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

**直播大全（ 1.4.0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 | 直播大全 |
| 版本 | 1.4.0 |
| 包名 | com.zbdq.tvhd |
| 域名线索 | 18条 |
| URL线索 | 2条 |
| APP图标 |  |
| 分析日期 | 2025年6月13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 | 直波大全\_(原电视大全)1.4.0TV端.apk |
| 文件大小 | 17.99MB |
| MD5值 | fe07a8c23bf124df5dc27d2870e00c1b |
| SHA1值 | 8c84e5ab438056897378d76b25d1bf2ee1335649 |
| SHA256值 | e2cb868a968a4984a09653a245ba2e0eef26de93ef72fb82122a5bb543ab96e0 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 直播大全 |
| 包名 | com.zbdq.tvhd |
| 主活动Activity | com.dsdqjx.tvhd.activity.StartActivity |
| 安卓版本名称 | 1.4.0 |
| 安卓版本 | 140 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| creativecommons.org | IP: 104.20.6.134  所属国家: United States of America  地区: California  城市: San Francisco |
| alog.umeng.com | IP: 223.109.148.179  所属国家: China  地区: Jiangsu  城市: Nanjing |
| file.91kds.cn.w.kunlunar.com | IP: 61.48.83.207  所属国家: China  地区: Beijing  城市: Beijing |
| c.appjiagu.com | IP: 106.63.25.12  所属国家: China  地区: Tianjin  城市: Tianjin |
| tvapi.dsdq.cc | IP: 172.67.217.101  所属国家: United States of America  地区: California  城市: San Francisco |
| tvapisg.dsdq.cc | IP: 8.210.40.191  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| alog-g.umeng.com | IP: 8.211.35.113  所属国家: Germany  地区: Hessen  城市: Frankfurt am Main |
| 192.168.1.2 | IP: 192.168.1.2  所属国家: -  地区: -  城市: - |
| www.apache.org | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| android.googlesource.com | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| ipv6.lookup.test-ipv6.com | 没有服务器地理信息. |
| www.source-code.biz | IP: 176.9.122.15  所属国家: Germany  地区: Bayern  城市: Gunzenhausen |
| www.openssl.org | IP: 34.49.79.89  所属国家: United States of America  地区: California  城市: Mountain View |
| file.91kds.cn | IP: 61.48.83.206  所属国家: China  地区: Beijing  城市: Beijing |
| tvapius.dsdq.cc | IP: 205.185.125.56  所属国家: United States of America  地区: Nevada  城市: Las Vegas |
| alog.umeng.co | 没有服务器地理信息. |
| goo.gl | IP: 74.125.20.138  所属国家: United States of America  地区: California  城市: Mountain View |
| baidu.com | IP: 182.61.201.211  所属国家: China  地区: Beijing  城市: Beijing |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://%1$s:%2$d | 摸瓜V1引擎 |
| alog.umeng.com | 摸瓜V3引擎 |
| tvapisg.dsdq.cc | 摸瓜V3引擎 |
| alog-g.umeng.com | 摸瓜V3引擎 |
| http://c.appjiagu.com/apk/cr.html | 摸瓜V3引擎 |
| play.googleapis.com | 摸瓜V3引擎 |
| tvapi.dsdq.cc | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android | 摸瓜V3引擎 |
| www.googleapis.com | 摸瓜V3引擎 |
| http://creativecommons.org/licenses/publicdomain | 摸瓜V3引擎 |
| http://www.apache.org/licenses/LICENSE-2.0 | 摸瓜V3引擎 |
| http://www.openssl.org/support/faq.htmldual | 摸瓜V3引擎 |
| http://baidu.com/1.m3u8 | 摸瓜V3引擎 |
| http://192.168.1.2:29191 | 摸瓜V3引擎 |
| https://android.googlesource.com/toolchain/llvm | 摸瓜V3引擎 |
| ipv6.lookup.test-ipv6.com | 摸瓜V3引擎 |
| file.91kds.cn | 摸瓜V3引擎 |
| tvapius.dsdq.cc | 摸瓜V3引擎 |
| alog.umeng.co | 摸瓜V3引擎 |
| http://www.openssl.org/support/faq.html | 摸瓜V3引擎 |
| http://www.source-code.biz/base64coder/java/Base64Coder.java.txt | 摸瓜V3引擎 |
| file.91kds.cn.w.kunlunar.com | 摸瓜V3引擎 |
| https://android.googlesource.com/toolchain/clang | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res-auto | 摸瓜V3引擎 |
| goo.gl | 摸瓜V3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: False 找到 1 个唯一证书 主题: C=china, ST=hongkong, L=hongkong, O=dsdq\_studio, OU=dsdq\_studio, CN=dsdq 签名算法: rsassa\_pkcs1v15 有效期自: 2024-05-27 02:16:48+00:00 有效期至: 2123-05-04 02:16:48+00:00 发行人: C=china, ST=hongkong, L=hongkong, O=dsdq\_studio, OU=dsdq\_studio, CN=dsdq 序列号: 0x25d58884 哈希算法: sha256 md5值: 622acf68c385a8634376cbb44a2d3f5b sha1值: 3cccd73fa5cc2aa463ecc8b8499a28009d2a8248 sha256值: c156167ad5bed450ee8ac2843aa8ca9e90cbd1ebdcabc2aee34a083221baf111 sha512值: 1fe1f322f5aebf9e80b6dd1cbb189a63e977da387fef1528b767b8e32bef730d6e5f8d29db7e96a903a83ae2a98623db57efbbd9c74cf7e1ddc3519c69e6de12 公钥算法: rsa 密钥长度: 2048 指纹: 26d912952447df1260ceed302c5c52c9f21734ba4c6496ab79eead840487e680**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "file\_provider\_authorities" : "com.zbdq.tvhd.fileprovider" |
| "umeng\_key" : "6761334b8f232a05f1d82dcc" |

## **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.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.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.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.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.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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.dsdqjx.tvhd.activity.StartActivity | **Schemes**: dsdq://,  **Hosts:** dsdq.com, |

**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。**