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

**夜猫视频（ 1.0.40.2df1cf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 | 夜猫视频 |
| 版本 | 1.0.40.2df1cf |
| 包名 | injKcNfp.rCCjELSwwt.iIRqIZNy |
| 域名线索 | 4条 |
| URL线索 | 2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 | videos61.apk |
| 文件大小 | 1.88MB |
| MD5值 | 3065f30a5dcbc25f1416adbbf7cd4714 |
| SHA1值 | cde12efb74f23db699ffa9114ffeb421fd7d23e3 |
| SHA256值 | cee01b0f9f83625d1eb2492d937c9020fe1d18896c29f0ce1b029b01039ee122 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 夜猫视频 |
| 包名 | injKcNfp.rCCjELSwwt.iIRqIZNy |
| 主活动Activity | com.anylife.framework.updateinstaller.MainActivity |
| 安卓版本名称 | 1.0.40.2df1cf |
| 安卓版本 | 12301835 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| ym.tabadminqwer1234.shop | IP: 45.155.220.209 所属国家: Korea (Republic of) 地区: Seoul-teukbyeolsi 城市: Seoul  |
| schemas.android.com | 没有服务器地理信息.  |
| ym.ymsp61xiazaiqwer5678.top | IP: 103.30.77.9 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| ym.ymsp61wzqwer5678.top | IP: 103.30.77.9 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://schemas.android.com/apk/res/android  | x/j.java  |
| https://ym.ymsp61xiazaiqwer5678.top/akplayer61.apk  | 摸瓜V1引擎  |
| https://ym.tabadminqwer1234.shop  | 摸瓜V1引擎  |
| https://ym.ymsp61wzqwer5678.top  | 摸瓜V1引擎  |

### **4.3 邮箱线索**

### **4.4 手机号线索**

## **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=(eCpldrw), ST=(RYHPABR), L=(LtacIG), O=(IGjZHNt), OU=(vEOnHstA), CN=(jutvwi) 签名算法: rsassa\_pkcs1v15 有效期自: 2025-06-11 01:00:56+00:00 有效期至: 2075-05-30 01:00:56+00:00 发行人: C=(eCpldrw), ST=(RYHPABR), L=(LtacIG), O=(IGjZHNt), OU=(vEOnHstA), CN=(jutvwi) 序列号: 0x4a67bf37b4ce6491 哈希算法: sha256 md5值: 5d113ccad23dad5e166a58b64d967d61 sha1值: 541f15a2a56e390f9c9283bcc61849af6aacc7a4 sha256值: 761bbb12d77bb3cea74081059a0dd67abf296efd8c0add3891a435ec2773e30b sha512值: 2fc3e9655a98ac035ad80a93f7079e5bfacf82bf301d712d62356322d5740f63a16135b006d662261bf8d18d277ed8ca6af9f80e87e7e3ae74182d644cc5f092 公钥算法: rsa 密钥长度: 2048 指纹: e66637f16530ab2d0a97448fcc44a4abfa583dfa513e5e83e33fdfef44b5952a**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "appKey" : "d992f48a379333b59ceae004c8151022849a27b8"  |

## **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.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| 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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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.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.REQUEST\_DELETE\_PACKAGES | 正常 |  | 允许应用程序请求删除包 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.anylife.framework.updateinstaller.MainActivity | **Schemes**: video://, **Hosts:** start,  |

**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。**