MoGua

萝莉岛 1.0.21.APK 分析报告

APP名称: 萝莉岛

包名:	com.oJSsoJ.ejbRcT
域名线索:	24条
URL线索:	18条
邮箱线索:	1条
分析日期:	2025年6月11日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: lolil-200313.apk
文件大小: 41.76MB
MD5值: 4e124dc7a0e6cba4f54169f19cec78d6
SHA1值: 2c8428e27e5ecbecc128377615af2601ba6f8081
SHA256值: 7bad4dc7f391ac8aef7ce1d545ac05b11d2b348d44ab0eacc326ae7dec78f0c1

APP 信息

App名称: 萝莉岛
包名: com.oJSsoJ.ejbRcT
主活动Activity: com.oJSsoJ.ejbRcT.MainActivity
安卓版本名称: 1.0.21
安卓版本: 21

域名线索

域名	服务器信息
issuetracker.google.com	**IP**: 142.251.211.238 **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.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
ns.adobe.com	没有服务器地理信息.
	IP: 121.36.116.8

grs.dbankcloud.cn	**所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
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.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
default.url	没有服务器地理信息.
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
metrics1.data.hicloud.com	IP: 111.202.16.252 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
aomedia.org	IP: 127.0.0.1 **所属国家**: - **地区**: -

	城市: - **纬度**: 0.000000 **经度**: 0.000000
api.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
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
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
metrics5.data.hicloud.com	**IP**: 159.138.203.215 **所属国家**: Russian Federation **地区**: Sverdlovskaya oblast' **城市**: Yekaterinburg **纬度**: 56.857498 **经度**: 60.612499
dashif.org	**IP**: 185.199.108.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
	IP: 104.18.22.19

www.w3.org	**所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
developer.apple.com	IP: 17.253.87.206 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
grs.dbankcloud.eu	没有服务器地理信息.
grs.platform.dbankcloud.ru	没有服务器地理信息.
developer.android.com	IP: 142.251.215.238 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
metrics.dt.dbankcloud.ru	IP: 159.138.204.140 **所属国家**: Russian Federation **地区**: Sverdlovskaya oblast' **城市**: Yekaterinburg **纬度**: 56.857498 **经度**: 60.612499
dartbug.com	IP: 216.239.36.21 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
	IP: 13.107.246.73

schemas.microsoft.com	**所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
metrics-dra.dt.hicloud.com	**IP**: 94.74.88.100 **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
https://)([\\s\\S]+)	com/huawei/hms/scankit/p/t3.java
http://www.example.com	com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/CustomTabsHelper.java
https://developer.android.com/guide/topics/media/issues/cleartext-not-permitted	c5/x.java
https://github.com/Baseflow/flutter-permission-handler/issues	g1/q.java
https://developer.android.com/guide/topics/media/issues/player-accessed-on-wrong-thread	g3/z0.java
https://developer.android.com/guide/topics/permissions/overview	io/flutter/plugin/platform/g.java
https://issuetracker.google.com/issues/new?component=413107&template=1096568	j0/c.java

http://dashif.org/guidelines/last-segment-number	m4/d.java
http://dashif.org/guidelines/trickmode	m4/d.java
http://dashif.org/thumbnail_tile	m4/d.java
http://dashif.org/guidelines/thumbnail_tile	m4/d.java
http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	k3/i0.java
https://x</LA_URL>	k3/h0.java
https://default.url	k3/h0.java
https://aomedia.org/emsg/ID3	a4/a.java
https://developer.apple.com/streaming/emsg-id3	a4/a.java
http://ns.adobe.com/xap/1.0/	q3/a.java
https://metrics1.data.hicloud.com:6447	摸瓜V2引擎
https://metrics-dra.dt.hicloud.com:6447	摸瓜V2引擎
https://metrics5.data.hicloud.com:6447	摸瓜V2引擎
https://metrics.dt.dbankcloud.ru	摸瓜V2引擎
https://grs.dbankcloud.com	摸瓜V2引擎
https://grs.dbankcloud.cn	摸瓜V2引擎
https://grs.dbankcloud.asia	摸瓜V2引擎
https://grs.platform.dbankcloud.ru	摸瓜V2引擎

https://grs.dbankcloud.eu	摸瓜V2引擎
https://github.com/nodeca/pica	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
https://api.flutter.dev/flutter/material/Scaffold/of.html	lib/arm64-v8a/libapp.so
http://www.unicode.org/copyright.html	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/libflutter.so

手机线索

手机号	所在文件
17512775099	i5/a.java
18222222222	r3/e.java

18222222222	r3/e.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: CN=., OU=., O=., L=Singapore, ST=Singapore, C=EN
签名算法: rsassa_pkcs1v15
有效期自: 2024-08-26 15:17:21+00:00
有效期至: 2049-08-20 15:17:21+00:00
发行人: CN=., OU=., O=., L=Singapore, ST=Singapore, C=EN
序列号: 0x1
哈希算法: sha256
md5值: 02f0ff83e8a478064c411b41277025ac
sha1值: 65047fbc6e0fb23d044a85807bd2aa3450b08c18
sha256值: 4e3d5dec98f9966e105312272bd08895fd629115b9092fa87c71b5b0c0131c94
sha512值: babc48115f848797f59816ee36500a3428c8bd04686843b7fc8415e405fc769d83671403c97fb825c7dec6f6cac7c0db5e3a1b68306ed627cb5b7d66d0380021
公钥算法: rsa
密钥长度: 2048
指纹: 06dc57feeb759ec77b083a52ba11fa8ed57e65d48e601072a59c46dedde2d976

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.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.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.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.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.ACCESS_MEDIA_LOCATION	危险	访问的任何地理位置	允许应用程序访问的任何地理位置持久保存在用户的共享集合
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.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.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.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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_BASIC_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_SMS	危险	阅读短信或彩信	允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息
android.permission.READ_PHONE_NUMBERS	危险		允许到设备的读访问的电话号码。这是 READ_PHONE_STATE 授予的功能的一个子集,但对即时应用程序公开
			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

android.permission.ACCESS_COARSE_LOCATION	危险	粗定位	用）。恶意应用程序可以使用它来确定您的大致位置
android.permission.READ_PRIVILEGED_PHONE_STATE	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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
com.oJSsoJ.ejbRcT.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信