



MoGua

萝莉岛 1.0.3.APK 分析报告



APP名称:

萝莉岛

包名:	uni.UNIFC3EFC3
域名线索:	26条
URL线索:	27条
邮箱线索:	1条
分析日期:	2025年6月3日
分析平台:	摸瓜APK反编译平台

文件名: 1.0.5.apk
文件大小: 44.2MB
MD5值: 1e97816ab075d4d342ec539fa9c7b6cc
SHA1值: 35f6734c1b7422243a52f714a0f2ebccf7143733
SHA256值: 2237e5331d1bc9ed92235ba1b41e37af51371ae63c9edc8a758c3a5aff2a49f5

i APP 信息

App名称: 萝莉岛
包名: uni.UNIFC3EFC3
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 1.0.3
安卓版本: 103

🔍 域名线索

域名	服务器信息
ns.adobe.com	没有服务器地理信息.
m3w.cn	IP: 211.93.212.129 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
raw.githubusercontent.com	IP: 0.0.0.0 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000

dag29jmgma1g.site	IP: 27.124.45.202 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
android.googleusercontent.com	IP: 74.125.197.82 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
t.me	IP: 149.154.167.99 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: Warrington 纬度: 52.184460 经度: -0.687590
example.com	IP: 93.184.215.14 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.052570 经度: -118.243904
at.alicdn.com	IP: 101.72.250.130 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
vuejs.org	IP: 54.67.4.46 所属国家: United States of America 地区: California 城市: San Jose

	纬度: 37.339390 经度: -121.894958
gac2.dcloud.net.cn	IP: 124.222.75.101 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
lame.sf.net	IP: 172.64.153.102 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
api.dankex.cn	IP: 43.142.104.214 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
er.dcloud.io	没有服务器地理信息.
service.dcloud.net.cn	IP: 124.220.57.196 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
aomedia.org	IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724

next.vuex.vuejs.org	IP: 43.202.159.188 所属国家: Korea (Republic of) 地区: Seoul-teukbyeolsi 城市: Seoul 纬度: 37.566311 经度: 126.977203
ask.dcloud.net.cn	IP: 116.196.150.176 所属国家: China 地区: Zhejiang 城市: Jinhua 纬度: 30.013470 经度: 120.288658
www.google.com	IP: 31.13.94.49 所属国家: Argentina 地区: Ciudad Autonoma de Buenos Aires 城市: Buenos Aires 纬度: -34.603600 经度: -58.381554
schemas.android.com	没有服务器地理信息.
apis.map.qq.com	IP: 116.130.224.140 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
lame.sf.net64bits	没有服务器地理信息.
er.dcloud.net.cn	IP: 43.142.57.168 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102

gac1.dcloud.net.cn	IP: 122.51.46.227 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
quilljs.com	IP: 172.66.40.163 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
www.w3.org	IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
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/hjq/permissions/AndroidManifestParser.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/35058	io/dcloud/feature/audio/AudioRecorderMgr.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/35627	io/dcloud/e/b/a.java
https://ask.dcloud.net.cn/article/35877	io/dcloud/e/b/a.java
https://er.dcloud.io/rv	io/dcloud/e/c/h/c.java
https://er.dcloud.net.cn/rv	io/dcloud/e/c/h/c.java
https://ask.dcloud.net.cn/article/283	io/dcloud/g/b.java
https://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.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/36199	摸瓜V1引擎
https://aomedia.org/emsg/ID3	摸瓜V2引擎
https://next.vuex.vuejs.org/	摸瓜V2引擎

https://vuejs.org/images/icons/favicon-96x96.png	摸瓜V2引擎
https://dag29jmgma1g.site/api/awsn.php	摸瓜V2引擎
https://t.me/luolidao001	摸瓜V2引擎
https://t.me/AdeleBlue007	摸瓜V2引擎
https://api.dankex.cn/app.html?method=	摸瓜V2引擎
https://dag29jmgma1g.site/api/	摸瓜V2引擎
https://dag29jmgma1g.site	摸瓜V2引擎
https://vuejs.org/error-reference/	摸瓜V2引擎
https://service.dcloud.net.cn/uniapp/feedback.html	摸瓜V2引擎
https://github.com/uuidjs/uuid	摸瓜V2引擎
https://apis.map.qq.com/jsapi?qt=translate&type=1&points=\$	摸瓜V2引擎
https://apis.map.qq.com/uri/v1/routeplan?type=drive&to=	摸瓜V2引擎
https://www.google.com/maps/?daddr=	摸瓜V2引擎
https://www.google.com/maps/	摸瓜V2引擎
https://quilljs.com/	摸瓜V2引擎
https://quilljs.com	摸瓜V2引擎
https://raw.githubusercontent.com/stefanpenner/es6-promise/master/LICENSE	摸瓜V2引擎

