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

**三只羊（ 1.0.0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 | 三只羊 |
| 版本 | 1.0.0 |
| 包名 | uni.UNI1A8D3EE |
| 域名线索 | 29条 |
| URL线索 | 31条 |
| APP图标 |  |
| 分析日期 | 2024年9月8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 | 170246.apk |
| 文件大小 | 45.69MB |
| MD5值 | f2f96460a94fc6cd0707c08327b31752 |
| SHA1值 | cb6368e3b8698e996605fbaf52f004bd1ff39323 |
| SHA256值 | d504f3af350b822ea1c91ff06845a53958e8f0cd66c53997c7c9424edffcf22f |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 三只羊 |
| 包名 | uni.UNI1A8D3EE |
| 主活动Activity | io.dcloud.PandoraEntry |
| 安卓版本名称 | 1.0.0 |
| 安卓版本 | 100 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| registry.npmjs.org | IP: 104.16.25.35 所属国家: United States of America 地区: California 城市: San Francisco  |
| feross.org | IP: 50.116.11.184 所属国家: United States of America 地区: California 城市: Fremont  |
| service.dcloud.net.cn | IP: 112.124.31.221 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| quilljs.com | IP: 216.24.57.253 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.openssl.org | IP: 104.71.138.221 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| api.dujin.org | IP: 183.134.17.116 所属国家: China 地区: Zhejiang 城市: Jiaojiang  |
| www.dybz.live | IP: 103.100.62.174 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| 96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com | IP: 47.93.95.208 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| apis.map.qq.com | IP: 109.244.244.109 所属国家: China 地区: Beijing 城市: Beijing  |
| clipboardjs.com | IP: 172.67.168.158 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| m3w.cn | IP: 36.102.212.110 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| shipin.ttch.xyz | 没有服务器地理信息.  |
| crbug.com | IP: 216.239.32.29 所属国家: United States of America 地区: California 城市: Mountain View  |
| github.com | IP: 20.205.243.166 所属国家: United States of America 地区: Washington 城市: Redmond  |
| ask.dcloud.net.cn | IP: 36.102.212.106 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| 127.0.0.1 | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| xinstall.top | IP: 121.199.162.178 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| test.com | 没有服务器地理信息.  |
| likeinstall.cn | IP: 121.199.65.132 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| ns.adobe.com | 没有服务器地理信息.  |
| lame.sf.net | IP: 104.18.27.198 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.google.com | IP: 108.160.167.158 所属国家: United States of America 地区: California 城市: San Francisco  |
| stream.mobihtml5.com | IP: 112.80.255.152 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| stream.dcloud.net.cn | IP: 118.31.71.109 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| schemas.android.com | 没有服务器地理信息.  |
| gwbj.tongwenkeji.com | IP: 47.110.11.29 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| fl.dyzb.online | IP: 116.0.89.230 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| www.mescroll.com | IP: 150.138.180.119 所属国家: China 地区: Shandong 城市: Qingdao  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://test.com  | org/song/videoplayer/Util.java  |
| http://127.0.0.1  | org/song/videoplayer/Util.java  |
| https://ask.dcloud.net.cn/article/35058  | io/dcloud/feature/audio/AudioRecorderMgr.java  |
| https://96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com/http/splash-screen/report  | io/dcloud/feature/gg/dcloud/ADHandler.java  |
| https://ask.dcloud.net.cn/article/287  | io/dcloud/share/IFShareApi.java  |
| http://ask.dcloud.net.cn/article/283  | io/dcloud/g/b.java  |
| http://ns.adobe.com/xap/1.0/\u0000  | io/dcloud/common/util/ExifInterface.java  |
| http://m3w.cn/s/  | io/dcloud/common/util/ShortCutUtil.java  |
| https://stream.mobihtml5.com/  | io/dcloud/common/constant/StringConst.java  |
| https://stream.dcloud.net.cn/  | io/dcloud/common/constant/StringConst.java  |
| http://ask.dcloud.net.cn/article/282  | io/dcloud/common/constant/DOMException.java  |
| https://96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com/http/rewarded-video/report?p=a&t=  | io/dcloud/e/c/h/b.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  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/GifTextView.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  |
| https://likeinstall.cn  | com/shubao/xinstall/a/e/c.java  |
| https://xinstall.top  | com/shubao/xinstall/a/e/c.java  |
| https://ask.dcloud.net.cn/article/36199  | Mogua Engine V1  |
| https://apis.map.qq.com/jsapi?qt=translate&type=1&points=  | Mogua Engine V2  |
| https://api.dujin.org/bing/1366.php  | Mogua Engine V2  |
| https://gwbj.tongwenkeji.com/html/static/play.png  | Mogua Engine V2  |
| https://service.dcloud.net.cn/uniapp/feedback.html  | Mogua Engine V2  |
| http://www.w3.org/1999/xlink  | Mogua Engine V2  |
| http://www.w3.org/2000/svg  | Mogua Engine V2  |
| http://www.w3.org/1998/Math/MathML  | Mogua Engine V2  |
| https://apis.map.qq.com/uri/v1/routeplan?type=drive&to=  | Mogua Engine V2  |
| https://www.google.com/maps/?daddr=  | Mogua Engine V2  |
| https://www.google.com/maps/  | Mogua Engine V2  |
| https://github.com/crypto-browserify/crypto-browserify  | Mogua Engine V2  |
| http://fl.dyzb.online/downApp.js  | Mogua Engine V2  |
| https://registry.npmjs.org/elliptic/-/elliptic-6.5.2.tgz  | Mogua Engine V2  |
| https://github.com/indutny/elliptic/issues  | Mogua Engine V2  |
| https://github.com/indutny/elliptic  | Mogua Engine V2  |
| http://www.mescroll.com/img/mescroll-totop.png?v=1  | Mogua Engine V2  |
| http://www.mescroll.com/img/mescroll-empty.png?v=1  | Mogua Engine V2  |
| http://fl.dyzb.online/areajm.js  | Mogua Engine V2  |
| http://shipin.ttch.xyz:9000  | Mogua Engine V2  |
| http://www.w3.org/2000/svg'></svg>  | Mogua Engine V2  |
| https://www.dybz.live  | Mogua Engine V2  |
| http://feross.org>  | Mogua Engine V2  |
| https://clipboardjs.com/  | Mogua Engine V2  |
| https://quilljs.com/  | Mogua Engine V2  |
| https://quilljs.com  | Mogua Engine V2  |
| http://shipin.ttch.xyz:9000/video/PlayUrl  | Mogua Engine V2  |
| https://crbug.com/v8/8520  | lib/x86/libweexjss.so  |
| http://lame.sf.net  | lib/x86/liblamemp3.so  |
| http://www.openssl.org/support/faq.html  | lib/x86/libijkffmpeg.so  |
| https://crbug.com/v8/8520  | lib/arm64-v8a/libweexjss.so  |
| http://lame.sf.net  | lib/arm64-v8a/liblamemp3.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| fedor@indutny.com git@github.com jhruby.web@gmail.com  | Mogua Engine V2  |
| ffmpeg-devel@ffmpeg.org  | lib/x86/libijkplayer.so  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869184  | tv/danmaku/ijk/media/player/IjkMediaMeta.java  |
| 19919152923  | Mogua Engine V2  |

