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

**Tiktok（ 1.0.4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 | Tiktok |
| 版本 | 1.0.4 |
| 包名 | com.android.tiktok.d1681786505291105505 |
| 域名线索 | 8条 |
| URL线索 | 14条 |
| APP图标 |  |
| 分析日期 | 2025年1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 | com.android.tiktok.d1681786505291105505.apk |
| 文件大小 | 10.4MB |
| MD5值 | 021179fac8df13a37fe8bfe1104d8b62 |
| SHA1值 | 0889b27623f48d775c997e953fbb97d189073348 |
| SHA256值 | f9ff8acd39012aeb6c802ae13bf3060f15747db3281a0abfd2f4e1fec042f70a |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | Tiktok |
| 包名 | com.android.tiktok.d1681786505291105505 |
| 主活动Activity | com.grass.cstore.ui.SplashActivity |
| 安卓版本名称 | 1.0.4 |
| 安卓版本 | 104 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| schemas.microsoft.com | IP: 13.107.237.74 所属国家: United States of America 地区: Washington 城市: Redmond  |
| playready.directtaps.net | IP: 40.70.71.156 所属国家: United States of America 地区: Virginia 城市: Boydton  |
| ldtest.cn-east-1.tropcdn.com | IP: 61.160.198.42 所属国家: China 地区: Jiangsu 城市: Changzhou  |
| www.openssl.org | IP: 104.71.138.221 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| schemas.android.com | 没有服务器地理信息.  |
| github.com | IP: 20.205.243.166 所属国家: United States of America 地区: Washington 城市: Redmond  |
| data.flurry.com | IP: 69.147.80.12 所属国家: United States of America 地区: New York 城市: New York City  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://data.flurry.com/v1/flr.do  | d/f/b/t0.java  |
| https://data.flurry.com/aap.do  | d/f/b/s0.java  |
| http://www.w3.org/ns/ttml  | d/g/a/a/k0/l/c.java  |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0  | io/reactivex/exceptions/UndeliverableException.java  |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling  | io/reactivex/exceptions/OnErrorNotImplementedException.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/GifTextView.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/GifTextureView.java  |
| http://schemas.android.com/apk/res/android  | j/a/a/f.java  |
| https://github.com/danikula/AndroidVideoCache/issues/43.  | com/danikula/videocache/HttpUrlSource.java  |
| https://github.com/danikula/AndroidVideoCache/issues.  | com/danikula/videocache/HttpUrlSource.java  |
| https://github.com/danikula/AndroidVideoCache/issues/88.  | com/danikula/videocache/HttpUrlSource.java  |
| http://%s:%d/%s  | com/danikula/videocache/Pinger.java  |
| https://github.com/danikula/AndroidVideoCache/issues/134.  | com/danikula/videocache/Pinger.java  |
| http://%s:%d/%s  | com/danikula/videocache/HttpProxyCacheServer.java  |
| https://ldtest.cn-east-1.tropcdn.com/json/tt.json  | com/grass/cstore/ui/SplashActivity.java  |
| http://playready.directtaps.net/pr/svc/rightsmanager.asmx  | tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java  |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense  | tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java  |
| 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 |
| --- | --- |
| danikula@gmail.com  | com/danikula/videocache/HttpUrlSource.java  |
| 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=24, ST=24, L=242, O=24, OU=24, CN=24 签名算法: rsassa\_pkcs1v15 有效期自: 2023-01-07 09:14:41+00:00 有效期至: 2048-01-01 09:14:41+00:00 发行人: C=24, ST=24, L=242, O=24, OU=24, CN=24 序列号: 0x30b4deb3 哈希算法: sha256 md5值: 36b6d0b21446c82c2609865889688336 sha1值: 113fb07d5543b7057b15eff1f9c743fa01bf7e24 sha256值: 05d276e683a127c19cf2dc72a1d018842942207f78661d238fc8ca5baed3bae8 sha512值: cc0874f6ebd1ded779f7f593d9970d8d6894592b89fbce5e4f02d0b1b8271521510b1d81be3bf6c66dc2719651a1e7df8dc79ad9f3bac079133772a501c6d5e3 公钥算法: rsa 密钥长度: 2048 指纹: 8ae67c0f92fb219a41909f7b7b0bd26662e5d7bbe5dbd2c0c3e9e727a044974a**

## **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.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.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.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.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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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.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.SYSTEM\_ALERT\_WINDOW | 危险 | 显示系统级警报 | 允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕 |
| android.permission.SYSTEM\_OVERLAY\_WINDOW | 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。**