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

**好·色·先·生TV（ 1.9.0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 | 好·色·先·生TV |
| 版本 | 1.9.0 |
| 包名 | com.vlcnqibbcghun.wdkre |
| 域名线索 | 12条 |
| URL线索 | 9条 |
| APP图标 |  |
| 分析日期 | 2025年7月1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 | hsxs\_CUSKFU\_131921niv.apk |
| 文件大小 | 26.46MB |
| MD5值 | 1de2ce9d6e2494330518eec164509a5d |
| SHA1值 | 8b483f7fb1d3d275db7c13e8ff11f54796dfff9d |
| SHA256值 | b7a8f0cf1a0901a2a0eae7c366af23d6d7e38f94602968d5bbe1cb1191a2023f |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 好·色·先·生TV |
| 包名 | com.vlcnqibbcghun.wdkre |
| 主活动Activity | com.vlcnqibbcghun.wdkre.MainActivity |
| 安卓版本名称 | 1.9.0 |
| 安卓版本 | 64 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| log.kibanabox.com | IP: 119.8.31.44 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| do.hstandup.com | IP: 8.210.54.95 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| gas.engrusur.com | IP: 8.210.54.95 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| app.flowerinstall.com | IP: 104.21.14.241 所属国家: United States of America 地区: California 城市: San Francisco  |
| wz.conceptph.com | IP: 8.210.54.95 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: -  |
| api.tickshenqu.com | IP: 172.67.140.96 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: United States of America 地区: Washington 城市: Redmond  |
| www.baidu.com | IP: 180.101.49.13 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| ns.adobe.com | 没有服务器地理信息.  |
| yt.biekesitan.com | IP: 8.210.54.95 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| www.openssl.org | IP: 184.27.21.43 所属国家: Japan 地区: Tokyo 城市: Tokyo  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://app.flowerinstall.com/index.php  | com/tinstall/tinstall/TInstall.java  |
| http://www.baidu.com/  | com/tinstall/tinstall/TInstall.java  |
| https://github.com/software-mansion/react-native-screens/issues/17  | com/swmansion/rnscreens/ScreenFragment.java  |
| https://github.com/software-mansion/react-native-screens/issues/17  | com/swmansion/rnscreens/ScreenStackFragment.java  |
| https://api.tickshenqu.com  | com/vlcnqibbcghun/wdkre/MainApplication.java  |
| http://127.0.0.1:%d%s  | com/vlcnqibbcghun/wdkre/m3u8downloader/server/M3U8HttpServer.java  |
| https://github.com/googleaidog/nocode/blob/master/address.txt  | com/vlcnqibbcghun/wdkre/ServerRequest/InitServerConnect.java  |
| https://gas.engrusur.com/device/register  | com/vlcnqibbcghun/wdkre/ServerRequest/InitServerConnect.java  |
| https://yt.biekesitan.com/device/register  | com/vlcnqibbcghun/wdkre/ServerRequest/InitServerConnect.java  |
| https://wz.conceptph.com/device/register  | com/vlcnqibbcghun/wdkre/ServerRequest/InitServerConnect.java  |
| https://do.hstandup.com/device/register  | com/vlcnqibbcghun/wdkre/ServerRequest/InitServerConnect.java  |
| https://log.kibanabox.com/app/log/raw/report  | com/vlcnqibbcghun/wdkre/ServerRequest/InitServerConnect.java  |
| http://ns.adobe.com/xap/1.0/  | lib/armeabi-v7a/libstatic-webp.so  |
| http://ns.adobe.com/xap/1.0/  | lib/armeabi-v7a/libnative-imagetranscoder.so  |
| 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 |
| --- | --- |
| 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 is signed v1 signature: True v2 signature: True v3 signature: True Found 1 unique certificates Subject: C=lxpf, ST=jybh, L=gdnjiuv, O=rvyowek, OU=cphkzl, CN=wmofdx Signature Algorithm: rsassa\_pkcs1v15 Valid From: 2022-11-26 05:19:21+00:00 Valid To: 2050-04-13 05:19:21+00:00 Issuer: C=lxpf, ST=jybh, L=gdnjiuv, O=rvyowek, OU=cphkzl, CN=wmofdx Serial Number: 0x226a94f7 Hash Algorithm: sha256 md5: 7fcc5862881a95d305869ec89148439a sha1: 1797de3ab87984bdb9b5027e362c70e61dee422c sha256: b108c16c81b8c76a88b1abc79d9f1f1e991bb3f8b27e13c0d60d40dde41ee1f0 sha512: 7520308164b9810711ecede07aaf27fdd89df878103488318f3bbf6fb51016072d984e424ffbbfa924f53d202a703383625050f83f88c96a7e630b45651e3dea PublicKey Algorithm: rsa Bit Size: 2048 Fingerprint: 89103de05de7901a379df525131af0425704b964bf2fe608c824a7d86111a26d**

## **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.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.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.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\_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\_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.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.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.BLUETOOTH | 正常 | 创建蓝牙连接 | 允许应用程序连接到配对的蓝牙设备 |
| com.vlcnqibbcghun.wdkre.permission.C2D\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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 |
| com.android.vending.CHECK\_LICENSE | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.c2dm.permission.RECEIVE | 合法 | C2DM 权限 | 云到设备消息传递的权限 |
| com.sec.android.provider.badge.permission.READ | 正常 | 在应用程序上显示通知计数 | 在三星手机的应用程序启动图标上显示通知计数或徽章。 |
| com.sec.android.provider.badge.permission.WRITE | 正常 | 在应用程序上显示通知计数 | 在三星手机的应用程序启动图标上显示通知计数或徽章。 |
| com.htc.launcher.permission.READ\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在 htc 手机的应用程序启动图标上显示通知计数或徽章。 |
| com.htc.launcher.permission.UPDATE\_SHORTCUT | 正常 | 在应用程序上显示通知计数 | 在 htc 手机的应用程序启动图标上显示通知计数或徽章。 |
| com.sonyericsson.home.permission.BROADCAST\_BADGE | 正常 | 在应用程序上显示通知计数 | 在索尼手机的应用程序启动图标上显示通知计数或徽章。 |
| com.sonymobile.home.permission.PROVIDER\_INSERT\_BADGE | 正常 | 在应用程序上显示通知计数 | 在索尼手机的应用程序启动图标上显示通知计数或徽章。 |
| com.anddoes.launcher.permission.UPDATE\_COUNT | 正常 | 在应用程序上显示通知计数 | 在应用程序启动图标上显示通知计数或徽章 |
| com.majeur.launcher.permission.UPDATE\_BADGE | 正常 | 在应用程序上显示通知计数 | 在应用程序启动图标上显示通知计数或标记为固体。 |
| com.huawei.android.launcher.permission.CHANGE\_BADGE | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章。 |
| com.huawei.android.launcher.permission.READ\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章 |
| com.huawei.android.launcher.permission.WRITE\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章 |
| android.permission.READ\_APP\_BADGE | 正常 | 显示应用程序通知 | 允许应用程序显示应用程序图标徽章 |
| com.oppo.launcher.permission.READ\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在oppo手机的应用程序启动图标上显示通知计数或徽章。 |
| com.oppo.launcher.permission.WRITE\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在oppo手机的应用程序启动图标上显示通知计数或徽章。 |
| me.everything.badger.permission.BADGE\_COUNT\_READ | 未知 | Unknown permission | Unknown permission from android reference |
| me.everything.badger.permission.BADGE\_COUNT\_WRITE | 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。**