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

**蜗牛云盘（ 2.1.7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 | 蜗牛云盘 |
| 版本 | 2.1.7 |
| 包名 | com.fjgd.ldcard |
| 域名线索 | 26条 |
| URL线索 | 14条 |
| APP图标 |  |
| 分析日期 | 2024年10月17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 | base(1).apk |
| 文件大小 | 69.58MB |
| MD5值 | 0484e6b702858a4022dd8978a30185bf |
| SHA1值 | 01f2e764d4b5062a52928bd677eacd2e29b8a66f |
| SHA256值 | e0b4f31d7c4b955411152cf5777dabcbcbe5191ff8ab91da6f842b63a85abd2b |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 蜗牛云盘 |
| 包名 | com.fjgd.ldcard |
| 主活动Activity | com.fjgd.ldcard.login.LoginActivity |
| 安卓版本名称 | 2.1.7 |
| 安卓版本 | 2 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| api.aliyundrive.com | IP: 49.7.149.106 所属国家: China 地区: Beijing 城市: Beijing  |
| api.assrt.net | IP: 43.155.72.46 所属国家: China 地区: Beijing 城市: Beijing  |
| www.aliyundrive.com | IP: 106.38.180.43 所属国家: China 地区: Beijing 城市: Beijing  |
| jsoup.org | IP: 172.67.132.26 所属国家: United States of America 地区: California 城市: San Francisco  |
| lame.sf.net | IP: 104.18.27.198 所属国家: United States of America 地区: California 城市: San Francisco  |
| 81.69.231.222 | IP: 81.69.231.222 所属国家: China 地区: Beijing 城市: Beijing  |
| musicbrainz.org | IP: 138.201.227.205 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main  |
| secure.assrt.net | IP: 132.145.91.175 所属国家: Korea (Republic of) 地区: Seoul-teukbyeolsi 城市: Seoul  |
| www.shoutcast.coms | 没有服务器地理信息.  |
| www.tvdr.de | IP: 88.198.76.220 所属国家: Germany 地区: Bayern 城市: Nuremberg  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.satip.info | IP: 35.214.201.169 所属国家: Netherlands 地区: Groningen 城市: Groningen  |
| xml.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| openapi.aliyundrive.com | IP: 101.201.69.253 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| assrt.net | IP: 43.155.72.46 所属国家: China 地区: Beijing 城市: Beijing  |
| auth.aliyundrive.com | IP: 49.7.63.220 所属国家: China 地区: Beijing 城市: Beijing  |
| www.shoutcast.com | IP: 13.70.37.114 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| www.videolan.org | IP: 213.36.253.2 所属国家: France 地区: Ile-de-France 城市: Paris  |
| relaxng.org | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| ns.adobe.com | 没有服务器地理信息.  |
| shop.mengchaxun.com | IP: 175.178.23.71 所属国家: China 地区: Beijing 城市: Beijing  |
| fingerprint.videolan.org | IP: 213.36.253.2 所属国家: France 地区: Ile-de-France 城市: Paris  |
| asr.cloud.tencent.com | IP: 159.75.141.192 所属国家: China 地区: Beijing 城市: Beijing  |
| www.icecast.org | IP: 140.211.166.31 所属国家: United States of America 地区: Oregon 城市: Eugene  |
| www.twolame.org | IP: 93.93.131.3 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: Cambridge  |
| www.oasis-open.org | IP: 172.99.100.168 所属国家: United States of America 地区: Texas 城市: Windcrest  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://'  | org/jsoup/helper/HttpConnection.java  |
| https://'.  | org/jsoup/helper/HttpConnection.java  |
| https://jsoup.org/cookbook/extracting-data/working-with-urls  | org/jsoup/helper/HttpConnection.java  |
| http://undefined/  | org/jsoup/helper/HttpConnection.java  |
| http://xml.apache.org/xslt  | com/elvishew/xlog/formatter/message/xml/DefaultXmlFormatter.java  |
| http://81.69.231.222:8080/api/woniu/checkUpdate  | com/fjgd/ldcard/util/UpdateUtils.java  |
