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

**抖阴（ 7.0.3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 | 抖阴 |
| 版本 | 7.0.3 |
| 包名 | com.tiktok.dy1008 |
| 域名线索 | 36条 |
| URL线索 | 29条 |
| APP图标 |  |
| 分析日期 | 2025年8月14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 | douyin\_zjdy6457\_7.0.3.apk |
| 文件大小 | 19.67MB |
| MD5值 | da28bb58841779ef36f1d8e88a540c19 |
| SHA1值 | 67c49030dcaabebdf8b070efc41fdd595daf01df |
| SHA256值 | bdea95a7dee6ec5ab04dd89b08a7afc842de79250bde151d0c3ae2a1f13737a6 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 抖阴 |
| 包名 | com.tiktok.dy1008 |
| 主活动Activity | com.niming.weipa.ui.splash.SplashActivity |
| 安卓版本名称 | 7.0.3 |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| loggw-exsdk.alipay.com | IP: 119.42.231.3  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| greenrobot.org | IP: 85.13.163.69  所属国家: Germany  地区: Thuringen  城市: Friedersdorf |
| mobilegw.alipaydev.com | IP: 110.75.132.131  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| pagead2.googlesyndication.com | IP: 114.250.67.38  所属国家: China  地区: Beijing  城市: Beijing |
| tmapi.tmsangewg.com | 没有服务器地理信息. |
| g74o5ibak.swr88q56hj.com | IP: 172.67.175.128  所属国家: United States of America  地区: California  城市: San Francisco |
| app.8dy.me | IP: 202.182.98.125  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| mcgw.alipay.com | IP: 123.125.216.192  所属国家: China  地区: Beijing  城市: Beijing |
| bak.dyfa3xmzzvd6ewigf7ywz79uf.com | 没有服务器地理信息. |
| schemas.android.com | 没有服务器地理信息. |
| m.alipay.com | IP: 203.209.245.74  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| mclient.alipay.com | IP: 221.204.65.242  所属国家: China  地区: Shanxi  城市: Taiyuan |
| mobilegw.alipay.com | IP: 203.209.245.129  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| ew5wk5bak.qxxbguupic.com | IP: 104.21.42.206  所属国家: United States of America  地区: California  城市: San Francisco |
| mobilegw-1-64.test.alipay.net | 没有服务器地理信息. |
| render.alipay.com | IP: 221.207.101.97  所属国家: China  地区: Heilongjiang  城市: Jiamusi |
| app.dylite.ipx.mx | 没有服务器地理信息. |
| wappaygw.alipay.com | IP: 123.125.216.192  所属国家: China  地区: Beijing  城市: Beijing |
| h5.m.taobao.com | IP: 125.38.11.130  所属国家: China  地区: Tianjin  城市: Tianjin |
| r5z99ibak.tubgbbwh27.com | IP: 104.21.27.40  所属国家: United States of America  地区: California  城市: San Francisco |
| api.buzhidaoxiesha.com | 没有服务器地理信息. |
| dyfire-01.firebaseio.com | IP: 34.120.206.254  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| bak.uogx0xftbl.com | IP: 104.21.112.1  所属国家: United States of America  地区: California  城市: San Francisco |
| schemas.microsoft.com | IP: 13.107.246.74  所属国家: United States of America  地区: Washington  城市: Redmond |
| asdsxddosbak.dr6hfub2f6.com | IP: 172.67.148.121  所属国家: United States of America  地区: California  城市: San Francisco |
| api.telegram.org | IP: 157.240.0.35  所属国家: United States of America  地区: California  城市: Menlo Park |
| playready.directtaps.net | IP: 104.45.231.79  所属国家: United States of America  地区: California  城市: San Francisco |
| xml.apache.org | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| mobilegw.stable.alipay.net | 没有服务器地理信息. |
| bak.wtk5y8b2jo.com | IP: 104.21.22.221  所属国家: United States of America  地区: California  城市: San Francisco |
| mobilegw.aaa.alipay.net | 没有服务器地理信息. |
| www.qq.com | IP: 221.198.70.47  所属国家: China  地区: Tianjin  城市: Tianjin |
| 2hw9z9bak.31rexvxfw3.com | IP: 172.67.192.147  所属国家: United States of America  地区: California  城市: San Francisco |
