MoGua

爱倍力 4.1.1.APK 分析报告

APP名称:	爱倍力

包名:	com.ampli.snplugin
域名线索:	21条
URL线索:	35条
邮箱线索:	0条
分析日期:	2025年6月8日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: amt_4.1.1_20250514172800_测试环境_debug.apk
文件大小: 59.14MB
MD5值: c649066a5e906bda0fbacb5189dc9cbc
SHA1值: 02dfdd53b9c198e9c6db00d43e3cbbb9a662e41f
SHA256值: 00da6fe165e37d39d1a04d28bc5c4194b889b7f45b0c10e1f14760d796855293

APP 信息

App名称: 爱倍力
包名: com.ampli.snplugin
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 4.1.1
安卓版本: 411

域名线索

域名	服务器信息
apilocate.amap.com	**IP**: 106.11.43.81 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
www.andykhan.com	**IP**: 213.171.195.105 **所属国家**: United Kingdom of Great Britain and Northern Ireland **地区**: England **城市**: Gloucester **纬度**: 51.865681 **经度**: -2.243100
cgicol.amap.com	**IP**: 110.253.188.148 **所属国家**: China **地区**: Hebei

	城市: Zhangjiakou **纬度**: 40.810024 **经度**: 114.879349
er.dcloud.net.cn	**IP**: 127.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
er.dcloud.io	没有服务器地理信息.
dxp.baidu.com	**IP**: 110.242.68.94 **所属国家**: China **地区**: Hebei **城市**: Baoding **纬度**: 38.851109 **经度**: 115.490280
abroad.apilocate.amap.com	**IP**: 59.82.44.11 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
schemas.android.com	**IP**: 127.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
restsdk.amap.com	**IP**: 203.119.169.174 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650

	经度: 120.161583
ask.dcloud.net.cn	**IP**: 124.163.195.89 **所属国家**: China **地区**: Shanxi **城市**: Taiyuan **纬度**: 37.869438 **经度**: 112.561508
restapi.amap.com	**IP**: 203.119.169.174 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
openrcv.baidu.com	**IP**: 111.206.209.112 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
adiu.amap.com	**IP**: 110.253.188.147 **所属国家**: China **地区**: Hebei **城市**: Zhangjiakou **纬度**: 40.810024 **经度**: 114.879349
m3w.cn	**IP**: 119.188.150.187 **所属国家**: China **地区**: Shandong **城市**: Jinan **纬度**: 36.668331 **经度**: 116.997223
ns.adobe.com	没有服务器地理信息.

lbs.amap.com	**IP**: 110.253.189.212 **所属国家**: China **地区**: Hebei **城市**: Zhangjiakou **纬度**: 40.810024 **经度**: 114.879349
hmma.baidu.com	**IP**: 110.242.68.196 **所属国家**: China **地区**: Hebei **城市**: Baoding **纬度**: 38.851109 **经度**: 115.490280
dualstack-arestapi.amap.com	**IP**: 203.119.169.174 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
dualstack-a.apilocate.amap.com	**IP**: 106.11.43.81 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
datax.baidu.com	没有服务器地理信息.
www.amazon.co.uk	**IP**: 3.164.118.50 **所属国家**: United States of America **地区**: Washington **城市**: Seattle **纬度**: 47.627499 **经度**: -122.346199

URL线索

URL信息	Url所在文件
https://ask.dcloud.net.cn/article/35627	b/a.java
https://ask.dcloud.net.cn/article/35877	b/a.java
https://datax.baidu.com/xs.gif	com/baidu/mobstat/y.java
https://dxp.baidu.com/upgrade	com/baidu/mobstat/y.java
https://hmma.baidu.com/auto.gif	com/baidu/mobstat/Config.java
http://hmma.baidu.com/app.gif	com/baidu/mobstat/Config.java
https://hmma.baidu.com/app.gif	com/baidu/mobstat/Config.java
https://openrcv.baidu.com/1010/bplus.gif	com/baidu/mobstat/r.java
http://schemas.android.com/apk/res/android	com/hjq/permissions/AndroidManifestParser.java
https://adiu.amap.com/ws/device/adius	com/loc/bo.java
http://cgicol.amap.com/collection/collectData?src=baseCol&ver=v74&	com/loc/df.java
http://apilocate.amap.com/mobile/binary	com/loc/fw.java
http://dualstack-a.apilocate.amap.com/mobile/binary	com/loc/fw.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/fw.java
https://restsdk.amap.com/sdk/compliance/params	com/loc/ay.java

