



MoGua

正太短视频 3.20.APK 分析报告



APP名称:

正太短视频

包名: com.android.huawei.oplls

域名线索: 44条

URL线索: 29条

邮箱线索: 1条

分析日期: 2025年5月9日

分析平台: [摸瓜APK反编译平台](#)

文件名: 正太短视频_3.20.apk
文件大小: 15.65MB
MD5值: 2bcdcf099e5f88c91089f31179c4b5fc
SHA1值: a71da8d4bed78b778af5c885db1b701c136047a4
SHA256值: 70152ac96fad1b55f49607a9aae8b0af043451492787f5978a8225da317ac4a9

i APP 信息

App名称: 正太短视频
包名: com.android.huawei.oplls
主活动Activity: com.ty.app.tongyanrealapp.ui.splash.SplashActivity
安卓版本名称: 3.20
安卓版本: 10

🔍 域名线索

域名	服务器信息
swybgjapi3.lls001.life	IP: 178.157.60.146 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.052231 经度: -118.243683
swybgjapi.skxxma001.online	IP: 178.157.60.146 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.052231 经度: -118.243683
sswybgjapi3.mzfkapi.info	没有服务器地理信息.
	IP: 178.157.58.68

swybgjapi.gxmtv.site	所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.052231 经度: -118.243683
swybgjapi.mzfkapi.info	IP: 178.157.60.146 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.052231 经度: -118.243683
dashif.org	IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065632 经度: -79.891708
exoplayer.dev	IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065632 经度: -79.891708
swybgjapi4.umzfkapi.info	IP: 178.157.58.68 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.052231 经度: -118.243683
swybgjapi3.gxmtv.online	IP: 178.157.60.146 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.052231 经度: -118.243683

swybgjapi.gxmtv.online	IP: 178.157.58.68 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.052231 经度: -118.243683
swybgjapi4.mzfkapi.info	IP: 178.157.58.68 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.052231 经度: -118.243683
swybgjapi2.skxxma001.online	IP: 45.78.53.69 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.043240 经度: -118.250916
xmlpull.org	IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065632 经度: -79.891708
swybgjapi3.skxxma001.online	IP: 178.157.58.68 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.052231 经度: -118.243683
h.trace.qq.com	IP: 109.244.244.61 所属国家: China 地区: Beijing

	城市: Beijing 纬度: 39.907501 经度: 116.397232
swybgjapi2.gxmtv.online	IP: 45.78.53.69 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.043240 经度: -118.250916
swybgjapi3.yqloli.online	IP: 178.157.58.68 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.052231 经度: -118.243683
swybgjapi.ils001.life	IP: 178.157.58.68 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.052231 经度: -118.243683
schemas.microsoft.com	IP: 13.107.238.49 所属国家: United States of America 地区: Washington 城市: Redmond 纬度: 47.682899 经度: -122.120903
github.com	IP: 20.205.243.166 所属国家: United States of America 地区: Washington 城市: Redmond 纬度: 47.682899 经度: -122.120903
	IP: 178.157.58.68

swybgjapi2.yqloli.online	所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.052231 经度: -118.243683
swybgjapi2.lls001.life	IP: 45.78.53.69 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.043240 经度: -118.250916
swybgjapi4.skxxma001.online	IP: 178.157.58.68 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.052231 经度: -118.243683
swybgjapi.gxmtv.life	IP: 178.157.58.68 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.052231 经度: -118.243683
othstr.beacon.qq.com	IP: 109.244.218.16 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
swybgjapi3.gxmtv.site	IP: 178.157.60.146 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.052231 经度: -118.243683

www.binance.com	IP: 104.244.46.85 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446
swybgjapi2.yqloli.space	IP: 45.78.53.69 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.043240 经度: -118.250916
swybgjapi2.mzfkapi.info	IP: 45.78.53.69 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.043240 经度: -118.250916
swybgjapi2.gxmtv.site	IP: 45.78.53.69 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.043240 经度: -118.250916
swybgjapi3.gxmtv.life	IP: 178.157.60.146 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.052231 经度: -118.243683
xml.apache.org	IP: 151.101.2.132 所属国家: United States of America 地区: California