## **5. 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=dyzb, ST=dyzb, L=dyzb, O=dyzb, OU=dyzb, CN=dyzb 签名算法: rsassa\_pkcs1v15 有效期自: 2022-11-07 16:17:47+00:00 有效期至: 2122-10-14 16:17:47+00:00 发行人: C=dyzb, ST=dyzb, L=dyzb, O=dyzb, OU=dyzb, CN=dyzb 序列号: 0x60f4e3fb 哈希算法: sha256 md5值: 1c4d84b5dee80f63a46bd89a79cd68f9 sha1值: 1de46ac8cb240f6c05d0118da7293b7192e0d314 sha256值: 77ea37f658980734d1f390450706aa860b74246bfcad0930410c57d6423681ce sha512值: 93002d4289730a940b0f32ae824f494e6568efbe7fc6554415b39c7e14aba952613d43f2eb037cfeed915e448ca325849afbe37de7fa896d98b4cccaeb53dc87 公钥算法: rsa 密钥长度: 2048 指纹: 6b285083b7f848d9fe88cd39e3bd1889b697f6bcf05d7c61e29097993290acb1**

## **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\_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"  |

## **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.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.CALL\_PHONE | 危险 | 直接拨打电话号码 | 允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码 |
| 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.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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| 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.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.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.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.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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.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.RECEIVE\_USER\_PRESENT | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |
| 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 |
| android.permission.SYSTEM\_ALERT\_WINDOW | 危险 | 显示系统级警报 | 允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| io.dcloud.PandoraEntry | **Schemes**: xia2d4yi6://,  |

**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。**