



# MoGua

## 香蕉圈短視頻 1.1.6.APK 分析報告



APP名称:

香蕉圈短視頻

|        |                            |
|--------|----------------------------|
| 包名:    | com.nineone.xjqd           |
| 域名线索:  | 6条                         |
| URL线索: | 3条                         |
| 邮箱线索:  | 0条                         |
| 分析日期:  | 2025年6月18日                 |
| 分析平台:  | <a href="#">摸瓜APK反编译平台</a> |

文件名: xjqd116192.apk  
文件大小: 22.1MB  
MD5值: cf751b244afb24d809874634851ad347  
SHA1值: 0d4e613225ae97d67a798fda4cf9d55735d07513  
SHA256值: 40dd2bbb7f3a32c064f4f88aaea611ae48bfe770208c5bff95f1fb7cc76d7be4

# i APP 信息

App名称: 香蕉圈短視頻  
包名: com.nineone.xjqd  
主活动Activity: com.nineone.xjqd.MainActivity  
安卓版本名称: 1.1.6  
安卓版本: 19

## 🔍 域名线索

| 域名                    | 服务器信息                                                                                                                          |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------|
| 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                      |
| reg.peoplexjq0611.xyz | IP: 172.67.134.39<br>所属国家: United States of America<br>地区: California<br>城市: San Francisco<br>纬度: 37.775700<br>经度: -122.395203 |
| reg.huaweixjq0611.com | IP: 34.92.44.128<br>所属国家: Hong Kong<br>地区: Hong Kong                                                                           |

|                      |                                                                                                          |
|----------------------|----------------------------------------------------------------------------------------------------------|
|                      | 城市: Hong Kong<br>纬度: 22.285521<br>经度: 114.157692                                                         |
| reg.maticxjq0611.xyz | IP: 34.92.44.128<br>所属国家: Hong Kong<br>地区: Hong Kong<br>城市: Hong Kong<br>纬度: 22.285521<br>经度: 114.157692 |
| up.logupload0611.com | IP: 34.92.82.239<br>所属国家: Hong Kong<br>地区: Hong Kong<br>城市: Hong Kong<br>纬度: 22.285521<br>经度: 114.157692 |
| reg.ethxjq0611.com   | IP: 34.92.44.128<br>所属国家: Hong Kong<br>地区: Hong Kong<br>城市: Hong Kong<br>纬度: 22.285521<br>经度: 114.157692 |

 URL线索

| URL信息                                                     | Url所在文件                                               |
|-----------------------------------------------------------|-------------------------------------------------------|
| https://github.com/azureaicat/cateatfish/blob/main/eating | com/nineone/xjqd/ServerRequest/InitServerConnect.java |
| https://reg.ethxjq0611.com/device/register                | com/nineone/xjqd/ServerRequest/InitServerConnect.java |
| https://reg.huaweixjq0611.com/device/register             | com/nineone/xjqd/ServerRequest/InitServerConnect.java |
|                                                           |                                                       |

|                                                 |                                                       |
|-------------------------------------------------|-------------------------------------------------------|
| https://reg.maticxjq0611.xyz/device/register    | com/nineone/xjqd/ServerRequest/InitServerConnect.java |
| https://reg.peoplexjq0611.xyz/device/register   | com/nineone/xjqd/ServerRequest/InitServerConnect.java |
| https://up.logupload0611.com/app/log/raw/report | com/nineone/xjqd/ServerRequest/InitServerConnect.java |

## 邮箱线索

## 手机线索

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

## 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=vm, ST=q, L=xj, O=nineone, OU=nineone, CN=xjq

签名算法: rsassa\_pkcs1v15

有效期自: 2021-03-22 04:08:08+00:00

有效期至: 2048-08-07 04:08:08+00:00

发行人: C=vm, ST=q, L=xj, O=nineone, OU=nineone, CN=xjq

序列号: 0x1444aadd

哈希算法: sha256

md5值: 9191d0d0d4f221a4ea40700603d9bec0

sha1值: 4774aea8a935e4dc842c96db983d496774021431

sha256值: b7064fa99c0cc1fa18bec1743acab4261a425c97ffebb2a52304ba76fe252fe7

sha512值: cb804a2d09a24cda5bbac47e999511d2c24a654de8e07a9befd562956544991b1cebf7de1d86e8f6a27cfb3c5cbbee9a42299a38035b38d8347d46b6c49a6666

公钥算法: rsa  
密钥长度: 2048  
指纹: 0c14f520bb76c4586dcb1c7d20ce7777b5301650f31c8c0203c5035bbc909516

## 硬编码敏感信息

## 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.INTERNET | 正常   | 互联网接入 | 允许应用程序创建网络套接字 |

|                                             |    |                    |                                                               |
|---------------------------------------------|----|--------------------|---------------------------------------------------------------|
| 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_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.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.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.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.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                                        |
| com.nineone.xjqd.permission.C2D_MESSAGE     | 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.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.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.RECORD_AUDIO             | 危险 | 录音                 | 允许应用程序访问音频记录路径                                                |
| 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.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                      |
|                                             |    |                    |                                                               |

|                                                       |    |                    |                                           |
|-------------------------------------------------------|----|--------------------|-------------------------------------------|
| com.android.vending.CHECK_LICENSE                     | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.c2dm.permission.RECEIVE            | 合法 | C2DM 权限            | 云到设备消息传递的权限                               |
| com.sec.android.provider.badge.permission.READ        | 正常 | 在应用程序上显示通知计数       | 在三星手机的应用程序启动图标上显示通知计数或徽章。                 |
| com.sec.android.provider.badge.permission.WRITE       | 正常 | 在应用程序上显示通知计数       | 在三星手机的应用程序启动图标上显示通知计数或徽章。                 |
| com.htc.launcher.permission.READ_SETTINGS             | 正常 | 在应用程序上显示通知计数       | 在 htc 手机的应用程序启动图标上显示通知计数或徽章。              |
| com.htc.launcher.permission.UPDATE_SHORTCUT           | 正常 | 在应用程序上显示通知计数       | 在 htc 手机的应用程序启动图标上显示通知计数或徽章。              |
| com.sonyericsson.home.permission.BROADCAST_BADGE      | 正常 | 在应用程序上显示通知计数       | 在索尼手机的应用程序启动图标上显示通知计数或徽章。                 |
| com.sonymobile.home.permission.PROVIDER_INSERT_BADGE  | 正常 | 在应用程序上显示通知计数       | 在索尼手机的应用程序启动图标上显示通知计数或徽章。                 |
| com.anddoes.launcher.permission.UPDATE_COUNT          | 正常 | 在应用程序上显示通知计数       | 在应用程序启动图标上显示通知计数或徽章                       |
| com.majeur.launcher.permission.UPDATE_BADGE           | 正常 | 在应用程序上显示通知计数       | 在应用程序启动图标上显示通知计数或标记为固体。                   |
| 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.huawei.android.launcher.permission.READ_SETTINGS  | 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.huawei.android.launcher.permission.WRITE_SETTINGS | 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                  |



## 应用内通信

| 活动(ACTIVITY)                  | 通信(INTENT)          |
|-------------------------------|---------------------|
| com.nineone.xjqd.MainActivity | Schemes: m3eiss://, |

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