所属国家**: China **地区**: Shandong **城市**: Jinan **纬度**: 36.668331 **经度**: 116.997223
android.bugly.qq.com	**IP**: 109.244.244.35 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
xdcs-collector.ximalaya.com	**IP**: 114.80.99.65 **所属国家**: China **地区**: Shanghai

	城市: Shanghai **纬度**: 31.222219 **经度**: 121.458061
aod.cos.tx.xmcdn.com	**IP**: 42.81.212.164 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142220 **经度**: 117.176666
schemas.android.com	没有服务器地理信息.
m.ximalaya.com	**IP**: 42.81.15.45 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142220 **经度**: 117.176666
test.9nali.com	没有服务器地理信息.
adse.ximalaya.com	**IP**: 114.80.99.85 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.222219 **经度**: 121.458061
www.baidu.com	**IP**: 110.242.68.4 **所属国家**: China **地区**: Hebei **城市**: Baoding **纬度**: 38.851109 **经度**: 115.490280
xdcs-collector.test.ximalaya.com	没有服务器地理信息.

mermaid.uat.ximalaya.com	没有服务器地理信息.
passport.ximalaya.com	**IP**: 42.81.16.110 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142220 **经度**: 117.176666
fdfs.xmcdn.com	**IP**: 123.151.98.196 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142220 **经度**: 117.176666
mermaid.test.ximalaya.com	没有服务器地理信息.
cms.9nali.com	**IP**: 61.172.194.131 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.222219 **经度**: 121.458061
rqd.uu.qq.com	**IP**: 175.27.12.121 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
api.ximalaya.com	**IP**: 114.80.99.73 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.222219 **经度**: 121.458061

www.ximalaya.com	**IP**: 140.249.84.8 **所属国家**: China **地区**: Shandong **城市**: Jinan **纬度**: 36.668331 **经度**: 116.997223
api.xchanger.cn	**IP**: 47.110.175.169 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
cms.uat.9nali.com	**IP**: 172.29.0.11 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
fdfs.uat.xmcdn.com	**IP**: 42.81.118.63 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142220 **经度**: 117.176666
mermaid.ximalaya.com	**IP**: 180.153.250.242 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.222219 **经度**: 121.458061
fdfs.test.ximalaya.com	没有服务器地理信息.

URL线索

URL信息	Url所在文件
http://mermaid.ximalaya.com/config/ts/v1/currTime	d/h/b/a/d/a.java
https://api.ximalaya.com/oauth2/refresh_token?	d/h/b/a/a/b/a/g.java
http://www.baidu.com	d/h/b/a/a/b/a/g.java
http://api.ximalaya.com/openapi-gateway-app/tracks/get_play_info	d/h/b/a/a/b/a/b.java
http://api.ximalaya.com/openapi-gateway-app/encrypt/exchange	d/h/b/a/a/b/a/b.java
http://adse.ximalaya.com/soundPatch	d/h/b/a/a/b/a/c.java
http://api.ximalaya.com/version/get_latest_version	d/h/b/a/a/b/a/c.java
https://mpay.ximalaya.com/openapi-payfacade-app/open_pay/get_obfuscated_play_info	d/h/b/a/a/b/a/c.java
http://api.ximalaya.com/version/get_latest_version	d/h/b/a/a/b/a/d.java
https://mpay.ximalaya.com/openapi-payfacade-app/open_pay/get_obfuscated_play_info	d/h/b/a/a/b/a/d.java
http://adse.ximalaya.com/soundPatch	d/h/b/a/a/b/a/d.java
http://api.ximalaya.com/oauth2/secure_access_token	d/h/b/a/a/b/a/d.java
http://www.ximalaya.com	d/h/b/a/a/b/a/d.java
http://api.ximalaya.com/openapi-gateway-app/tracks/get_play_info	d/h/b/a/a/b/a/d.java
http://api.ximalaya.com/openapi-gateway-app/encrypt/exchange	d/h/b/a/a/b/a/d.java