| ddosbak.p2jgys50gvb.com | IP: 172.67.187.8  所属国家: United States of America  地区: California  城市: San Francisco |
| bak.dy4bzju8p2tzhhmaf9sc95qpj.com | 没有服务器地理信息. |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://mobilegw.alipaydev.com/mgw.htm | c/a/b/c/a.java |
| https://mcgw.alipay.com/sdklog.do | c/a/b/c/a.java |
| https://loggw-exsdk.alipay.com/loggw/logUpload.do | c/a/b/c/a.java |
| http://m.alipay.com/?action=h5quit | c/a/b/c/a.java |
| https://wappaygw.alipay.com/home/exterfaceAssign.htm? | c/a/b/c/a.java |
| https://mclient.alipay.com/home/exterfaceAssign.htm? | c/a/b/c/a.java |
| https://mobilegw.alipay.com/mgw.htm | c/a/b/c/a.java |
| https://h5.m.taobao.com/mlapp/olist.html | c/a/b/d/a.java |
| https://pagead2.googlesyndication.com/pagead/gen\_204?id=gmob-apps | c/c/a/a/b/a/b.java |
| http://mobilegw.stable.alipay.net/mgw.htm | com/alipay/apmobilesecuritysdk/b/a.java |
| https://mobilegw.alipay.com/mgw.htm | com/alipay/apmobilesecuritysdk/b/a.java |
| http://mobilegw-1-64.test.alipay.net/mgw.htm | com/alipay/apmobilesecuritysdk/b/a.java |
| http://mobilegw.aaa.alipay.net/mgw.htm | com/alipay/apmobilesecuritysdk/b/a.java |
| https://render.alipay.com/p/s/i?scheme=%s | com/alipay/sdk/app/OpenAuthTask.java |
| https://wappaygw.alipay.com/service/rest.htm | com/alipay/sdk/app/PayTask.java |
| http://wappaygw.alipay.com/service/rest.htm | com/alipay/sdk/app/PayTask.java |
| https://mclient.alipay.com/service/rest.htm | com/alipay/sdk/app/PayTask.java |
| http://mclient.alipay.com/service/rest.htm | com/alipay/sdk/app/PayTask.java |
| https://mclient.alipay.com/home/exterfaceAssign.htm | com/alipay/sdk/app/PayTask.java |
| http://mclient.alipay.com/home/exterfaceAssign.htm | com/alipay/sdk/app/PayTask.java |
| https://mclient.alipay.com/cashier/mobilepay.htm | com/alipay/sdk/app/PayTask.java |
| http://mclient.alipay.com/cashier/mobilepay.htm | com/alipay/sdk/app/PayTask.java |
| http://xml.apache.org/xslt | com/blankj/utilcode/util/LogUtils.java |
| https://github.com/danikula/AndroidVideoCache/issues/88. | com/danikula/videocache/k.java |
| https://github.com/danikula/AndroidVideoCache/issues/43. | com/danikula/videocache/k.java |
| https://github.com/danikula/AndroidVideoCache/issues. | com/danikula/videocache/k.java |
| https://github.com/danikula/AndroidVideoCache/issues/134. | com/danikula/videocache/m.java |
| http://%s:%d/%s | com/danikula/videocache/m.java |
| http://%s:%d/%s | com/danikula/videocache/i.java |
| https://github.com/lingochamp/FileDownloader/wiki/filedownloader.properties | com/liulishuo/filedownloader/services/a.java |
| http://schemas.android.com/apk/res/android | com/flyco/tablayout/SegmentTabLayout.java |
| http://schemas.android.com/apk/res/android | com/flyco/tablayout/CommonTabLayout.java |
| http://schemas.android.com/apk/res/android | com/flyco/tablayout/SlidingTabLayout.java |
| http://app.dylite.ipx.mx | com/niming/weipa/c.java |
| http://app.8dy.me | com/niming/weipa/c.java |
| http://tmapi.tmsangewg.com/cxapi/ | com/niming/weipa/newnet/NetConfig.java |
| http://api.buzhidaoxiesha.com/cxapi/ | com/niming/weipa/utils/v.java |
| https://asdsxddosbak.dr6hfub2f6.com/mmapi/ | com/niming/weipa/utils/m0.java |
| https://g74o5ibak.swr88q56hj.com/mmapi/ | com/niming/weipa/utils/m0.java |
| https://r5z99ibak.tubgbbwh27.com/mmapi/ | com/niming/weipa/utils/m0.java |
| https://2hw9z9bak.31rexvxfw3.com/mmapi/ | com/niming/weipa/utils/m0.java |
| https://ew5wk5bak.qxxbguupic.com/mmapi/ | com/niming/weipa/utils/m0.java |
