Evaluation Warning: The document was created with Spire.Doc for Python.

**萝莉岛（ 1.0.3版本）
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | 萝莉岛 |
| 版本 | 1.0.3 |
| 包名 | uni.UNIFC3EFC3 |
| 域名线索 | 26条 |
| URL线索 | 27条 |
| APP图标 |  |
| 分析日期 | 2025年6月3日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | 1.0.5.apk |
| 文件大小 | 44.2MB |
| MD5值 | 1e97816ab075d4d342ec539fa9c7b6cc |
| SHA1值 | 35f6734c1b7422243a52f714a0f2ebccf7143733 |
| SHA256值 | 2237e5331d1bc9ed92235ba1b41e37af51371ae63c9edc8a758c3a5aff2a49f5 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| 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 |

## **4. 线索情况**

### **4.1 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  |
| raw.githubusercontent.com | IP: 0.0.0.0 所属国家: - 地区: - 城市: -  |
| dag29jmgma1g.site | IP: 27.124.45.202 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| android.googlesource.com | IP: 74.125.197.82 所属国家: United States of America 地区: California 城市: Mountain View  |
| 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  |
| example.com | IP: 93.184.215.14 所属国家: United States of America 地区: California 城市: Los Angeles  |
| at.alicdn.com | IP: 101.72.250.130 所属国家: China 地区: Hebei 城市: Langfang  |
| vuejs.org | IP: 54.67.4.46 所属国家: United States of America 地区: California 城市: San Jose  |
| gac2.dcloud.net.cn | IP: 124.222.75.101 所属国家: China 地区: Beijing 城市: Beijing  |
| lame.sf.net | IP: 172.64.153.102 所属国家: United States of America 地区: California 城市: San Francisco  |
| api.dankex.cn | IP: 43.142.104.214 所属国家: China 地区: Beijing 城市: Beijing  |
| 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  |
| aomedia.org | IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| next.vuex.vuejs.org | IP: 43.202.159.188 所属国家: Korea (Republic of) 地区: Seoul-teukbyeolsi 城市: Seoul  |
| ask.dcloud.net.cn | IP: 116.196.150.176 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| www.google.com | IP: 31.13.94.49 所属国家: Argentina 地区: Ciudad Autonoma de Buenos Aires 城市: Buenos Aires  |
| 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  |
| 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  |
| gac1.dcloud.net.cn | IP: 122.51.46.227 所属国家: China 地区: Beijing 城市: Beijing  |
| quilljs.com | IP: 172.66.40.163 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |

### **4.2 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  |

### **4.3 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 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  | 摸瓜V2引擎  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869184  | tv/danmaku/ijk/media/player/IjkMediaMeta.java  |

## **5. 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=xeR018v2wRDuKyB2tOruy27ZM6nFk5QMAOJIRKbuRnfIQgO57P1rXjEBa46%2BIik6IR7Hy7yJbydzzPpipAPqGg%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=xeR018v2wRDuKyB2tOruy27ZM6nFk5QMAOJIRKbuRnfIQgO57P1rXjEBa46%2BIik6IR7Hy7yJbydzzPpipAPqGg%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 指纹: 5be4c5db65c38123c66f315879b6f1687db21f795af877be42fab09e082e04c2**

## **6. 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"  |

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看  |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看  |  |  |

## **9. 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.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 |

## **10. 应用内通信**

**报告由**  [**摸瓜APK反编译平台**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**