| https://www.aliyundrive.com/drive  | com/fjgd/ldcard/util/RequestConfig.java  |
| https://shop.mengchaxun.com/woniu/product  | com/fjgd/ldcard/pad/PadMainActivity.java  |
| https://api.aliyundrive.com/v2/batch?jsonmask=responses(id%2Cstatus%2Cbody(next\_marker%2Ctotal\_count%2Citems(name%2Cfile\_id%2Cdrive\_id%2Cupdated\_at%2Csize%2Cdescription%2Cparent\_file\_id)))  | com/fjgd/ldcard/net/GetFoldersThread.java  |
| https://api.aliyundrive.com/v2/batch?jsonmask=responses(id%2Cstatus%2Cbody(total\_count%2Citems(file\_id%2Cname%2Cparent\_file\_id)))  | com/fjgd/ldcard/net/GetFoldersThread.java  |
| https://api.aliyundrive.com/v2/batch  | com/fjgd/ldcard/net/GetFoldersThread.java  |
| https://openapi.aliyundrive.com/  | com/fjgd/ldcard/net/AliApiUtils.java  |
| http://81.69.231.222:8080/api/woniu/loginByCode  | com/fjgd/ldcard/net/AliApiUtils.java  |
| http://81.69.231.222:8080/api/woniu/refreshToken  | com/fjgd/ldcard/net/AliApiUtils.java  |
| http://81.69.231.222:8080/api/woniu/getQrcode  | com/fjgd/ldcard/net/AliApiUtils.java  |
| https://api.aliyundrive.com/v2/batch?jsonmask=responses(id%2Cstatus%2Cbody(next\_marker%2Ctotal\_count%2Citems(punish\_flag%2Cname%2Cfile\_id%2Cdrive\_id%2Cupdated\_at%2Csize%2Cdescription%2Cparent\_file\_id)))  | com/fjgd/ldcard/net/GetWeiguiThread.java  |
| http://assrt.net/sub/?searchword=  | com/fjgd/ldcard/net/ShooterUtils.java  |
| http://assrt.net  | com/fjgd/ldcard/net/ShooterUtils.java  |
| https://api.assrt.net/v1/sub/search?token=  | com/fjgd/ldcard/net/ShooterUtils.java  |
| http://assrt.net/download/  | com/fjgd/ldcard/net/ShooterUtils.java  |
| http://assrt.net/  | com/fjgd/ldcard/net/ShooterUtils.java  |
| https://api.assrt.net/v1/sub/detail?token=  | com/fjgd/ldcard/net/ShooterUtils.java  |
| http://81.69.231.222:8080/api/woniu/getShooterToken?userId=  | com/fjgd/ldcard/net/ShooterUtils.java  |
| http://81.69.231.222:8080/api/woniu/updateShooterToken  | com/fjgd/ldcard/net/ShooterUtils.java  |
| https://secure.assrt.net/user/logon.xml  | com/fjgd/ldcard/net/ShooterUtils.java  |
| http://81.69.231.222:8080/api/woniu/listUser?page=  | com/fjgd/ldcard/net/TestCase.java  |
| https://auth.aliyundrive.com/v2/account/token  | com/fjgd/ldcard/net/AliUtils.java  |
| https://api.aliyundrive.com/v2/file/get\_video\_preview\_play\_info  | com/fjgd/ldcard/net/AliUtils.java  |
| https://api.aliyundrive.com/v2/databox/get\_audio\_play\_info  | com/fjgd/ldcard/net/AliUtils.java  |
| https://api.aliyundrive.com/adrive/v3/file/search?jsonmask=next\_marker,items(updated\_at,thumbnail,url,punish\_flag,size,category,drive\_id,file\_extension,file\_id,name,parent\_file\_id,type)  | com/fjgd/ldcard/net/AliUtils.java  |
| https://api.aliyundrive.com/v2/batch?jsonmask=responses(id,status,body(next\_marker,total\_count,items(updated\_at,thumbnail,url,punish\_flag,size,category,drive\_id,file\_extension,file\_id,name,parent\_file\_id,type)))  | com/fjgd/ldcard/net/AliUtils.java  |
| https://api.aliyundrive.com/adrive/v3/file/list?jsonmask=next\_marker,items(updated\_at,thumbnail,punish\_flag,url,size,file\_extension,category,drive\_id,file\_id,name,parent\_file\_id,type)  | com/fjgd/ldcard/net/AliUtils.java  |
| https://api.aliyundrive.com/adrive/v1/file/get\_path  | com/fjgd/ldcard/net/AliUtils.java  |
| https://api.aliyundrive.com/v2/file/get\_download\_url  | com/fjgd/ldcard/net/AliUtils.java  |