http://www.baidu.com	d/h/b/a/a/b/a/f.java
http://schemas.android.com/apk/res/android	a/g/d/c/g.java
http://api.ximalaya.com/openapi-gateway-app/subscribe/is_subscribed	com/ximalaya/ting/android/opensdk/player/service/h.java
http://api.ximalaya.com/openapi-gateway-app/encrypt/exchange	com/ximalaya/ting/android/opensdk/datatrasfer/b.java
http://api.ximalaya.com/openapi-gateway-app/tracks/get_play_info	com/ximalaya/ting/android/opensdk/datatrasfer/b.java
http://api.ximalaya.com/openapi-gateway-app/albums/browse	com/ximalaya/ting/android/opensdk/datatrasfer/CommonRequest.java
http://api.ximalaya.com/openapi-gateway-app/tracks/get_last_play_tracks	com/ximalaya/ting/android/opensdk/datatrasfer/CommonRequest.java
http://api.ximalaya.com/openapi-gateway-app/search/all	com/ximalaya/ting/android/opensdk/datatrasfer/CommonRequest.java
http://api.ximalaya.com/iot/openapi-smart-device-api/play-records	com/ximalaya/ting/android/opensdk/datatrasfer/CommonRequest.java
http://api.ximalaya.com/oauth2/authorize	com/ximalaya/ting/android/opensdk/datatrasfer/CommonRequest.java
http://api.ximalaya.com/openapi-gateway-app/encrypt/exchange	com/ximalaya/ting/android/opensdk/datatrasfer/CommonRequest.java
http://api.ximalaya.com/openapi-gateway-app/albums/get_batch	com/ximalaya/ting/android/opensdk/datatrasfer/CommonRequest.java
http://api.ximalaya.com/openapi-gateway-app/tracks/get_play_info	com/ximalaya/ting/android/opensdk/datatrasfer/CommonRequest.java
https://api.ximalaya.com/iot/openapi-smart-device-api/xxm/tracks/	com/ximalaya/ting/android/opensdk/datatrasfer/CommonRequest.java
http://api.ximalaya.com/openapi-gateway-app/subscribe/add_or_delete	com/ximalaya/ting/android/opensdk/datatrasfer/CommonRequest.java
http://api.ximalaya.com/oauth2/secure_access_token	com/ximalaya/ting/android/opensdk/datatrasfer/c.java
http://api.ximalaya.com/oauth2/exchange_access_token	com/ximalaya/ting/android/opensdk/datatrasfer/c.java

https://api.ximalaya.com	com/ximalaya/ting/android/opensdk/login/constant/a.java
http://mermaid.ximalaya.com/config/ts/v2/tracks/cdn/	com/ximalaya/ting/android/xmtrace/l.java
http://cms.uat.9nali.com/mermaid/ts/v2/tracks/cdn/	com/ximalaya/ting/android/xmtrace/l.java
http://test.9nali.com/mermaid/ts/v2/tracks/cdn/	com/ximalaya/ting/android/xmtrace/l.java
http://cms.9nali.com/mermaid/config/debug/trackName	com/ximalaya/ting/android/xmtrace/l.java
http://test.9nali.com/mermaid/config/debug/trackName	com/ximalaya/ting/android/xmtrace/l.java
http://mermaid.uat.ximalaya.com/collector/v1	com/ximalaya/ting/android/xmtrace/l.java
http://test.9nali.com/mermaid/collector/v1	com/ximalaya/ting/android/xmtrace/l.java
http://mermaid.ximalaya.com/collector/v1	com/ximalaya/ting/android/xmtrace/l.java
http://fdfs.uat.xmcdn.com/	com/ximalaya/ting/android/xmtrace/l.java
http://fdfs.test.ximalaya.com/	com/ximalaya/ting/android/xmtrace/l.java
http://fdfs.xmcdn.com/	com/ximalaya/ting/android/xmtrace/l.java
http://xdcs-collector.ximalaya.com/api/v1/cdnAndroid	com/ximalaya/ting/android/player/cdn/CdnUtil.java
http://xdcs-collector.test.ximalaya.com/api/v1/cdnAndroid	com/ximalaya/ting/android/player/cdn/CdnUtil.java
https://passport.ximalaya.com/	com/ximalaya/ting/android/loginservice/h.java
http://mermaid.ximalaya.com/collector/xl/v2	com/ximalaya/ting/android/xmlogmanager/uploadlog/f.java
http://mermaid.test.ximalaya.com/collector/xl/v2	com/ximalaya/ting/android/xmlogmanager/uploadlog/f.java
http://test.9nali.com/mermaid/collector/xy-xld/v1	com/ximalaya/ting/android/xmlogmanager/uploadlog/f.java

