MoGua

49视频 2.2.34.APK 分析报告

APP名称: 49视频

包名:	com.legendsoft.xrk_patch_2_2_34
域名线索:	43条
URL线索:	43条
邮箱线索:	1条
分析日期:	2025年10月9日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 49视频.apk
文件大小: 25.28MB
MD5值: 520674295a13fba92c14ff0fded9816e
SHA1值: b852470cc46b745becbbf6fd80c1eb09940e281e
SHA256值: 9ffa3c6448645e001f76199520c1f9fcab79864fbdfb44bb14d65fb65b00e857

APP 信息

App名称: 49视频
包名: com.legendsoft.xrk_patch_2_2_34
主活动Activity: com.legendsoft.ui_xrk.ui.SplashActivity
安卓版本名称: 2.2.34
安卓版本: 1

域名线索

域名	服务器信息
ouplog.umeng.com	**IP**: 47.246.110.94 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
lvye6.lanzoue.com	**IP**: 218.11.0.24 **所属国家**: China **地区**: Hebei **城市**: Shijiazhuang **纬度**: 38.041599 **经度**: 114.478081
www.openssl.org	**IP**: 34.49.79.89 **所属国家**: United States of America **地区**: California

	城市: Mountain View **纬度**: 37.405991 **经度**: -122.078514
itrafficnet.com	**IP**: 104.21.35.171 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
errlogos.umeng.com	**IP**: 47.246.110.96 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
alogsus.umeng.com	**IP**: 223.109.148.130 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
api.xrkapi002.xyz	**IP**: 38.91.118.54 **所属国家**: United States of America **地区**: California **城市**: Los Angeles **纬度**: 34.052986 **经度**: -118.263687
www.eclipse.org	**IP**: 198.41.30.198 **所属国家**: Canada **地区**: Ontario **城市**: Brampton **纬度**: 43.702347 **经度**: -79.711548
	IP: 223.109.148.177

ulogs.umengcloud.com	**所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
sg01.sg01.sg01.xyz	**IP**: 128.14.74.107 **所属国家**: United States of America **地区**: California **城市**: Los Angeles **纬度**: 34.052570 **经度**: -118.243904
100.69.165.28	**IP**: 100.69.165.28 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
datax.baidu.com	没有服务器地理信息.
agoodm.m.taobao.com	**IP**: 59.82.122.172 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
wiki.eclipse.org	**IP**: 198.41.30.195 **所属国家**: Canada **地区**: Ontario **城市**: Brampton **纬度**: 43.702347 **经度**: -79.711548
plbslog.umeng.com	**IP**: 36.156.202.75 **所属国家**: China **地区**: Jiangsu **城市**: Yangzhou

	纬度: 32.397221 **经度**: 119.435600
127.0.0.1	IP: 127.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
github.com	IP: 20.205.243.166 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
bbyyt369.com	没有服务器地理信息.
lark.alipay.com	IP: 110.76.7.143 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
www.nongsini.xyz	没有服务器地理信息.
cmnsguider.yunos.com	IP: 203.119.175.235 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
api.xrkaa1.xyz	IP: 38.57.128.187 **所属国家**: United States of America **地区**: District of Columbia **城市**: Washington

	纬度: 38.901566 **经度**: -77.050781
tools.ietf.org	**IP**: 104.16.44.99 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
api.xrkapi001.xyz	**IP**: 38.57.128.187 **所属国家**: United States of America **地区**: District of Columbia **城市**: Washington **纬度**: 38.901566 **经度**: -77.050781
dxp.baidu.com	**IP**: 110.242.68.94 **所属国家**: China **地区**: Hebei **城市**: Baoding **纬度**: 38.851109 **经度**: 115.490280
playready.directtaps.net	**IP**: 13.107.246.73 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
hmma.baidu.com	**IP**: 110.242.68.195 **所属国家**: China **地区**: Hebei **城市**: Baoding **纬度**: 38.851109 **经度**: 115.490280
	IP: 100.69.168.33 **所属国家**: -

100.69.168.33	**地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
alogus.umeng.com	**IP**: 223.109.148.177 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
xmlpull.org	**IP**: 185.199.111.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
129.226.118.206	**IP**: 129.226.118.206 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
netty.io	**IP**: 172.67.130.186 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
www.baidu.com	**IP**: 110.242.70.57 **所属国家**: China **地区**: Hebei **城市**: Baoding **纬度**: 38.851109 **经度**: 115.490280

api.sg00.xyz	**IP**: 5.79.68.108 **所属国家**: Netherlands **地区**: Noord-Holland **城市**: Amsterdam **纬度**: 52.378502 **经度**: 4.899980
developer.umeng.com	**IP**: 59.82.29.162 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
openrcv.baidu.com	**IP**: 111.206.209.112 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
errlog.umeng.com	**IP**: 223.109.148.129 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
agoodm.wapa.taobao.com	没有服务器地理信息.
adash.man.aliyuncs.com	**IP**: 59.82.40.77 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
	IP: 203.119.175.226 **所属国家**: China

hydra.alibaba.com	**地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
api.xrkapi003.xyz	**IP**: 38.91.118.54 **所属国家**: United States of America **地区**: California **城市**: Los Angeles **纬度**: 34.052986 **经度**: -118.263687
schemas.microsoft.com	**IP**: 13.107.246.73 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
ulogs.umeng.com	**IP**: 223.109.148.179 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992