	城市: San Francisco 纬度: 37.775700 经度: -122.395203
schemas.android.com	没有服务器地理信息.
www.w3.org	IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
otheve.beacon.qq.com	IP: 109.244.244.85 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
swybgjapi3.yqloli.space	IP: 178.157.60.146 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.052231 经度: -118.243683
t.me	IP: 149.154.167.99 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: Lowestoft 纬度: 52.475201 经度: 1.751590
playready.directtaps.net	IP: 40.70.71.156 所属国家: United States of America 地区: Virginia 城市: Boydton 纬度: 36.667641

	经度: -78.387497
swybgjapi3.umzfkapi.info	IP: 178.157.58.68 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.052231 经度: -118.243683
swybgjapi.umzfkapi.info	IP: 178.157.60.146 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.052231 经度: -118.243683
app.iqiyi.com	IP: 220.181.109.166 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
www.huobi.com	IP: 108.160.163.116 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
swybgjapi2.umzfkapi.info	IP: 45.78.53.69 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.043240 经度: -118.250916
	IP: 45.78.53.69 所属国家: United States of America

swybgjapi2.gxmtv.life	地区: California 城市: Los Angeles 纬度: 34.043240 经度: -118.250916
-----------------------	---

URL线索

URL信息	Url所在文件
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	io/reactivex/rxjava3/exceptions/UndeliverableException.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/rxjava3/exceptions/OnErrorNotImplementedException.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	defpackage/m60.java
https://exoplayer.dev/issues/player-accessed-on-wrong-thread	defpackage/ax1.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	defpackage/z51.java
http://www.w3.org/ns/ttml	defpackage/g82.java
http://%s:%d/%s	defpackage/yf1.java
https://github.com/danikula/AndroidVideoCache/issues/134	defpackage/yf1.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	defpackage/vu0.java
http://%s:%d/%s	defpackage/fh0.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	defpackage/bm.java
http://xmlpull.org/v1/doc/features.html	defpackage/rj1.java

http://dashif.org/guidelines/last-segment-number	defpackage/ur.java
http://swybgjapi2.yqloli.online	defpackage/y21.java
http://swybgjapi3.yqloli.online	defpackage/y21.java
http://swybgjapi2.yqloli.space	defpackage/y21.java
http://swybgjapi3.yqloli.space	defpackage/y21.java
http://swybgjapi.lls001.life	defpackage/y21.java
http://swybgjapi2.lls001.life	defpackage/y21.java
http://swybgjapi3.lls001.life	defpackage/y21.java
http://swybgjapi.gxmtv.life	defpackage/y21.java
http://swybgjapi2.gxmtv.life	defpackage/y21.java
http://swybgjapi3.gxmtv.life	defpackage/y21.java
http://swybgjapi.gxmtv.site	defpackage/y21.java
http://swybgjapi2.gxmtv.site	defpackage/y21.java
http://swybgjapi3.gxmtv.site	defpackage/y21.java
http://swybgjapi.gxmtv.online	defpackage/y21.java
http://swybgjapi2.gxmtv.online	defpackage/y21.java
http://swybgjapi3.gxmtv.online	defpackage/y21.java
http://swybgjapi.umzfkapi.info	defpackage/y21.java