http://aod.cos.tx.xmcdn.com/storages/622d-audiofreehighqps/16/50/GMCoOSQH8enUAACyzQIF_Y2g.html	com/ximalaya/ting/android/carkids/business/module/onlineprotocol/a.java
http://aod.cos.tx.xmcdn.com/storages/4321-audiofreehighqps/5E/2D/GMCoOSMH8el2AADj6gIF_Wjc.html	com/ximalaya/ting/android/carkids/business/module/onlineprotocol/a.java
http://ximalaya	com/ximalaya/ting/android/carkids/b/b/d/b.java
http://www.ximalaya.com	com/ximalaya/ting/android/carkids/mcapi/f.java
http://api.xchanger.cn/auth/oauth2/access_token/f0da847e9e4c513c9320a0215dcbe670	com/ximalaya/ting/android/carkids/mcapi/f.java
https://api.ximalaya.com/xy-os-console/xy-os-ucenter/account/auth-callback/	com/ximalaya/ting/android/car/carbusiness/g/c/m.java
http://m.ximalaya.com/iot/vehicle-app/pay	com/ximalaya/ting/android/car/carbusiness/g/b/a.java
http://api.ximalaya.com/iot/openapi-smart-device-api	com/ximalaya/ting/android/car/carbusiness/g/b/a.java
http://api.ximalaya.com/iot/openapi-smart-device-pay-api	com/ximalaya/ting/android/car/carbusiness/g/b/a.java
http://rqd.uu.qq.com/rqd/sync	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
http://android.bugly.qq.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java

邮箱线索

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: C=CN, ST=shanghai, L=shanghai, O=ximalaya.com, OU=ximalaya.com, CN=ximalaya.com
签名算法: rsassa_pkcs1v15
有效期自: 2015-09-28 10:08:19+00:00
有效期至: 2097-11-16 10:08:19+00:00
发行人: C=CN, ST=shanghai, L=shanghai, O=ximalaya.com, OU=ximalaya.com, CN=ximalaya.com
序列号: 0x7261b071
哈希算法: sha256
md5值: bea1326c8bf697091d6d0483749dff69
sha1值: f01d1c379eeccca86d805ce256eea1e59355e469
sha256值: 1ebe4dac495ec6524eba6bfc021bbdd14e8f41de1b5ddacdefad0ac83e2c42d1
sha512值: 092db1940b79d97243aeb98d9b5f6bda849c9d692bf2edde530f5c6089cb4c531ddd20f08b257af8836a43f1c186d7013e3d137429e35ef5afbe84c081464daf
公钥算法: rsa
密钥长度: 2048
指纹: fbab53a4e057e85144b94a5038100df569895d289dceccc185a79b9422883ae6

硬编码敏感信息

可能的敏感信息
"user_info_aes_password" : "ppnn13%dkstFeb1st"

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.BROADCAST_STICKY	正常	发送粘性广播	允许应用程序发送粘性广播,在广播结束后保留。恶意应用程序会导致手机使用过多内存,从而使手机运行缓慢或不稳定
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_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.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_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.PROCESS_OUTGOING_CALLS	危险	拦截拨出电话	允许应用程序处理拨出电话并更改要拨打的号码。恶意应用程序可能会监控,重定向或阻止拨出电话

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.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.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
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
com.mirrorlink.android.service.ACCESS_PERMISSION	未知	Unknown permission	Unknown permission from android reference
com.huawei.hmsauto.permission.intelligence.SERVICE_PROVIDER	未知	Unknown permission	Unknown permission from android reference
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_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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.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

应用内通信
