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

**小蓝视频（ 4.9.0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 | 小蓝视频 |
| 版本 | 4.9.0 |
| 包名 | tv.wgady.wxvzqk |
| 域名线索 | 20条 |
| URL线索 | 30条 |
| APP图标 |  |
| 分析日期 | 2025年6月15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 | xlp\_4.9.0\_250610\_6.apk |
| 文件大小 | 20.95MB |
| MD5值 | 68a4bad5b634e91bec991ebe7bbbb88b |
| SHA1值 | 02e81db8b92e1a6673e4890abd173d920c4107be |
| SHA256值 | 575970339caac62209dd5ccc7237b88cfdee71de1fdf0bffe80c4cb3c489b89b |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 小蓝视频 |
| 包名 | tv.wgady.wxvzqk |
| 主活动Activity |  |
| 安卓版本名称 | 4.9.0 |
| 安卓版本 | 490 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| api3.eacysftg.xyz | IP: 156.255.123.38 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| api.login.yahoo.com | IP: 74.6.160.138 所属国家: United States of America 地区: New York 城市: New York City  |
| cfg.flurry.com | IP: 69.147.80.12 所属国家: United States of America 地区: New York 城市: New York City  |
| exoplayer.dev | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| dashif.org | IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| api2.eacysftg.xyz | IP: 154.207.77.38 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| www.slf4j.org | IP: 159.100.250.151 所属国家: Switzerland 地区: Zurich 城市: Zurich  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| schemas.android.com | 没有服务器地理信息.  |
| imgpublic.ycomesc.com | 没有服务器地理信息.  |
| www.example.com | IP: 92.122.244.33 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main  |
| playready.directtaps.net | IP: 13.107.246.73 所属国家: United States of America 地区: Washington 城市: Redmond  |
| data.flurry.com | 没有服务器地理信息.  |
| h.trace.qq.com | IP: 113.56.189.246 所属国家: China 地区: Hubei 城市: Huangshi  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| schemas.microsoft.com | IP: 13.107.246.73 所属国家: United States of America 地区: Washington 城市: Redmond  |
| www.openssl.org | IP: 34.49.79.89 所属国家: United States of America 地区: California 城市: Mountain View  |
| raw.githubusercontent.com | IP: 185.199.108.133 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| api1.eacysftg.xyz | IP: 154.207.77.38 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| 127.0.0.1 | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://127.0.0.1  | com/bluegay/AppContext.java  |
| https://raw.githubusercontent.com/little-5/backup/master/xblue.txt  | com/bluegay/activity/SplashActivity.java  |
| http://www.example.com  | com/flurry/sdk/ee.java  |
| https://cfg.flurry.com/sdk/v1/config  | com/flurry/sdk/cm.java  |
| https://data.flurry.com/aap.do  | com/flurry/sdk/br.java  |
| https://data.flurry.com/v1/flr.do  | com/flurry/sdk/bs.java  |
| https://cfg.flurry.com/sdk/v1/config  | com/flurry/sdk/bz.java  |
| https://api.login.yahoo.com/oauth2/device\_session  | com/flurry/sdk/eg.java  |
| https://api1.eacysftg.xyz/api.php  | d/a/b.java  |
| https://api2.eacysftg.xyz/api.php  | d/a/b.java  |
| https://api3.eacysftg.xyz/api.php  | d/a/b.java  |
| http://imgpublic.ycomesc.com/  | d/a/j/d/f.java  |
| https://github.com/danikula/AndroidVideoCache/issues/88.  | d/h/a/i.java  |
| https://github.com/danikula/AndroidVideoCache/issues/43.  | d/h/a/i.java  |
| https://github.com/danikula/AndroidVideoCache/issues.  | d/h/a/i.java  |
| http://%s:%d/%s  | d/h/a/k.java  |
| https://github.com/danikula/AndroidVideoCache/issues/134.  | d/h/a/k.java  |
| http://%s:%d/%s  | d/h/a/g.java  |
| https://exoplayer.dev/issues/player-accessed-on-wrong-thread  | d/l/a/a/m1.java  |
| http://dashif.org/guidelines/trickmode  | d/l/a/a/d2/s0/d.java  |
| http://dashif.org/guidelines/last-segment-number  | d/l/a/a/d2/s0/k/c.java  |
| http://dashif.org/guidelines/trickmode  | d/l/a/a/d2/s0/k/c.java  |
| https://x</LA\_URL>  | d/l/a/a/w1/b0.java  |
| https://x  | d/l/a/a/w1/b0.java  |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense  | d/l/a/a/w1/c0.java  |
| http://schemas.android.com/apk/res/android  | d/m/a/s.java  |
| https://h.trace.qq.com/kv  | d/w/a/a/b/b.java  |
| http://127.0.0.1:%d%s  | d/s/a/i/a.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | f/a/a/a/g.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | f/a/a/a/j.java  |
| http://www.slf4j.org/codes.html  | i/e/c.java  |
| https://github.com/TooTallNate/Java-WebSocket/wiki/Lost-connection-detection  | i/b/a.java  |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling  | io/reactivex/rxjava3/exceptions/OnErrorNotImplementedException.java  |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0  | io/reactivex/rxjava3/exceptions/UndeliverableException.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  |
| http://www.openssl.org/support/faq.html  | lib/armeabi-v7a/libijkffmpeg.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| danikula@gmail.com  | d/h/a/i.java  |
| ffmpeg-devel@ffmpeg.org  | lib/armeabi-v7a/libijkplayer.so  |