http://swybgjapi2.umzfkapi.info	defpackage/y21.java
http://swybgjapi3.umzfkapi.info	defpackage/y21.java
http://swybgjapi4.umzfkapi.info	defpackage/y21.java
http://swybgjapi.mzfkapi.info	defpackage/y21.java
http://swybgjapi2.mzfkapi.info	defpackage/y21.java
http://sswybgjapi3.mzfkapi.info	defpackage/y21.java
http://swybgjapi4.mzfkapi.info	defpackage/y21.java
http://swybgjapi.skxxma001.online	defpackage/y21.java
http://swybgjapi2.skxxma001.online	defpackage/y21.java
http://swybgjapi3.skxxma001.online	defpackage/y21.java
http://swybgjapi4.skxxma001.online	defpackage/y21.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	defpackage/mx1.java
https://github.com/danikula/AndroidVideoCache/issues/43	defpackage/qh0.java
https://github.com/danikula/AndroidVideoCache/issues	defpackage/qh0.java
https://github.com/danikula/AndroidVideoCache/issues/88	defpackage/qh0.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/SlidingTabLayout.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/CommonTabLayout.java

http://schemas.android.com/apk/res/android	com/flyco/tablayout/SegmentTabLayout.java
http://xml.apache.org/xslt	com/orhanobut/logger/LoggerPrinter.java
https://t.me/tysptv001	com/ty/app/tongyanrealapp/ui/splash/SplashActivity\$bindEvent\$2.java
http://app.iqiyi.com	com/ty/app/tongyanrealapp/ui/video/p000long/LongVideoDetailActivity\$videoPlayHeader\$2.java
http://app.iqiyi.com	com/ty/app/tongyanrealapp/ui/video/p001short/ShortListPlayFragment\$videoPlayHeader\$2.java
https://otheve.beacon.qq.com/analytics/upload	com/tencent/beacon/base/net/c/b.java
https://othstr.beacon.qq.com/analytics/upload	com/tencent/beacon/base/net/c/b.java
https://h.trace.qq.com/kv	com/tencent/beacon/a/b/c.java
http://xmllpull.org/v1/doc/features.html	com/tencent/cos/xml/transfer/XmlBuilder.java
http://www.w3.org/2001/XMLSchema-instance	com/tencent/cos/xml/transfer/XmlBuilder.java
http://xmllpull.org/v1/doc/features.html	com/tencent/cos/xml/transfer/XmlSlimBuilder.java
http://playready.directtaps.net/pr/svc/rightsmanager.asmx	tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java
http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java
https://www.binance.com	Mogua Engine V1
https://www.huobi.com	Mogua Engine V1

 邮箱线索

--	--

邮箱地址	所在文件
danikula@gmail.com	defpackage/qh0.java

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=silkand, ST=dslnknkfk, L=sdlfna, O=dsnf, OU=eapsihfd, CN=wehosdf
签名算法: rsassa_pkcs1v15
有效期自: 2023-02-17 14:33:27+00:00
有效期至: 2077-11-20 14:33:27+00:00
发行人: C=silkand, ST=dslnknkfk, L=sdlfna, O=dsnf, OU=eapsihfd, CN=wehosdf
序列号: 0x2508e16
哈希算法: sha256
md5值: e8069a2a8367d3b753fbec0c6db6aefc
sha1值: 2a2a3fe8aafb2c8fcfb8f85fc605cba31863271
sha256值: 77867e2a5200c565dd0e6a6d89ef2693cb0e15f8994de44406f8ce646954d7d1
sha512值: 793b8d04cac327b1b41bbf25dfdb21f38b3d76a3dc5863a8e72e0103c5c1bf974e7984ef8ebde75673f884349faf3b9cb8cd3807c3fc5002ecc241050da4409f
公钥算法: rsa
密钥长度: 2048
指纹: d8a8f37f514509e54625d157b5664e1deec9c65973ca617545a8f95173d84243

 硬编码敏感信息

可能的敏感信息
"accountCredentials" : "账号凭证"
"ordinaryUser" : "我是普通用户，购买正式会员才可兑现"
"retrieveByCertificate" : "凭证找回"
"accountCredentials" : "Account Credentials"
"ordinaryUser" : "I am an ordinary user, only VIP can be redeemed"
"retrieveByCertificate" : "Retrieve by certificate"

 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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.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.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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒

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。