# MoGua

# video virtual camera 2.0.40.APK 分析报告

APP名称: video virtual camera

| | |
|---|---|
| 包名: | com.telegram.a1064 |
| 域名线索: | 4条 |
| URL线索: | 3条 |
| 邮箱线索: | 0条 |
| 分析日期: | 2025年6月26日 |
| 分析平台: | 摸瓜APK反编译平台 |

## 文件信息

**文件名**: 虚拟视频相机10.11.13.apk
**文件大小**: 19.83MB
**MD5值**: d72daa9848ddac3cf5d714d85e3d7575
**SHA1值**: 24c846e5f71cf9959eed08870d317f4ede113645
**SHA256值**: f9b3e3ec97acf7b718df0ba35786724e0fab3b0632eb65ac7d9cb316d9d4bf78

# APP 信息

**App名称**: video virtual camera
**包名**: com.telegram.a1064
**主活动Activity**: com.nvshen.chmp4.SplashActivity
**安卓版本名称**: 2.0.40
**安卓版本**: 20329

# 域名线索

| 域名 | 服务器信息 |
| --- | --- |
| journeyapps.com | **IP**: 18.65.168.90<br>**所属国家**: Japan<br>**地区**: Tokyo<br>**城市**: Tokyo<br>**纬度**: 35.689499<br>**经度**: 139.692322 |
| schemas.android.com | 没有服务器地理信息. |
| github.com | **IP**: 20.205.243.166<br>**所属国家**: Singapore<br>**地区**: Singapore<br>**城市**: Singapore<br>**纬度**: 1.289987<br>**经度**: 103.850281 |

| | |
|---|---|
| oopo.top | **IP**: 23.145.248.117<br>**所属国家**: United States of America<br>**地区**: Colorado<br>**城市**: Denver<br>**纬度**: 39.705940<br>**经度**: -104.960487 |

# URL线索

| URL信息 | Url所在文件 |
|---|---|
| https://oopo.top | com/nvshen/chmp4/d.java |
| http://schemas.android.com/apk/res/android | j2/b.java |
| https://journeyapps.com/ | 摸瓜V1引擎 |
| https://github.com/journeyapps/zxing-android-embedded | 摸瓜V1引擎 |

# 邮箱线索

# 手机线索

# 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=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
签名算法: rsassa_pkcs1v15
有效期自: 2008-02-29 01:33:46+00:00
有效期至: 2035-07-17 01:33:46+00:00
发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
序列号: 0x936eacbe07f201df
哈希算法: sha1
md5值: e89b158e4bcf988ebd09eb83f5378e87
sha1值: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81
sha256值: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
sha512值: 5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea303977272d17958704d89b7711292a4569
公钥算法: rsa
密钥长度: 2048
指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75

# 硬编码敏感信息

| 可能的敏感信息 |
| --- |
| "input_cdkey" : "please input cdkey" |
| "library_zxingandroidembedded_author" : "JourneyApps" |
| "library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/" |
| "input_cdkey" : "请输入激活码" |

# 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 | 是否危险 | 类型 | 详细情况 |
| --- | --- | --- | --- |
| 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.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.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.READ_MEDIA_VIDEO | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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 |

# 应用内通信

---