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

**探色视频（ 1.0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 | 探色视频 |
| 版本 | 1.0 |
| 包名 | vxdekdlk.bhyrmdci.dtgzecpb |
| 域名线索 | 6条 |
| URL线索 | 23条 |
| APP图标 |  |
| 分析日期 | 2025年6月24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 | 探色视频.apk |
| 文件大小 | 16.11MB |
| MD5值 | 78738f2222d27ea8a2c24b5888759c3d |
| SHA1值 | 409d6ab4f101fed0b2a57959fa766c861673bf82 |
| SHA256值 | 0214abcf117053e42e256d130d72a773014a70bd1ea9e99e48a59311db6bab58 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 探色视频 |
| 包名 | vxdekdlk.bhyrmdci.dtgzecpb |
| 主活动Activity | com.youku.phone.ui.activity.WelcomeActivity |
| 安卓版本名称 | 1.0 |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| schemas.android.com | 没有服务器地理信息.  |
| lvye6.lanzoup.com | IP: 221.194.141.162 所属国家: China 地区: Hebei 城市: Langfang  |
| txtossali.oss-accelerate.aliyuncs.com | IP: 39.107.216.7 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| journeyapps.com | IP: 18.65.168.24 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| xml.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://lvye6.lanzoup.com/hbrjk  | com/amir/common/utils/Utils.java  |
| https://txtossali.oss-accelerate.aliyuncs.com/  | com/amir/common/api/ApiContents.java  |
| http://xml.apache.org/xslt  | com/blankj/utilcode/util/LogUtils.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  | com/danikula/videocache/HttpUrlSource.java  |
| https://github.com/danikula/AndroidVideoCache/issues.  | com/danikula/videocache/HttpUrlSource.java  |
| http://%s:%d/%s  | com/danikula/videocache/f.java  |
| https://github.com/danikula/AndroidVideoCache/issues/134.  | com/danikula/videocache/f.java  |
| http://%s:%d/%s  | com/danikula/videocache/HttpProxyCacheServer.java  |
| http://schemas.android.com/apk/res/android  | com/hjq/permissions/AndroidManifestParser.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  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/Completable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/Single.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/Maybe.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/Observable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/Flowable.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  |
| https://lvye6.lanzoup.com/hbrjk  | im/delight/android/webview/AdvancedWebView.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/c.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/GifTextureView.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/GifTextView.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://journeyapps.com/  | 摸瓜V1引擎  |
| https://github.com/journeyapps/zxing-android-embedded  | 摸瓜V1引擎  |

### **4.3 邮箱线索**

### **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=42DFI6, ST=SCGJ9V, L=BNHI1Q, O=C8ZLVT, OU=AHES0A, CN=16TWAI 签名算法: rsassa\_pkcs1v15 有效期自: 2024-11-21 11:57:40+00:00 有效期至: 2049-11-15 11:57:40+00:00 发行人: C=42DFI6, ST=SCGJ9V, L=BNHI1Q, O=C8ZLVT, OU=AHES0A, CN=16TWAI 序列号: 0x60b22de5 哈希算法: sha512 md5值: 9946433404a6dc5507183ad62c285203 sha1值: c43e8a3b47be8513950c0d55686ce7b792f0c54f sha256值: 3afd196c277d071f19a0739463192b3511c3b4de5f6bc87373e1b0119925ea49 sha512值: a1b34a8a634bf9508bd331eaf7a71da675c451f3f474b1c3a217d44591e0643ca3c30a9ea599f02c91907525d269a3bf11ba38c72003eeae5949ec372d205f20 公钥算法: rsa 密钥长度: 2048 指纹: 202e44c70711add0086f6bb4f27cee4b579f082d30bf163456b52d3b32aa9e91**

## **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"  |
| "library\_zxingandroidembedded\_author" : "JourneyApps"  |
| "library\_zxingandroidembedded\_authorWebsite" : "https://journeyapps.com/"  |

## **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.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.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.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.READ\_MEDIA\_IMAGES | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_SYNC\_SETTINGS | 正常 | 读取同步设置 | 允许应用程序读取同步设置,例如是否为联系人启用同步 |
| android.permission.MANAGE\_EXTERNAL\_STORAGE | 危险 | 允许应用程序广泛访问范围存储中的外部存储 | 允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用 |
| 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.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.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 |
| 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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.MODIFY\_AUDIO\_SETTINGS | 正常 | 更改您的音频设置 | 允许应用程序修改全局音频设置,例如音量和路由 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| vxdekdlk.bhyrmdci.dtgzecpb.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 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.WRITE\_SETTINGS | 危险 | 修改全局系统设置 | 允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。 |
| com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| freemme.permission.msa | 未知 | Unknown permission | Unknown permission from android reference |

## **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。**