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

**毛片库（ 1.0.1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 | 毛片库 |
| 版本 | 1.0.1 |
| 包名 | com.TgrzM.rMdLB |
| 域名线索 | 14条 |
| URL线索 | 12条 |
| APP图标 |  |
| 分析日期 | 2025年6月15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 | newmpk250611\_newmpkpro\_20250610\_1.0.1 01.apk |
| 文件大小 | 19.98MB |
| MD5值 | a8a355906691e8a291cf62795e11ba9e |
| SHA1值 | 646b909ba51cde1db05571e94a2da48c910c32a3 |
| SHA256值 | 637dad89f22aec59d095e21cc447171601a38170275f105c97dca6e025f615f8 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 毛片库 |
| 包名 | com.TgrzM.rMdLB |
| 主活动Activity | io.dcloud.PandoraEntry |
| 安卓版本名称 | 1.0.1 |
| 安卓版本 | 100 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| d2daq4vgbv2z7v.cloudfront.net | IP: 18.65.214.157 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| quilljs.com | IP: 172.66.43.93 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.google.com | IP: 199.59.148.229 所属国家: United States of America 地区: California 城市: San Francisco  |
| dsddwg3dw16m0.cloudfront.net | IP: 13.225.175.91 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| lame.sf.net | IP: 104.18.20.237 所属国家: United States of America 地区: California 城市: San Francisco  |
| d2e8n3l1gjaqgi.cloudfront.net | IP: 13.35.226.78 所属国家: India 地区: Telangana 城市: Hyderabad  |
| d1k8zjfla25adt.cloudfront.net | IP: 3.166.243.143 所属国家: United States of America 地区: Washington 城市: Seattle  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| ns.adobe.com | 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: Singapore 地区: Singapore 城市: Singapore  |
| apis.map.qq.com | IP: 116.130.223.114 所属国家: China 地区: Beijing 城市: Beijing  |
| ask.dcloud.net.cn | IP: 220.194.123.111 所属国家: China 地区: Tianjin 城市: Tianjin  |
| service.dcloud.net.cn | IP: 110.40.181.119 所属国家: China 地区: Beijing 城市: Beijing  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://ask.dcloud.net.cn/article/36199  | 摸瓜V1引擎  |
| https://quilljs.com/  | 摸瓜V2引擎  |
| https://quilljs.com  | 摸瓜V2引擎  |
| https://apis.map.qq.com/jsapi?qt=translate&type=1&points=  | 摸瓜V2引擎  |
| https://d2daq4vgbv2z7v.cloudfront.net  | 摸瓜V2引擎  |
| https://d2e8n3l1gjaqgi.cloudfront.net  | 摸瓜V2引擎  |
| https://d1k8zjfla25adt.cloudfront.net  | 摸瓜V2引擎  |
| https://dsddwg3dw16m0.cloudfront.net  | 摸瓜V2引擎  |
| https://github.com/facebook/regenerator/blob/main/LICENSE  | 摸瓜V2引擎  |
| https://service.dcloud.net.cn/uniapp/feedback.html  | 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  |
| http://ns.adobe.com/xap/1.0/  | lib/armeabi-v7a/libstatic-webp.so  |
| http://lame.sf.net  | lib/armeabi-v7a/liblamemp3.so  |
| http://ns.adobe.com/xap/1.0/  | lib/armeabi-v7a/libnative-imagetranscoder.so  |
| https://crbug.com/v8/8520  | lib/armeabi-v7a/libweexjss.so  |
| http://lame.sf.net  | lib/arm64-v8a/liblamemp3.so  |
| https://crbug.com/v8/8520  | lib/arm64-v8a/libweexjss.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| jhruby.web@gmail.com  | 摸瓜V2引擎  |

### **4.4 手机号线索**

## **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='中国', ST='北京', L='北京', O='北京', OU='北京', CN='中国' 签名算法: rsassa\_pkcs1v15 有效期自: 2025-06-11 01:00:25+00:00 有效期至: 2035-06-09 01:00:25+00:00 发行人: C='中国', ST='北京', L='北京', O='北京', OU='北京', CN='中国' 序列号: 0x51b0d22c 哈希算法: sha256 md5值: b44f1dcd2f32f8d7e4bd198ec30d23ff sha1值: ba85d1119bae6e4661918402f3a8dbd4b943b677 sha256值: 07c8ba8ebe70446a84fca027d75905dd68cf26be54c67891c574ba6e2492de27 sha512值: e1959c803660acc2cc3fd1815a8ae458912b90e3c7b95d17e82826cb3343d2c7fc03c46440d6617f3ee12fd73e7f991903283bfab83e8533f8450174997ff144 公钥算法: rsa 密钥长度: 2048 指纹: 76ec9e9721c6205c39b260e96d4dd00ea9a66fb4f75753cf8b751b4617ae0a0f**

## **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.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.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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |
| 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.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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |

## **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。**