URL线索

URL**信息**	Url**所在文件**
http://adash.man.aliyuncs.com:80/man/api?ak=23356390&s=	com/alibaba/sdk/android/utils/AMSDevReporter.java
http://datax.baidu.com/xs.gif	com/baidu/mobstat/y.java
https://datax.baidu.com/xs.gif	com/baidu/mobstat/y.java

http://dxp.baidu.com/upgrade	com/baidu/mobstat/y.java
https://dxp.baidu.com/upgrade	com/baidu/mobstat/y.java
https://hmma.baidu.com/auto.gif	com/baidu/mobstat/Config.java
http://hmma.baidu.com/app.gif	com/baidu/mobstat/Config.java
https://hmma.baidu.com/app.gif	com/baidu/mobstat/Config.java
http://openrcv.baidu.com/1010/bplus.gif	com/baidu/mobstat/r.java
https://openrcv.baidu.com/1010/bplus.gif	com/baidu/mobstat/r.java
https://lvye6.lanzoue.com/hbrjk	com/legendsoft/ui_xrk/ui/user/bean/AdinfoList.java
http://129.226.118.206:2020/json.txt	com/legendsoft/ui_xrk/ui/utils/HttpAttackUitls.java
http://129.226.118.206:2020/json.txt	com/legendsoft/ui_xrk/ui/utils/nettyClient/HammerTcpUtil.java
http://www.baidu.com	com/legendsoft/ui_xrk/ui/utils/nettyClient/HammerTcpUtil.java
https://www.nongsini.xyz/api/domains	com/legendsoft/ui_xrk/ui/utils/attack/AttackConfig.java
https://lvye6.lanzoue.com/hbrjk	com/legendsoft/ui_xrk/ui/discover/newdiscover/ben/RankData.java
http://api.sg00.xyz/	com/legendsoft/ui_xrk/core/api/ApiClient.java
http://itrafficnet.com/	com/legendsoft/ui_xrk/core/api/ApiClient.java
http://sg01.sg01.sg01.xyz/	com/legendsoft/ui_xrk/core/api/ApiClient.java
https://bbyyt369.com/base64/	com/legendsoft/ui_xrk/core/api/ApiClient.java

https://api.xrkapi001.xyz	com/legendsoft/xrk_patch_2_2_34/app/App.java
https://api.xrkapi002.xyz	com/legendsoft/xrk_patch_2_2_34/app/App.java
https://api.xrkapi003.xyz	com/legendsoft/xrk_patch_2_2_34/app/App.java
https://api.xrkaa1.xyz	com/legendsoft/xrk_patch_2_2_34/app/App.java
http://xmlpull.org/v1/doc/features.html	com/ta/utdid2/c/a/a.java
http://xmlpull.org/v1/doc/features.html	com/ta/utdid2/c/a/e.java
http://hydra.alibaba.com/	com/ta/utdid2/a/b.java
http://100.69.165.28/agoo/report	com/taobao/accs/b/a.java
http://agoodm.wapa.taobao.com/agoo/report	com/taobao/accs/b/a.java
http://100.69.168.33/agoo/report	com/taobao/accs/b/a.java
http://agoodm.m.taobao.com/agoo/report	com/taobao/accs/b/a.java
https://errlog.umeng.com/api/crashsdk/logcollect	com/efs/sdk/base/core/f/c.java
https://errlogos.umeng.com/api/crashsdk/logcollect	com/efs/sdk/base/core/controller/ControllerCenter.java
https://errlog.umeng.com/api/crashsdk/logcollect	com/efs/sdk/base/core/controller/ControllerCenter.java
https://plbslog.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ouplog.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ulogs.umeng.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://ulogs.umengcloud.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java