https://example.com	摸瓜V2引擎
http://schemas.android.com/apk/res/android00androidx.appcompat.widget.FitWindowsLinearLayout((androi	摸瓜V3引擎
https://ask.dcloud.net.cn/article/35627	摸瓜V3引擎
https://android.googlesource.com/toolchain/llvm	摸瓜V3引擎
http://schemas.android.com/apk/res-auto00androidx.appcompat.widget.ActionBarOverlayLayout	摸瓜V3引擎
http://schemas.android.com/apk/res/android//com.taobao.weex.ui.view.listview.WXRecyclerView	摸瓜V3引擎
https://ask.dcloud.net.cn/article/283	摸瓜V3引擎
https://er.dcloud.io/sc	摸瓜V3引擎
https://er.dcloud.net.cn/rv	摸瓜V3引擎
https://raw.githubusercontent.com/stefanpenner/es6-promise/master/LICENSE	摸瓜V3引擎
https://m3w.cn/s/	摸瓜V3引擎
https://ask.dcloud.net.cn/article/35877	摸瓜V3引擎
gac2.dcloud.net.cn	摸瓜V3引擎
http://schemas.android.com/apk/res/android	摸瓜V3引擎
http://lame.sf.net	摸瓜V3引擎
https://er.dcloud.net.cn/sc	摸瓜V3引擎
play.googleapis.com	摸瓜V3引擎
http://schemas.android.com/apk/res-auto	摸瓜V3引擎

https://ask.dcloud.net.cn/article/282	摸瓜V3引擎
https://android.googlesource.com/toolchain/clang	摸瓜V3引擎
https://at.alicdn.com/t/font_2225171_8kdcwk4po24.ttf	摸瓜V3引擎
https://er.dcloud.io/rv	摸瓜V3引擎
infinitedata-pa.googleapis.com	摸瓜V3引擎
https://android.googlesource.com/toolchain/llvm-project	摸瓜V3引擎
https://ask.dcloud.net.cn/article/35058	摸瓜V3引擎
gac1.dcloud.net.cn	摸瓜V3引擎
http://lame.sf.net64bits	摸瓜V3引擎

 邮箱线索

邮箱地址	所在文件
8@2x.png frame@2x.png frame@2x4.png 309@2x.png 308@2x.png 305@2x.png 304@2x.png frame1@2x.png frame@2x2.png frame@2x5.png frame@2x6.png	摸瓜V2引擎

frame@2x3.png 73@2x.png 72@2x.png 136@2x.png 137@2x.png 320@2x.png union@2x.png jhruby.web@gmail.com	
---	--

☰ 手机线索

手机号	所在文件
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: True
找到 1 个唯一证书
主题: C=CN, ST=, L=, O=Android, OU=Android, CN=xer018v2wRDuKyB2tOruy27ZM6nFk5QMAOJIRKbuRnflQgO57P1rXjEBa46%2Blik6IR7Hy7yJbydzzPpipAPqGg%3D%3D
签名算法: rsassa_pkcs1v15
有效期自: 2024-08-16 08:05:09+00:00
有效期至: 2124-07-23 08:05:09+00:00
发行人: C=CN, ST=, L=, O=Android, OU=Android, CN=xer018v2wRDuKyB2tOruy27ZM6nFk5QMAOJIRKbuRnflQgO57P1rXjEBa46%2Blik6IR7Hy7yJbydzzPpipAPqGg%3D%3D
序列号: 0x439bd328
哈希算法: sha256
md5值: 8e9888623100bd9e52f960ab5207abb9
sha1值: f004a73a911f7522336b9a912b436d65fd6e5a95
sha256值: 43175dba99f134f8bf73a4a3f7465e993d2598d35f2204dbdb1f49421e00ab2c
sha512值: 927f67472b8e7153b09335a6d8f1ee4c28de21574fc2f68b63bf2c8dc1642ad890b832842d4882f7ea74c24d909e88c073a57bf39db2253cfd81d42b6074b099
公钥算法: rsa
密钥长度: 2048

硬编码敏感信息

可能的敏感信息
"dcloud_common_user_refuse_api" : "the user denies access to the API"
"dcloud_io_without_authorization" : "not authorized"
"dcloud_oauth_authentication_failed" : "failed to obtain authorization to log in to the authentication service"
"dcloud_oauth_empower_failed" : "the Authentication Service operation to obtain authorized logon failed"
"dcloud_oauth_logout_tips" : "not logged in or logged out"
"dcloud_oauth_oauth_not_empower" : "oAuth authorization has not been obtained"
"dcloud_oauth_token_failed" : "failed to get token"
"dcloud_permissions_reauthorization" : "reauthorize"
"dcloud_tips_certificate" : "certificate"
"dcloud_common_user_refuse_api" : "用户拒绝该API访问"
"dcloud_io_without_authorization" : "没有获得授权"
"dcloud_oauth_authentication_failed" : "获取授权登录认证服务操作失败"
"dcloud_oauth_empower_failed" : "获取授权登录认证服务操作失败"
"dcloud_oauth_logout_tips" : "未登录或登录已注销"

"dcloud_oauth_oauth_not_empower" : "尚未获取oauth授权"
"dcloud_oauth_token_failed" : "获取token失败"
"dcloud_permissions_reauthorization" : "重新授权"
"dcloud_tips_certificate" : "证书"

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	类型	详细情况

	险		
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.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.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.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.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.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
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
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.GET_ACCOUNTS	危险	列出帐户	允许访问账户服务中的账户列表
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.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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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
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

应用内通信