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

**UU视频（ 3.2.1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 | UU视频 |
| 版本 | 3.2.1 |
| 包名 | com.crse.lu2ee |
| 域名线索 | 26条 |
| URL线索 | 22条 |
| APP图标 |  |
| 分析日期 | 2025年6月16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 | uusp\_8tswa6cy15\_3.2.1.apk |
| 文件大小 | 26.96MB |
| MD5值 | 876d6065f117009498a82ed4892e1c55 |
| SHA1值 | 2a0e06d727b9a469336ca2069b000ed4ef2766c6 |
| SHA256值 | 91608286f2196e8c97b359522d823da2323d33df47ba4b7aa4f9c9a404e32dab |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | UU视频 |
| 包名 | com.crse.lu2ee |
| 主活动Activity | com.jbzd.media.fiveonehl.ui.splash.SplashActivity |
| 安卓版本名称 | 3.2.1 |
| 安卓版本 | 222 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| sdosadkwda.apiyoo7xaws.cc | IP: 13.35.238.18 所属国家: India 地区: Telangana 城市: Hyderabad  |
| xml.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| m.alipay.com | IP: 203.209.245.74 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| mobilegw.stable.alipay.net | 没有服务器地理信息.  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| h5.m.taobao.com | IP: 125.39.155.171 所属国家: China 地区: Tianjin 城市: Tianjin  |
| mobilegw.aaa.alipay.net | 没有服务器地理信息.  |
| 127.0.0.1 | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| schemas.microsoft.com | IP: 13.107.246.74 所属国家: United States of America 地区: Washington 城市: Redmond  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| eedcdvrf.apiv7635fgi.cc | IP: 18.172.52.25 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| playready.directtaps.net | IP: 13.107.246.74 所属国家: United States of America 地区: Washington 城市: Redmond  |
| dashif.org | IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| pcasdmsan.apio0vrtnho.cc | IP: 18.172.52.25 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| tmapi.tmsangewg.com | 没有服务器地理信息.  |
| schemas.android.com | 没有服务器地理信息.  |
| api.telegram.org | IP: 31.13.75.5 所属国家: Ireland 地区: Dublin 城市: Dublin  |
| vskdkd.api8k88ep7h.cc | IP: 13.35.238.18 所属国家: India 地区: Telangana 城市: Hyderabad  |
| loggw-exsdk.alipay.com | IP: 110.76.6.92 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| wappaygw.alipay.com | IP: 111.202.5.210 所属国家: China 地区: Beijing 城市: Beijing  |
| mobilegw.alipay.com | IP: 203.209.247.65 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| voxocdcof.api1izml4uo.cc | IP: 13.35.238.18 所属国家: India 地区: Telangana 城市: Hyderabad  |
| api.buzhidaoxiesha.com | 没有服务器地理信息.  |
| mobilegw-1-64.test.alipay.net | 没有服务器地理信息.  |
| mcgw.alipay.com | IP: 111.202.5.210 所属国家: China 地区: Beijing 城市: Beijing  |
| mclient.alipay.com | IP: 116.142.235.203 所属国家: China 地区: Beijing 城市: Beijing  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://github.com/danikula/AndroidVideoCache/issues/88.  | af/ag/aa/ai.java  |
| https://github.com/danikula/AndroidVideoCache/issues/43.  | af/ag/aa/ai.java  |
| https://github.com/danikula/AndroidVideoCache/issues.  | af/ag/aa/ai.java  |
| http://%s:%d/%s  | af/ag/aa/al.java  |
| http://%s:%d/%s  | af/ag/aa/ag.java  |
| https://github.com/danikula/AndroidVideoCache/issues/134.  | af/ag/aa/ag.java  |
| http://schemas.android.com/apk/res/android  | af/ak/aa/aa/odin/an.java  |
| http://dashif.org/guidelines/last-segment-number  | af/ak/aa/aa/chi/bl/ak/ac.java  |
| http://m.alipay.com/?action=h5quit  | af/aa/ab/aj/ah.java  |
| https://h5.m.taobao.com/mlapp/olist.html  | af/aa/ab/ac/aa.java  |
| https://mobilegw.alipay.com/mgw.htm  | af/aa/ab/ac/ad.java  |
| https://mobilegw.alipay.com/mgw.htm  | af/aa/ab/af/ac.java  |
| https://mcgw.alipay.com/sdklog.do  | af/aa/ab/af/ad/ac.java  |
| https://loggw-exsdk.alipay.com/loggw/logUpload.do  | af/aa/ab/af/ad/ad.java  |
| https://api.telegram.org/bot6086117813:AAFwiL2Rn\_qZbWa\_a6DkegGeAx1gIJorQzA/sendMessage  | af/aq/aa/aa/ac.java  |