http://restsdk.amap.com/sdk/compliance/params	com/loc/ay.java
http://restsdk.amap.com	com/loc/w.java
http://restsdk.amap.com/v3/place/text?	com/loc/a.java
http://restsdk.amap.com/v3/place/around?	com/loc/a.java
http://restsdk.amap.com/v3/config/district?	com/loc/a.java
https://restapi.amap.com/rest/aaid/get	com/loc/ag.java
http://restapi.amap.com/rest/aaid/get	com/loc/ag.java
https://restsdk.amap.com/v3/iasdkauth	com/loc/n.java
https://dualstack-arestapi.amap.com/v3/iasdkauth	com/loc/n.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/gc.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/fo.java
http://dualstack-arestapi.amap.com/v3/geocode/regeo	com/loc/fq.java
http://restsdk.amap.com/v3/geocode/regeo	com/loc/fq.java
http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/	com/amap/api/location/AMapLocation.java
http://ns.adobe.com/xap/1.0/\u0000	io/dcloud/common/util/ExifInterface.java
https://m3w.cn/s/	io/dcloud/common/util/ShortCutUtil.java
https://ask.dcloud.net.cn/article/282	io/dcloud/common/constant/DOMException.java

https://ask.dcloud.net.cn/article/283	io/dcloud/feature/utsplugin/ProxyModule.java
https://er.dcloud.io/sc	io/dcloud/feature/gg/dcloud/ADHandler.java
https://er.dcloud.net.cn/sc	io/dcloud/feature/gg/dcloud/ADHandler.java
https://ask.dcloud.net.cn/article/35058	io/dcloud/feature/audio/AudioRecorderMgr.java
https://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.java
https://er.dcloud.io/rv	d/c.java
https://er.dcloud.net.cn/rv	d/c.java
http://www.andykhan.com/jexcelapi/index.html	jxl/read/biff/HyperlinkRecord.java
http://www.andykhan.com/jexcelapi/index.html	jxl/demo/ReadWrite.java
http://www.andykhan.com/jexcelapi	jxl/demo/Write.java
http://www.amazon.co.uk/exec/obidos/ASIN/0571058086/qid=1099836249/sr=1-3/ref=sr_1_11_3/202-6017285-1620664	jxl/demo/Write.java
http://www.andykhan.com/jexcelapi\	jxl/demo/Write.java
http://www.amazon.co.uk/exec/obidos/ASIN/0571058086qid=1099836249/sr=1-3/ref=sr_1_11_3/202-6017285-1620664\	jxl/demo/Write.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifViewUtils.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextView.java
https://ask.dcloud.net.cn/article/283	j/b.java

邮箱线索

手机线索

手机号	所在文件
14222222222	com/loc/n.java
17179869184	tv/danmaku/ijk/media/player/IjkMediaMeta.java

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=js, L=nj, O=zhengqi, OU=suruan, CN=zhong
签名算法: rsassa_pkcs1v15
有效期自: 2022-12-27 10:18:13+00:00
有效期至: 2077-09-29 10:18:13+00:00
发行人: C=cn, ST=js, L=nj, O=zhengqi, OU=suruan, CN=zhong
序列号: 0x1d313f97
哈希算法: sha1
md5值: 15e17be6b0f8515d6fccdc5a66afcbe1
sha1值: fcdd9659b4b46277c341bb336c730c43a2d9fcbf
sha256值: e3cd2a03014b0b67ca2dbd5c912927202085ea3e121359cfa0750f838aee63d3
sha512值: e4a8a2ca2c28293d750effacf506ccc411c6709c61ad2c78d1695c5533ec24d16557b85e599edfc83b62fdfb56671ca8e2830f3d44826b8bbd233b2758ca235f
公钥算法: rsa
密钥长度: 1024
指纹: 928aad8d9d04afa7d6b6a7f69e696c2cb131793ccea231904b722355474d5d20

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.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.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_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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.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.ACCESS_LOCATION_EXTRA_COMMANDS	正常	访问额外的位置提供程序命令	访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.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_GPS	未知	Unknown permission	Unknown permission from android reference
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.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.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_ADMIN	正常	蓝牙管理	允许应用程序发现和配对蓝牙设备。
android.permission.BLUETOOTH_CONNECT	未知	Unknown permission	Unknown permission from android reference

android.permission.BLUETOOTH_SCAN	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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.INSTALL_PACKAGES	系统需要	直接安装应用程序	允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序
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.REQUEST_DELETE_PACKAGES	正常		允许应用程序请求删除包
android.permission.KILL_BACKGROUND_PROCESSES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
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_VISUAL_USER_SELECTED	未知	Unknown permission	Unknown permission from android reference
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.vivo.notification.permission.BADGE_ICON	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
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序为可移动存储安装和卸载文件系统

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
io.dcloud.PandoraEntry	Schemes: hbuilder://, Mime Types: image/*,
io.dcloud.amtrain.GaiaSunnyAlias	Schemes: hbuilder://, Mime Types: image/*,
io.dcloud.amtrain.LianHaoAlias	Schemes: hbuilder://, Mime Types: image/*,
io.dcloud.amtrain.IBeliveAlias	Schemes: hbuilder://, Mime Types: image/*,
io.dcloud.amtrain.DefaultAlias	Schemes: hbuilder://, Mime Types: image/*,
io.dcloud.PandoraEntryActivity	Schemes: ://,