



## 蘑菇视频 1.0.3.APK 分析报告



APP名称:

蘑菇视频

|        |                            |
|--------|----------------------------|
| 包名:    | syhdr.kgkwzt.dtgou         |
| 域名线索:  | 20条                        |
| URL线索: | 18条                        |
| 邮箱线索:  | 3条                         |
| 分析日期:  | 2025年6月14日                 |
| 分析平台:  | <a href="#">摸瓜APK反编译平台</a> |

文件名: ndlp7988-20250610-v226-2.apk  
文件大小: 25.4MB  
MD5值: 66ee1d190bbb0ac53b7c04bd8b6b603c  
SHA1值: bfd12ba523c523c0a7d5c404591bb864bf4ae6fd  
SHA256值: 781999cd5151defa4ac99b49354884580b0c825b68b85df0067bd617272e9320

## i APP 信息

App名称: 蘑菇视频  
包名: syhdr.kgkwzt.dtgou  
主活动Activity: syhdr.kgkwzt.dtgou.MainActivity  
安卓版本名称: 1.0.3  
安卓版本: 4

## 🔍 域名线索

| 域名                      | 服务器信息                                                                                                                           |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| developer.mozilla.org   | IP: 34.111.97.67<br>所属国家: United States of America<br>地区: Missouri<br>城市: Kansas City<br>纬度: 39.099731<br>经度: -94.578568        |
| issuetracker.google.com | IP: 142.250.217.78<br>所属国家: United States of America<br>地区: California<br>城市: Mountain View<br>纬度: 37.405991<br>经度: -122.078514 |
| dashif.org              | IP: 185.199.108.153<br>所属国家: United States of America<br>地区: Pennsylvania                                                       |

|                       |                                                                                                                                                                           |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <b>城市:</b> California<br><b>纬度:</b> 40.065647<br><b>经度:</b> -79.891724                                                                                                    |
| docs.flutter.dev      | <b>IP:</b> 199.36.158.100<br><b>所属国家:</b> United States of America<br><b>地区:</b> California<br><b>城市:</b> Mountain View<br><b>纬度:</b> 37.405991<br><b>经度:</b> -122.078514 |
| github.com            | <b>IP:</b> 20.205.243.166<br><b>所属国家:</b> Singapore<br><b>地区:</b> Singapore<br><b>城市:</b> Singapore<br><b>纬度:</b> 1.289987<br><b>经度:</b> 103.850281                       |
| default.url           | 没有服务器地理信息.                                                                                                                                                                |
| developer.apple.com   | <b>IP:</b> 2.18.190.104<br><b>所属国家:</b> Singapore<br><b>地区:</b> Singapore<br><b>城市:</b> Singapore<br><b>纬度:</b> 1.289987<br><b>经度:</b> 103.850281                         |
| schemas.microsoft.com | <b>IP:</b> 13.107.253.39<br><b>所属国家:</b> Germany<br><b>地区:</b> Hessen<br><b>城市:</b> Frankfurt am Main<br><b>纬度:</b> 50.110882<br><b>经度:</b> 8.681996                      |
| www.w3.org            | <b>IP:</b> 104.18.22.19<br><b>所属国家:</b> United States of America<br><b>地区:</b> California<br><b>城市:</b> San Francisco<br><b>纬度:</b> 37.775700                             |

|                       |                                                                                                                                  |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------|
|                       | 经度: -122.395203                                                                                                                  |
| ns.adobe.com          | 没有服务器地理信息.                                                                                                                       |
| developer.android.com | IP: 142.251.215.238<br>所属国家: United States of America<br>地区: California<br>城市: Mountain View<br>纬度: 37.405991<br>经度: -122.078514 |
| journeyapps.com       | IP: 13.35.37.37<br>所属国家: Taiwan (Province of China)<br>地区: Taipei<br>城市: Taipei<br>纬度: 25.038172<br>经度: 121.563599               |
| api.flutter.dev       | IP: 199.36.158.100<br>所属国家: United States of America<br>地区: California<br>城市: Mountain View<br>纬度: 37.405991<br>经度: -122.078514  |
| www.ibm.com           | IP: 23.1.167.82<br>所属国家: Japan<br>地区: Osaka<br>城市: Ibaraki<br>纬度: 34.816425<br>经度: 135.568909                                    |
| flutter.dev           | IP: 199.36.158.100<br>所属国家: United States of America<br>地区: California<br>城市: Mountain View<br>纬度: 37.405991<br>经度: -122.078514  |
|                       |                                                                                                                                  |

|                 |                                                                                                                                  |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------|
| r9nhvkt.vip     | IP: 104.21.36.105<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   |
| www.unicode.org | IP: 64.182.27.164<br>所属国家: United States of America<br>地区: Texas<br>城市: Dallas<br>纬度: 32.814899<br>经度: -96.879204                |
| aomedia.org     | IP: 108.160.167.147<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 |
| g.co            | IP: 142.250.69.174<br>所属国家: United States of America<br>地区: California<br>城市: Mountain View<br>纬度: 37.405991<br>经度: -122.078514  |
| dartbug.com     | IP: 216.239.38.21<br>所属国家: United States of America<br>地区: Virginia<br>城市: Ashburn<br>纬度: 39.039474<br>经度: -77.491806            |