| http://api.buzhidaoxiesha.com/cxapi/  | af/aq/aa/aa/ai/al.java  |
| http://tmapi.tmsangewg.com/cxapi/  | af/aq/aa/aa/ai/al.java  |
| https://eedcdvrf.apiv7635fgi.cc/uxuxsxpx/  | af/aq/aa/aa/al/ar.java  |
| https://voxocdcof.api1izml4uo.cc/uxuxsxpx/  | af/aq/aa/aa/al/ar.java  |
| https://sdosadkwda.apiyoo7xaws.cc/uxuxsxpx/  | af/aq/aa/aa/al/ar.java  |
| https://vskdkd.api8k88ep7h.cc/uxuxsxpx/  | af/aq/aa/aa/al/ar.java  |
| https://pcasdmsan.apio0vrtnho.cc/uxuxsxpx/  | af/aq/aa/aa/al/ar.java  |
| http://api.  | af/aq/aa/aa/al/ar.java  |
| http://xml.apache.org/xslt  | ad/aa/aa/ab/aa/am.java  |
| https://mobilegw.alipay.com/mgw.htm  | com/alipay/apmobilesecuritysdk/b/a.java  |
| http://mobilegw.aaa.alipay.net/mgw.htm  | com/alipay/apmobilesecuritysdk/b/a.java  |
| http://mobilegw-1-64.test.alipay.net/mgw.htm  | com/alipay/apmobilesecuritysdk/b/a.java  |
| http://mobilegw.stable.alipay.net/mgw.htm  | com/alipay/apmobilesecuritysdk/b/a.java  |
| https://wappaygw.alipay.com/home/exterfaceAssign.htm?  | com/alipay/sdk/app/PayTask.java  |
| https://mclient.alipay.com/home/exterfaceAssign.htm?  | com/alipay/sdk/app/PayTask.java  |
| https://wappaygw.alipay.com/service/rest.htm  | com/alipay/sdk/app/PayTask.java  |
| http://wappaygw.alipay.com/service/rest.htm  | com/alipay/sdk/app/PayTask.java  |
| https://mclient.alipay.com/service/rest.htm  | com/alipay/sdk/app/PayTask.java  |
| http://mclient.alipay.com/service/rest.htm  | com/alipay/sdk/app/PayTask.java  |
| https://mclient.alipay.com/home/exterfaceAssign.htm  | com/alipay/sdk/app/PayTask.java  |
| http://mclient.alipay.com/home/exterfaceAssign.htm  | com/alipay/sdk/app/PayTask.java  |
| https://mclient.alipay.com/cashier/mobilepay.htm  | com/alipay/sdk/app/PayTask.java  |
| http://mclient.alipay.com/cashier/mobilepay.htm  | com/alipay/sdk/app/PayTask.java  |
| http://schemas.android.com/apk/res/android  | com/flyco/tablayout/SegmentTabLayout.java  |
| http://schemas.android.com/apk/res/android  | com/flyco/tablayout/CommonTabLayout.java  |
| http://schemas.android.com/apk/res/android  | com/flyco/tablayout/SlidingTabLayout.java  |
| http://127.0.0.1:  | com/jbzd/media/fiveonehl/ui/download/MergeTsToMp4Helper.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  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| danikula@gmail.com  | af/ag/aa/ai.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: CN=tiktok, OU=tiktok, O=tiktok, L=tiktok, ST=tiktok, C=886 签名算法: rsassa\_pkcs1v15 有效期自: 2024-07-29 17:56:25+00:00 有效期至: 2049-07-23 17:56:25+00:00 发行人: CN=tiktok, OU=tiktok, O=tiktok, L=tiktok, ST=tiktok, C=886 序列号: 0x1 哈希算法: sha256 md5值: 0d28843ce5247728d27d3bab9c101d32 sha1值: e921b34552492497b8ca366964f4375e52905fb8 sha256值: 7c897c35d710fb9cff3182cea51c80a4904dd2c61321e3bde8ab50ae644bb2e3 sha512值: 13eb6bc89c0268a7bed8b33c48df11c6eb95d7486cf5e4bdbf3e95bf3f0a5ff6a8cd2f522b3724e2308966cbd54c2c28d4f4cfecb8015ca2b8e779d8c939379b 公钥算法: rsa 密钥长度: 2048 指纹: 4591cef4b7f13d401c9f48f3da198bd77d927d863b67dd8a108db76b846e0bff**

## **6. 硬编码敏感信息**

## **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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.SYSTEM\_ALERT\_WINDOW | 危险 | 显示系统级警报 | 允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕 |
| 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.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 |
| android.permission.KILL\_BACKGROUND\_PROCESSES | 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.READ\_PRIVILEGED\_PHONE\_STATE | 未知 | Unknown permission | Unknown permission from android reference |
| 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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |

## **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。**