| http://app.8dy.me | com/niming/weipa/utils/y.java |
| http://www.qq.com | com/niming/weipa/utils/n0.java |
| https://api.telegram.org/bot6086117813:AAFwiL2Rn\_qZbWa\_a6DkegGeAx1gIJorQzA/sendMessage | com/niming/weipa/utils/d0.java |
| http://www.qq.com | com/niming/weipa/f/b.java |
| http://app.8dy.me | com/niming/weipa/base/BaseActivity.java |
| http://ddosbak.p2jgys50gvb.com | com/niming/weipa/g/c.java |
| http://bak.uogx0xftbl.com | com/niming/weipa/g/c.java |
| http://bak.wtk5y8b2jo.com | com/niming/weipa/g/c.java |
| http://bak.dyfa3xmzzvd6ewigf7ywz79uf.com | com/niming/weipa/g/c.java |
| http://bak.dy4bzju8p2tzhhmaf9sc95qpj.com | com/niming/weipa/g/c.java |
| http://app.dylite.ipx.mx | com/niming/weipa/g/c.java |
| https://api.telegram.org/bot743083118:AAFcQa9POAvUhMcS2\_AGFR6BKBf\_nj\_vGbE/sendMessage | com/niming/weipa/g/b.java |
| https://greenrobot.org/greendao/documentation/database-encryption/ | org/greenrobot/greendao/database/DatabaseOpenHelper.java |
| http://playready.directtaps.net/pr/svc/rightsmanager.asmx | tv/danmaku/ijk/media/exo/c/b.java |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense | tv/danmaku/ijk/media/exo/c/b.java |
| https://dyfire-01.firebaseio.com | 摸瓜V1引擎 |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| danikula@gmail.com | com/danikula/videocache/k.java |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869184 | tv/danmaku/ijk/media/player/i.java |

## **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: CN=chen, L=Shenzhen 签名算法: rsassa\_pkcs1v15 有效期自: 2024-10-08 05:01:05+00:00 有效期至: 2049-10-02 05:01:05+00:00 发行人: CN=chen, L=Shenzhen 序列号: 0x1 哈希算法: sha256 md5值: 27bb6fcb81c89a5f90cbde21682754bc sha1值: 4ae6b3511c5403adf6ec07f59067e3ff71713bf9 sha256值: 7016559146c252d2f3b77ffc35a6e7efef4f969f01633c579ef78cb86b452887 sha512值: 61d06f0cee8cfdefa15a2a584bcfb9362458941fe6202094aeb566d29d63811f1ca94330776a501f25a3959d2b35768619fa97c105e2dbf66739d8afa2654d8b 公钥算法: rsa 密钥长度: 2048 指纹: 7947a0587ee39a2b535f2ee8db5c90be3085f64813271c5de3a75efb2d1e2651**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "anonymous\_user" : "老湿" |
| "be\_gesture\_password" : "密码锁" |
| "firebase\_database\_url" : "https://dyfire-01.firebaseio.com" |
| "google\_api\_key" : "AIzaSyAPpyowD\_8PwYOJXOupAv2XaiI\_aflJCfc" |
| "google\_crash\_reporting\_api\_key" : "AIzaSyAPpyowD\_8PwYOJXOupAv2XaiI\_aflJCfc" |

## **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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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 |
| com.qti.permission.PROFILER | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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.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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| 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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.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.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.EXPAND\_STATUS\_BAR | 正常 | 展开/折叠状态栏 | 允许应用程序展开或折叠状态栏 |
| 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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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.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 |
| com.google.android.finsky.permission.BIND\_GET\_INSTALL\_REFERRER\_SERVICE | 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 |

## **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。**