### **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: False 找到 1 个唯一证书 主题: C=Singapore, ST=Singapore, L=Singapore, O=., OU=., CN=. 签名算法: rsassa\_pkcs1v15 有效期自: 2025-06-10 23:28:34+00:00 有效期至: 2026-06-10 23:28:34+00:00 发行人: C=Singapore, ST=Singapore, L=Singapore, O=., OU=., CN=. 序列号: 0x784efe9c 哈希算法: sha256 md5值: a446fc67f2c5b6a1fb85833c655a47c6 sha1值: c5d519585e9343c13b8e4fc7f14507f94f0bdf5b sha256值: ccffaaa3687859efb6bb2f5634832ffb557f2d31cd154042a1101aae5c5c607f sha512值: b87c9786ec169b2be7c4e250d414e84aba83e973640d1aa6373cbb6add7dadfd89838da80582c0093d27d00dd5b8e4d16767d28f65d95b3db289e6d4dc7d69ea 公钥算法: rsa 密钥长度: 2048 指纹: 63fb2d96c2885ea855199c2d700f17546df8d5d0b28d9b07d7b9d6b0b27d92e5**

## **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"  |
| "modify\_pwd" : "修改密码"  |
| "modify\_pwd\_img" : "修改中…"  |
| "modify\_pwd\_success" : "密码修改成功"  |
| "pwd\_not\_same" : "前后密码不一致"  |
| "reg\_input\_pwd\_1" : "請填写密码"  |
| "reg\_input\_pwd\_2" : "請确认密码"  |
| "str\_auth\_apply" : "原创博主申请"  |
| "str\_input\_account\_user\_name" : "请输入持卡人姓名"  |
| "str\_mod\_pwd" : "修改密码"  |
| "str\_private\_letters" : "私信"  |
| "str\_user" : "用户"  |
| "video\_author" : "视频作者"  |

## **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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.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.ACCESS\_COARSE\_LOCATION | 危险 | 粗定位 | 访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置 |
| 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.READ\_PRIVILEGED\_PHONE\_STATE | 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.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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.READ\_CLIPBOARD\_IN\_BACKGROUND | 未知 | Unknown permission | Unknown permission from android reference |
| 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.WRITE\_CLIPBOARD | 未知 | Unknown permission | Unknown permission from android reference |
| 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.SYSTEM\_OVERLAY\_WINDOW | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.MOUNT\_UNMOUNT\_FILESYSTEMS | 危险 | 装载和卸载文件系统 | 允许应用程序为可移动存储安装和卸载文件系统 |
| android.permission.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |

## **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。**