| URL信息                                                                                                                                                                                         | Url所在文件                                               |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|
| <a href="http://dashif.org/guidelines/last-segment-number">http://dashif.org/guidelines/last-segment-number</a>                                                                               | a1/d.java                                             |
| <a href="http://dashif.org/guidelines/trickmode">http://dashif.org/guidelines/trickmode</a>                                                                                                   | a1/d.java                                             |
| <a href="http://dashif.org/thumbnail_tile">http://dashif.org/thumbnail_tile</a>                                                                                                               | a1/d.java                                             |
| <a href="http://dashif.org/guidelines/thumbnail_tile">http://dashif.org/guidelines/thumbnail_tile</a>                                                                                         | a1/d.java                                             |
| <a href="http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense">http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense</a>                                             | b1/n0.java                                            |
| <a href="https://x&lt;/LA_URL&gt;">https://x&lt;/LA_URL&gt;</a>                                                                                                                               | b1/m0.java                                            |
| <a href="https://default.url">https://default.url</a>                                                                                                                                         | b1/m0.java                                            |
| <a href="https://developer.android.com/guide/topics/permissions/overview">https://developer.android.com/guide/topics/permissions/overview</a>                                                 | io/flutter/plugin/platform/PlatformPlugin.java        |
| <a href="https://docs.flutter.dev/deployment/android">https://docs.flutter.dev/deployment/android</a>                                                                                         | io/flutter/embedding/engine/loader/FlutterLoader.java |
| <a href="https://github.com/Baseflow/flutter-permission-handler/issues">https://github.com/Baseflow/flutter-permission-handler/issues</a>                                                     | o3/t.java                                             |
| <a href="https://developer.android.com/guide/topics/media/issues/cleartext-not-permitted">https://developer.android.com/guide/topics/media/issues/cleartext-not-permitted</a>                 | u0/q.java                                             |
| <a href="http://g.co/dev/packagevisibility">http://g.co/dev/packagevisibility</a>                                                                                                             | u0/w.java                                             |
| <a href="https://issuetracker.google.com/issues/new?component=907884&amp;template=1466542">https://issuetracker.google.com/issues/new?component=907884&amp;template=1466542</a>               | e0/m.java                                             |
| <a href="https://developer.android.com/guide/topics/media/issues/player-accessed-on-wrong-thread">https://developer.android.com/guide/topics/media/issues/player-accessed-on-wrong-thread</a> | w0/v0.java                                            |
| <a href="http://ns.adobe.com/xap/1.0/">http://ns.adobe.com/xap/1.0/</a>                                                                                                                       | c2/b.java                                             |
| <a href="https://aomedia.org/emsg/ID3">https://aomedia.org/emsg/ID3</a>                                                                                                                       | f2/a.java                                             |
|                                                                                                                                                                                               |                                                       |

|                                                                                                                                                                         |                               |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| <a href="https://developer.apple.com/streaming/emsg-id3">https://developer.apple.com/streaming/emsg-id3</a>                                                             | f2/a.java                     |
| <a href="https://journeyapps.com/">https://journeyapps.com/</a>                                                                                                         | 摸瓜V1引擎                        |
| <a href="https://github.com/journeyapps/zxing-android-embedded">https://github.com/journeyapps/zxing-android-embedded</a>                                               | 摸瓜V1引擎                        |
| <a href="https://github.com/richtr/NoSleep.js/issues/15">https://github.com/richtr/NoSleep.js/issues/15</a>                                                             | 摸瓜V2引擎                        |
| <a href="https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released">https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released</a>     | 摸瓜V2引擎                        |
| <a href="https://api.flutter.dev/flutter/material/Scaffold/of.html">https://api.flutter.dev/flutter/material/Scaffold/of.html</a>                                       | lib/arm64-v8a/libapp.so       |
| <a href="http://www.unicode.org/copyright.html">http://www.unicode.org/copyright.html</a>                                                                               | lib/arm64-v8a/libflutter.so   |
| <a href="https://github.com/flutter/flutter/issues">https://github.com/flutter/flutter/issues</a>                                                                       | lib/arm64-v8a/libflutter.so   |
| <a href="https://dartbug.com/52121">https://dartbug.com/52121</a>                                                                                                       | lib/arm64-v8a/libflutter.so   |
| <a href="https://r9nhvykt.vip/front/">https://r9nhvykt.vip/front/</a>                                                                                                   | lib/armeabi-v7a/libapp.so     |
| <a href="https://developer.mozilla.org/en-US/docs/Web/HTTP/Status">https://developer.mozilla.org/en-US/docs/Web/HTTP/Status</a>                                         | lib/armeabi-v7a/libapp.so     |
| <a href="http://www.ibm.com/data/dtd/v11/ibmhtml1-transitional.dtd">http://www.ibm.com/data/dtd/v11/ibmhtml1-transitional.dtd</a>                                       | lib/armeabi-v7a/libapp.so     |
| <a href="https://api.flutter.dev/flutter/material/Scaffold/of.html">https://api.flutter.dev/flutter/material/Scaffold/of.html</a>                                       | lib/armeabi-v7a/libapp.so     |
| <a href="https://github.com/dart-lang/language/issues/3488">https://github.com/dart-lang/language/issues/3488</a>                                                       | lib/armeabi-v7a/libapp.so     |
| <a href="https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android">https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android</a> | lib/armeabi-v7a/libapp.so     |
| <a href="http://www.unicode.org/copyright.html">http://www.unicode.org/copyright.html</a>                                                                               | lib/armeabi-v7a/libflutter.so |
| <a href="https://github.com/flutter/flutter/issues">https://github.com/flutter/flutter/issues</a>                                                                       | lib/armeabi-v7a/libflutter.so |
| <a href="https://dartbug.com/52121">https://dartbug.com/52121</a>                                                                                                       | lib/armeabi-v7a/libflutter.so |

