Evaluation Warning: The document was created with Spire.Doc for Python.

**49视频（ 2.2.34版本）   
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。  
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | 49视频 |
| 版本 | 2.2.34 |
| 包名 | com.legendsoft.xrk\_patch\_2\_2\_34 |
| 域名线索 | 43条 |
| URL线索 | 43条 |
| APP图标 |  |
| 分析日期 | 2025年10月9日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | 49视频.apk |
| 文件大小 | 25.28MB |
| MD5值 | 520674295a13fba92c14ff0fded9816e |
| SHA1值 | b852470cc46b745becbbf6fd80c1eb09940e281e |
| SHA256值 | 9ffa3c6448645e001f76199520c1f9fcab79864fbdfb44bb14d65fb65b00e857 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| 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 |

## **4. 线索情况**

### **4.1 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 |
| lvye6.lanzoue.com | IP: 218.11.0.24  所属国家: China  地区: Hebei  城市: Shijiazhuang |
| www.openssl.org | IP: 34.49.79.89  所属国家: United States of America  地区: California  城市: Mountain View |
| itrafficnet.com | IP: 104.21.35.171  所属国家: United States of America  地区: California  城市: San Francisco |
| errlogos.umeng.com | IP: 47.246.110.96  所属国家: Singapore  地区: Singapore  城市: Singapore |
| alogsus.umeng.com | IP: 223.109.148.130  所属国家: China  地区: Jiangsu  城市: Nanjing |
| api.xrkapi002.xyz | IP: 38.91.118.54  所属国家: United States of America  地区: California  城市: Los Angeles |
| www.eclipse.org | IP: 198.41.30.198  所属国家: Canada  地区: Ontario  城市: Brampton |
| ulogs.umengcloud.com | IP: 223.109.148.177  所属国家: China  地区: Jiangsu  城市: Nanjing |
| sg01.sg01.sg01.xyz | IP: 128.14.74.107  所属国家: United States of America  地区: California  城市: Los Angeles |
| 100.69.165.28 | IP: 100.69.165.28  所属国家: -  地区: -  城市: - |
| 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 |
| wiki.eclipse.org | IP: 198.41.30.195  所属国家: Canada  地区: Ontario  城市: Brampton |
| plbslog.umeng.com | IP: 36.156.202.75  所属国家: China  地区: Jiangsu  城市: Yangzhou |
| 127.0.0.1 | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| 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 |
| 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 |
| api.xrkaa1.xyz | IP: 38.57.128.187  所属国家: United States of America  地区: District of Columbia  城市: Washington |
| tools.ietf.org | IP: 104.16.44.99  所属国家: United States of America  地区: California  城市: San Francisco |
| api.xrkapi001.xyz | IP: 38.57.128.187  所属国家: United States of America  地区: District of Columbia  城市: Washington |
| dxp.baidu.com | IP: 110.242.68.94  所属国家: China  地区: Hebei  城市: Baoding |
| playready.directtaps.net | IP: 13.107.246.73  所属国家: United States of America  地区: Washington  城市: Redmond |
| hmma.baidu.com | IP: 110.242.68.195  所属国家: China  地区: Hebei  城市: Baoding |
| 100.69.168.33 | IP: 100.69.168.33  所属国家: -  地区: -  城市: - |
| alogus.umeng.com | IP: 223.109.148.177  所属国家: China  地区: Jiangsu  城市: Nanjing |
| xmlpull.org | IP: 185.199.111.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| 129.226.118.206 | IP: 129.226.118.206  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| netty.io | IP: 172.67.130.186  所属国家: United States of America  地区: California  城市: San Francisco |
| www.baidu.com | IP: 110.242.70.57  所属国家: China  地区: Hebei  城市: Baoding |
| api.sg00.xyz | IP: 5.79.68.108  所属国家: Netherlands  地区: Noord-Holland  城市: Amsterdam |
| developer.umeng.com | IP: 59.82.29.162  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| openrcv.baidu.com | IP: 111.206.209.112  所属国家: China  地区: Beijing  城市: Beijing |
| errlog.umeng.com | IP: 223.109.148.129  所属国家: China  地区: Jiangsu  城市: Nanjing |
| 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 |
| hydra.alibaba.com | IP: 203.119.175.226  所属国家: China  地区: Beijing  城市: Beijing |
| api.xrkapi003.xyz | IP: 38.91.118.54  所属国家: United States of America  地区: California  城市: Los Angeles |
| schemas.microsoft.com | IP: 13.107.246.73  所属国家: United States of America  地区: Washington  城市: Redmond |
| ulogs.umeng.com | IP: 223.109.148.179  所属国家: China  地区: Jiangsu  城市: Nanjing |

### **4.2 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 |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| danikula@gmail.com | com/danikula/videocache/HttpUrlSource.java |

### **4.4 手机号线索**

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

## **5. 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**

## **6. 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" |

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看 |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看 |  |  |

## **9. 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 |

## **10. 应用内通信**

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