| https://api.aliyundrive.com/v2/file/get\_office\_preview\_url  | com/fjgd/ldcard/net/AliUtils.java  |
| https://api.aliyundrive.com/adrive/v1/user/albums\_info  | com/fjgd/ldcard/net/AliUtils.java  |
| https://api.aliyundrive.com/adrive/v1/file/get\_folder\_size\_info  | com/fjgd/ldcard/net/AliUtils.java  |
| https://api.aliyundrive.com/adrive/v1/file/duplicateList  | com/fjgd/ldcard/net/AliUtils.java  |
| https://api.aliyundrive.com/v2/batch  | com/fjgd/ldcard/net/AliUtils.java  |
| https://api.aliyundrive.com/adrive/v2/share\_link/create  | com/fjgd/ldcard/net/AliUtils.java  |
| https://api.aliyundrive.com/adrive/v2/share\_link/cancel  | com/fjgd/ldcard/net/AliUtils.java  |
| https://api.aliyundrive.com/adrive/v3/share\_link/list  | com/fjgd/ldcard/net/AliUtils.java  |
| https://api.aliyundrive.com/v2/share\_link/get\_share\_token  | com/fjgd/ldcard/net/AliUtils.java  |
| https://api.aliyundrive.com/v2/recyclebin/clear  | com/fjgd/ldcard/net/AliUtils.java  |
| https://api.aliyundrive.com/v2/async\_task/get  | com/fjgd/ldcard/net/AliUtils.java  |
| https://api.aliyundrive.com/adrive/v3/file/list  | com/fjgd/ldcard/net/AliUtils.java  |
| https://api.aliyundrive.com/users/v1/users/device\_list  | com/fjgd/ldcard/net/AliUtils.java  |
| https://www.aliyundrive.com/drive  | com/fjgd/vlc/VLCOptions.java  |
| https://asr.cloud.tencent.com/server\_time  | com/tencent/aai/task/net/networktime/QCloudServiceTimeClient.java  |
| http://%s%s%s  | lib/arm64-v8a/libvlc.so  |
| http://www.tvdr.de/).  | lib/arm64-v8a/libvlc.so  |
| http://www.satip.info/Playlists/%s.m3u  | lib/arm64-v8a/libvlc.so  |
| http://www.w3.org/ns/ttml  | lib/arm64-v8a/libvlc.so  |
| http://www.w3.org/2004/11/ttaf1  | lib/arm64-v8a/libvlc.so  |
| http://www.w3.org/2006/04/ttaf1  | lib/arm64-v8a/libvlc.so  |
| http://www.w3.org/2006/10/ttaf1  | lib/arm64-v8a/libvlc.so  |
| http://ns.adobe.com/xap/1.0/  | lib/arm64-v8a/libvlc.so  |
| http://%s:%d  | lib/arm64-v8a/libvlc.so  |
| http://www.w3.org/1999/xhtml  | lib/arm64-v8a/libvlc.so  |
| http://www.videolan.org/vlc  | lib/arm64-v8a/libvlc.so  |
| http://%s%s  | lib/arm64-v8a/libvlc.so  |
| http://%s:%d%s  | lib/arm64-v8a/libvlc.so  |
| https://fingerprint.videolan.org/acoustid.php?meta=recordings+tracks+usermeta+releases&duration=%d&fingerprint=%s  | lib/arm64-v8a/libvlc.so  |
| http://location  | lib/arm64-v8a/libvlc.so  |
| http://musicbrainz.org  | lib/arm64-v8a/libvlc.so  |
| http://www.shoutcast.com/sbin/newxml.phtml?genre=%s  | lib/arm64-v8a/libvlc.so  |
| http://www.shoutcast.com/sbin/tunein-tvstation.pls?id=%s  | lib/arm64-v8a/libvlc.so  |
| http://www.shoutcast.com%s?id=%s  | lib/arm64-v8a/libvlc.so  |
| http://www.videolan.org/vlc/playlist/0  | lib/arm64-v8a/libvlc.so  |
| http://%s:8008%s  | lib/arm64-v8a/libvlc.so  |
| http://lame.sf.net  | lib/arm64-v8a/libvlc.so  |
| http://www.w3.org/XML/1998/namespace  | lib/arm64-v8a/libvlc.so  |
| http://www.w3.org/2000/xmlns/  | lib/arm64-v8a/libvlc.so  |
| http://www.w3.org/TR/REC-html40/loose.dtd  | lib/arm64-v8a/libvlc.so  |
| http://www.w3.org/2002/08/xquery-functions  | lib/arm64-v8a/libvlc.so  |
| http://www.oasis-open.org/committees/entity/release/1.0/catalog.dtd  | lib/arm64-v8a/libvlc.so  |
| http://www.w3.org/2001/XMLSchema  | lib/arm64-v8a/libvlc.so  |
| http://www.w3.org/2003/XInclude  | lib/arm64-v8a/libvlc.so  |