 邮箱线索

| 邮箱地址                                                                                                                                                                                                          | 所在文件                          |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| appro@openssl.org                                                                                                                                                                                             | lib/arm64-v8a/libflutter.so   |
| appro@openssl.org                                                                                                                                                                                             | lib/arm64-v8a/libwebcrypto.so |
| _double@0150898.fromintege<br>_growablelist@0150898._literal<br>_immutablelist@0150898._yk<br>_typeerror@0150898._create<br>_jea@379287047.wpe<br>_bytebuffer@7027147._new<br>_assertionerror@0150898._create | lib/armeabi-v7a/libapp.so     |

 手机线索

| 手机号         | 所在文件      |
|-------------|-----------|
| 17512775099 | q5/a.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=CN, ST=Province, L=City, O=shunfeng, OU=Dev, CN=shunfeng.com  
签名算法: rsassa\_pkcs1v15  
有效期自: 2025-06-09 05:08:24+00:00  
有效期至: 2035-06-07 05:08:24+00:00  
发行人: C=CN, ST=Province, L=City, O=shunfeng, OU=Dev, CN=shunfeng.com  
序列号: 0x535f6f45ebb1b893  
哈希算法: sha256  
md5值: c1d76608e604f8262e8c6f021886373a  
sha1值: d887c7d21012eca214d1d44cccbab5c19e55b5fe  
sha256值: ab424f7788fa20accc4ec438cb4e6b0e4f5bf5e26ac231428e135d9054a6b6bc  
sha512值: d668f3ac4327cd48abf1bb65e25615d0d9a82b98647334a4f29f57ff430bb098d8f5c1803d4c834d4aa3f8cbcc69b83bbbe590ec99d337cff3a584145b4743a5  
公钥算法: rsa  
密钥长度: 2048  
指纹: 2c12cf18c71538acdeb56071289f7c85af30fb77605e139f6acd3e84bc7be0a4

## 硬编码敏感信息

| 可能的敏感信息                                                                   |
|---------------------------------------------------------------------------|
| "library_zxingandroidembedded_author" : "JourneyApps"                     |
| "library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/" |

## 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.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.INTERNET                 | 正常   | 互联网接入              | 允许应用程序创建网络套接字                             |
| 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.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_AUDIO      | 未知 | Unknown permission | Unknown permission from android reference                           |
| 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.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.ADD_VOICEMAIL         | 危险 | 将语音邮件添加到系统中        | 允许应用程序将语音邮件添加到系统中                                                   |
| android.permission.USE_SIP               | 危险 | 拨打/接听互联网电话         | 允许应用程序使用 SIP 服务拨打/接听互联网电话                                           |
| android.permission.READ_CALL_LOG         | 危险 |                    | 允许应用程序读取用户的通话日志                                                     |
| android.permission.WRITE_CALL_LOG        | 危险 |                    | 允许应用程序写入（但不读取）用户号召日志数据。                                             |
| android.permission.ACCESS_MEDIA_LOCATION | 危险 | 访问的任何地理位置          | 允许应用程序访问的任何地理位置持久保存在用户的共享集合                                         |
| 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.RECORD_AUDIO          | 危险 | 录音                 | 允许应用程序访问音频记录路径                                                      |
| android.permission.FOREGROUND_SERVICE    | 正常 |                    | 允许常规应用程序使用 Service.startForeground。                                 |

|                                                             |    |                    |                                           |
|-------------------------------------------------------------|----|--------------------|-------------------------------------------|
| syhdr.kgkwzt.dtgou.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
|-------------------------------------------------------------|----|--------------------|-------------------------------------------|



应用内通信

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。