MoGua

Tiktok 3.3.3.APK 分析报告

APP名称: Tiktok

包名:	com.jKFEG.DUeZd
域名线索:	21条
URL线索:	30条
邮箱线索:	1条
分析日期:	2024年9月8日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: Tiktok_3.3.3.apk
文件大小: 11.83MB
MD5值: 107074855c55cc8a8ce309dd02b519f7
SHA1值: 27859945de6eece06b3b91be27b4d962011f019a
SHA256值: 6ac87d8d8456857f74a323a41f32135a18ff91fae629242375fc6b21234243c3

APP 信息

App名称: Tiktok
包名: com.jKFEG.DUeZd
主活动Activity: com.yyds.tomato.splash.ui.SplashActivity
安卓版本名称: 3.3.3
安卓版本: 302

域名线索

域名	服务器信息
schemas.android.com	没有服务器地理信息.
stackoverflow.com	**IP**: 104.18.32.7 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
34.96.172.142	**IP**: 34.96.172.142 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692

exoplayer.dev	**IP**: 185.199.110.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
developer.apple.com	**IP**: 17.253.87.198 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
douyin.weizhen.pub	没有服务器地理信息.
github.com	**IP**: 20.205.243.166 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
wuanziyuan.lanzouj.com	**IP**: 125.39.165.87 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
ccdcapi.alipay.com	**IP**: 203.209.245.74 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
ns.adobe.com	没有服务器地理信息.

schemas.microsoft.com	**IP**: 13.107.246.74 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
d3ekdcyt77miso.cloudfront.net	**IP**: 3.165.16.225 **所属国家**: United States of America **地区**: Washington **城市**: Seattle **纬度**: 47.627499 **经度**: -122.346199
www.w3.org	**IP**: 104.18.23.19 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
xml.apache.org	**IP**: 151.101.2.132 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
www.wshifen.com	**IP**: 103.235.46.96 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
aomedia.org	**IP**: 185.199.110.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647

	经度: -79.891724
dashif.org	**IP**: 185.199.110.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
www.baidu.com	**IP**: 110.242.68.3 **所属国家**: China **地区**: Hebei **城市**: Baoding **纬度**: 38.851109 **经度**: 115.490280
wyht.cestalt.com	**IP**: 172.67.202.42 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
t.me	**IP**: 149.154.167.99 **所属国家**: United Kingdom of Great Britain and Northern Ireland **地区**: England **城市**: Warrington **纬度**: 52.184460 **经度**: -0.687590
d3cd3rn5299ol7.cloudfront.net	**IP**: 13.35.51.139 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689499 **经度**: 139.692322

URL线索

URL信息	Url所在文件
https://wuanziyuan.lanzouj.com/iVTAW0mwp3be	com/yyds/b_uiCommonWidget/bannerViews/BannerView.java
https://t.me/+jhSYhvKRxBw2MmM1	com/yyds/b_uiCommonWidget/popup/LineCheckPopup.java
https://wuanziyuan.lanzouj.com/iVTAW0mwp3be	com/yyds/e_utils/UIUtil.java
https://wuanziyuan.lanzouj.com/iVTAW0mwp3be	com/yyds/e_utils/pageUtils/UIUtils.java
http://34.96.172.142:1111/wy	com/yyds/e_config/Control.java
https://wyht.cestalt.com	com/yyds/e_config/HttpRequestConstants.java
https://d3ekdcyt77miso.cloudfront.net	com/yyds/e_config/HttpRequestConstants.java
https://d3cd3rn5299ol7.cloudfront.net	com/yyds/e_config/HttpRequestConstants.java
https://douyin.weizhen.pub	com/yyds/e_config/HttpRequestConstants.java
http://xml.apache.org/xslt	com/blankj/utilcode/util/b.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://schemas.android.com/apk/res/android	com/flyco/tablayout/CommonTabHorizontalLayout.java
https://wuanziyuan.lanzouj.com/iVTAW0mwp3be	com/kongzue/baseframework/BaseFragment.java