| http://www.w3.org/2001/XInclude  | lib/arm64-v8a/libvlc.so  |
| http://www.w3.org/2001/XMLSchema-datatypes  | lib/arm64-v8a/libvlc.so  |
| http://relaxng.org/ns/structure/1.0  | lib/arm64-v8a/libvlc.so  |
| http://www.w3.org/2000/xmlns  | lib/arm64-v8a/libvlc.so  |
| http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd  | lib/arm64-v8a/libvlc.so  |
| http://www.w3.org/TR/xhtml1/DTD/xhtml1-frameset.dtd  | lib/arm64-v8a/libvlc.so  |
| http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd  | lib/arm64-v8a/libvlc.so  |
| http://www.w3.org/2001/XMLSchema-instance  | lib/arm64-v8a/libvlc.so  |
| http://[  | lib/arm64-v8a/libvlc.so  |
| http://www.icecast.org/  | lib/arm64-v8a/libvlc.so  |
| http://www.twolame.org/  | lib/arm64-v8a/libvlc.so  |
| http://www.videolan.org/x264.html  | lib/arm64-v8a/libvlc.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| sam@zoy.org libdvbpsi-devel@videolan.org fsync@openssh.com fstatvfs@openssh.com a2-nistp256-cert-v01@openssh.com a2-nistp384-cert-v01@openssh.com a2-nistp521-cert-v01@openssh.com keepalive@libssh2.orgw auth-agent-req@openssh.com rijndael-cbc@lysator.liu hmac-ripemd160@openssh.com zlib@openssh.com twolame-discuss@lists.sourceforg  | lib/arm64-v8a/libvlc.so  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 15897600000  | com/ibm/icu/impl/TimeZoneGenericNames.java  |
| 14389071831  | lib/arm64-v8a/libvlc.so  |

## **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: CN=dxr 签名算法: rsassa\_pkcs1v15 有效期自: 2022-11-17 11:05:37+00:00 有效期至: 3021-03-20 11:05:37+00:00 发行人: CN=dxr 序列号: 0x25c97b5c 哈希算法: sha256 md5值: 5e84d48b1c55d587f71c95a2f9065820 sha1值: 019ffba4777547621d5be7de89e48969b311d84b sha256值: af6fcf5d14ae95a63a578c8fca0b6bc6e22767f74ca79fddfd47f125dec39b13 sha512值: b8d1443cb36a0e2faa67939506ac2a32b6ce042c4c376102441af9c73dc22c742a170e8b398b9bc02fc14357c0741931af5ad2b551038b6838029e7bf0e8c288 公钥算法: rsa 密钥长度: 2048 指纹: c77b9e645c157c95d6dded2951bcb1613ef764432eff5607136545d90300ff2f**

## **6. 硬编码敏感信息**

## **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.HDMI\_CEC | 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 |
| android.permission.SYSTEM\_OVERLAY\_WINDOW | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.STOP\_APP\_SWITCHES | 合法 | 防止应用程序切换 | 防止用户切换到另一个应用程序 |
| 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.SCHEDULE\_EXACT\_ALARM | 正常 |  | 允许应用程序使用精确的警报调度 API 来执行对时间敏感的后台工作 |
| android.hardware.usb.host | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.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.CHANGE\_CONFIGURATION | 系统需要 | 更改您的 UI 设置 | 允许应用程序更改当前配置,例如语言环境或整体字体大小 |
| 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\_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.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.MANAGE\_EXTERNAL\_STORAGE | 危险 | 允许应用程序广泛访问范围存储中的外部存储 | 允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用 |
| android.permission.READ\_MEDIA\_IMAGES | 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.READ\_MEDIA\_VIDEO | 未知 | Unknown permission | Unknown permission from android reference |
| 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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| com.fjgd.ldcard.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 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。**