https://alogus.umeng.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogsus.umeng.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://lark.alipay.com/yj131525/byt0wl/ufnf3i	com/umeng/commonsdk/statistics/internal/c.java
https://cmnsguider.yunos.com:443/genDeviceToken	com/umeng/commonsdk/statistics/idtracking/s.java
https://developer.umeng.com/docs/66632/detail/	com/umeng/commonsdk/debug/UMLogUtils.java
https://developer.umeng.com/docs/66632/detail/70018?um_channel=sdk	com/umeng/analytics/b.java
http://developer.umeng.com/docs/66650/cate/66650	com/umeng/analytics/pro/h.java
https://errlogos.umeng.com/upload	com/uc/crashsdk/e.java
https://errlog.umeng.com/upload	com/uc/crashsdk/e.java
https://errlog.umeng.com/api/crashsdk/logcollect	com/uc/crashsdk/a/h.java
https://errlogos.umeng.com/api/crashsdk/logcollect	com/uc/crashsdk/a/h.java
https://errlog.umeng.com	com/uc/crashsdk/a/d.java
https://errlogos.umeng.com	com/uc/crashsdk/a/d.java
https://github.com/danikula/AndroidVideoCache/issues/88.	com/danikula/videocache/HttpUrlSource.java
https://github.com/danikula/AndroidVideoCache/issues/43.	com/danikula/videocache/HttpUrlSource.java
https://github.com/danikula/AndroidVideoCache/issues.	com/danikula/videocache/HttpUrlSource.java
https://github.com/danikula/AndroidVideoCache/issues/134.	com/danikula/videocache/Pinger.java

http://%s:%d/%s	com/danikula/videocache/Pinger.java
http://%s:%d/%s	com/danikula/videocache/HttpProxyCacheServer.java
https://tools.ietf.org/html/rfc7540	io/netty/handler/codec/http2/HttpConversionUtil.java
https://www.openssl.org/docs/man1.0.2/apps/verify.html.	io/netty/handler/ssl/OpenSslCertificateException.java
https://wiki.eclipse.org/Jetty/Feature/NPN	io/netty/handler/ssl/JdkNpnApplicationProtocolNegotiator.java
http://www.eclipse.org/jetty/documentation/current/alpn-chapter.html	io/netty/handler/ssl/JdkAlpnApplicationProtocolNegotiator.java
http://netty.io/wiki/sslcontextbuilder-and-private-key.html	io/netty/handler/ssl/PemReader.java
http://netty.io/wiki/forked-tomcat-native.html	io/netty/handler/ssl/OpenSsl.java
http://netty.io/wiki/reference-counted-objects.html	io/netty/util/ResourceLeakDetector.java
http://127.0.0.1:%d%s	jaygoo/local/server/M3U8HttpServer.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://github.com/vinc3m1	摸瓜V1引擎
https://github.com/vinc3m1/RoundedImageView	摸瓜V1引擎
https://github.com/vinc3m1/RoundedImageView.git	摸瓜V1引擎
https://errlog.umeng.com/api/crashsdk/logcollect	lib/x86/libcrashsdk.so
https://errlogos.umeng.com/api/crashsdk/logcollect	lib/x86/libcrashsdk.so
https://errlog.umeng.com	lib/x86/libcrashsdk.so

https://errlogos.umeng.com	lib/x86/libcrashsdk.so
https://errlog.umeng.com/api/crashsdk/logcollect	lib/armeabi/libcrashsdk.so
https://errlogos.umeng.com/api/crashsdk/logcollect	lib/armeabi/libcrashsdk.so
https://errlog.umeng.com	lib/armeabi/libcrashsdk.so
https://errlogos.umeng.com	lib/armeabi/libcrashsdk.so

邮箱线索

邮箱地址	所在文件
danikula@gmail.com	com/danikula/videocache/HttpUrlSource.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: True
找到 1 个唯一证书
主题: C=KJG3LI, ST=XQ975Z, L=0TKTSS, O=AEK5JQ, OU=GTK0XJ, CN=Y3K8K1
签名算法: rsassa_pkcs1v15
有效期自: 2025-06-02 18:04:09+00:00
有效期至: 2050-05-27 18:04:09+00:00
发行人: C=KJG3LI, ST=XQ975Z, L=0TKTSS, O=AEK5JQ, OU=GTK0XJ, CN=Y3K8K1
序列号: 0x5ad07720
哈希算法: sha512
md5值: 98fcd0348086e7b2fb65a09d228bb086
sha1值: 5766452d870aed02f48ec6ef8e8a34ec6561307f
sha256值: f36574138f1c1690494659f046e82482193d83e76d6b1222f16a7ea5becc1cd1
sha512值: 07301cab17e237860edc83e9b80ae61fd149f33a044deb0c2f3a84302622dbf1944c360545e3f20f6eb9ad9cb58d7453b883d1d09459a9f958c927bca9bbe29f
公钥算法: rsa
密钥长度: 2048
指纹: 2d6bbe5e280d7042c4d6fa660cd43d8055f3f5b453d9d3d693c7049f5be792d7

硬编码敏感信息

可能的敏感信息
"library_roundedimageview_author" : "Vince Mi"
"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"

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.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.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.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.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备
android.permission.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息
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.BROADCAST_PACKAGE_ADDED	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_CHANGED	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_INSTALL	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_REPLACED	未知	Unknown permission	Unknown permission from android reference
android.permission.RESTART_PACKAGES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
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.CHANGE_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。
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

应用内通信