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

**探色 视频（ 2.50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 | 2.50 |
| 包名 | amowyh.eacavmwzz.pbhq |
| 域名线索 | 5条 |
| URL线索 | 10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 | psyhLbl8636.apk |
| 文件大小 | 8.42MB |
| MD5值 | 200c473c15bb9d383e719fc539c1843f |
| SHA1值 | 8f9f2abfe544cb89cabe5a791fce9dcaf23e8a28 |
| SHA256值 | dfa7b98316f2439e2750baca9ff804841076d3b3bcd94328e70ae2bf67aca159 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 探色 视频 |
| 包名 | amowyh.eacavmwzz.pbhq |
| 主活动Activity | com.want.game.controller.activity.WelcomeActivity |
| 安卓版本名称 | 2.50 |
| 安卓版本 | 5 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| ns.adobe.com | 没有服务器地理信息.  |
| schemas.android.com | 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  |
| www.baidu.com | IP: 110.242.69.21 所属国家: China 地区: Hebei 城市: Baoding  |
| 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 |
| --- | --- |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0  | com/bumptech/glide/d.java  |
| http://www.baidu.com/s?wd=  | com/tamsiree/rxui/activity/ActivityWebView.java  |
| http://schemas.android.com/apk/res/android  | a0/b.java  |
| https://github.com/danikula/AndroidVideoCache/issues/43.  | g0/d.java  |
| https://github.com/danikula/AndroidVideoCache/issues.  | g0/d.java  |
| http://schemas.android.com/apk/res/android  | fb/d.java  |
| http://127.0.0.1:  | u2/d.java  |
| http://ns.adobe.com/xap/1.0/\u0000  | u0/g.java  |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling  | aa/c.java  |
| https://github.com/google/gson/blob/main/Troubleshooting.md  | l4/a.java  |
| https://github.com/google/gson/blob/main/Troubleshooting.md  | k4/c.java  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| danikula@gmail.com  | g0/d.java  |

### **4.4 手机号线索**

## **5. 签名证书**

**APK已签名 v1 签名: False v2 签名: True v3 签名: True 找到 1 个唯一证书 主题: C=pkwBc, ST=CCBVM, L=voRhg, O=wl1748877663706, OU=aa1748877663706, CN=bxtb 签名算法: rsassa\_pkcs1v15 有效期自: 2025-06-02 15:21:05+00:00 有效期至: 2075-05-21 15:21:05+00:00 发行人: C=pkwBc, ST=CCBVM, L=voRhg, O=wl1748877663706, OU=aa1748877663706, CN=bxtb 序列号: 0x6a61417e 哈希算法: sha512 md5值: 5b7c6a51a00b10ed11e7aab6cf04f63b sha1值: 5e504565f1b3e6acf74fadb4cdeb3b1c4234bc30 sha256值: 93b5ba6ffdf61068d03bd34e4c52f0be5b7bf7303bd5074ed85d8b68577f409d sha512值: ea5291f0238572347b769e5768ac14387cc666a9103dd09f7f7b9832eab5bd6edde76d64f9ff3cf836f7cb9fe9ef6c71354975cc4fc17e49ca162cd1a2d856a4 公钥算法: rsa 密钥长度: 4096 指纹: 9d943a4b8c5bc23d12c737c6829dbf665433130c9cd8297979a62cdedcf8a68b**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "login\_forget\_pwd" : "忘记密码"  |

## **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.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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.READ\_MEDIA\_VISUAL\_USER\_SELECTED | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_IMAGES | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_VIDEO | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_AUDIO | 未知 | Unknown permission | Unknown permission from android reference |
| 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.CALL\_PHONE | 危险 | 直接拨打电话号码 | 允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码 |
| 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.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.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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| android.permission.REORDER\_TASKS | 正常 | 重新排序正在运行的应用程序 | 允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前 |
| amowyh.eacavmwzz.pbhq.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| 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。 |
| amowyh.eacavmwzz.pbhq\_com.google.android.gms.permission.AD\_ID | 未知 | Unknown permission | Unknown permission from android reference |
| amowyh.eacavmwzz.pbhq\_com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| amowyh.eacavmwzz.pbhq\_freemme.permission.msa | 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 |

## **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。**