https://wuanziyuan.lanzouj.com/iVTAW0mwp3be	com/kongzue/baseframework/BaseActivity.java
https://exoplayer.dev/issues/cleartext-not-permitted	h3/y.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	f8/b.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	f8/d.java
https://exoplayer.dev/issues/player-accessed-on-wrong-thread	j1/i0.java
https://x</LA_URL>	n1/s.java
https://x	n1/s.java
http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	n1/t.java
https://github.com/gotev/android-upload-service	net/gotev/uploadservice/UploadServiceConfig.java
https://empty	net/gotev/uploadservice/CreateUploadRequest.java
http://stackoverflow.com/a/4410331	net/gotev/uploadservice/data/NameValue.java
http://dashif.org/guidelines/trickmode	r2/d.java
http://dashif.org/guidelines/last-segment-number	r2/d.java
http://ns.adobe.com/xap/1.0/	v1/a.java
https://wuanziyuan.lanzouj.com/iVTAW0mwp3be	widget/recharge/RechargeBottomPopup.java
https://ccdcapi.alipay.com/validateAndCacheCardInfo.json	widget/recharge/AddBankAccountPopup.java
https://wuanziyuan.lanzouj.com/iVTAW0mwp3be	ando/file/core/FileOpener.java

https://aomedia.org/emsg/ID3	f2/a.java
https://developer.apple.com/streaming/emsg-id3	f2/a.java
https://wuanziyuan.lanzouj.com/iVTAW0mwp3be	util/pageUtils/UIController.java
https://wuanziyuan.lanzouj.com/iVTAW0mwp3be	摸瓜V3引擎
http://schemas.android.com/apk/res-auto11androidx.constraintlayout.widget.ConstraintLayout	摸瓜V3引擎
https://wyht.cestalt.com	摸瓜V3引擎
http://schemas.android.com/aapt	摸瓜V3引擎
douyin.weizhen.pub	摸瓜V3引擎
http://schemas.android.com/apk/res-auto11androidx.constraintlayout.widget.ConstraintLayout((com.luck	摸瓜V3引擎
https://github.com/gotev/android-upload-service	摸瓜V3引擎
http://schemas.android.com/apk/res/android	摸瓜V3引擎
http://dashif.org/guidelines/last-segment-number	摸瓜V3引擎
http://schemas.android.com/apk/res-auto	摸瓜V3引擎
https://ccdcapi.alipay.com/validateAndCacheCardInfo.json	摸瓜V3引擎
https://aomedia.org/emsg/ID3	摸瓜V3引擎
https://douyin.weizhen.pub	摸瓜V3引擎
www.googleapis.com	摸瓜V3引擎
https://exoplayer.dev/issues/cleartext-not-permitted	摸瓜V3引擎

http://schemas.android.com/apk/res-auto11androidx.constraintlayout.widget.ConstraintLayout//com.yyds	摸瓜V3引擎
https://d3cd3rn5299ol7.cloudfront.net	摸瓜V3引擎
https://exoplayer.dev/issues/player-accessed-on-wrong-thread	摸瓜V3引擎
http://schemas.android.com/apk/res-auto%%androidx.core.widget.NestedScrollView	摸瓜V3引擎
https://d3ekdcyt77miso.cloudfront.net	摸瓜V3引擎
www.wshifen.com	摸瓜V3引擎
http://schemas.android.com/apk/res/android??com.google.android.material.datepicker.MaterialCalendarG	摸瓜V3引擎
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	摸瓜V3引擎
http://xml.apache.org/xslt	摸瓜V3引擎
https://github.com/ReactiveX/RxJava/wiki/What	摸瓜V3引擎
www.baidu.com	摸瓜V3引擎
http://schemas.android.com/apk/res/android11androidx.constraintlayout.widget.ConstraintLayout	摸瓜V3引擎
https://t.me/	摸瓜V3引擎
http://schemas.android.com/apk/res/android00com.luck.picture.lib.widget.SquareRelativeLayout	摸瓜V3引擎
http://dashif.org/guidelines/trickmode	摸瓜V3引擎
http://stackoverflow.com/a/4410331	摸瓜V3引擎

邮箱线索

邮箱地址	所在文件
tiktokgf999@gmail.com	com/yyds/b_uiCommonWidget/popup/LineCheckPopup.java

手机线索

手机号	所在文件
17512775099	o3/a.java

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=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
签名算法: rsassa_pkcs1v15
有效期自: 2008-02-29 01:33:46+00:00
有效期至: 2035-07-17 01:33:46+00:00
发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
序列号: 0x936eacbe07f201df
哈希算法: sha1
md5值: e89b158e4bcf988ebd09eb83f5378e87
sha1值: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81
sha256值: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
sha512值: 5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea303977272d17958704d89b7711292a4569
公钥算法: rsa

密钥长度: 2048
指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75

硬编码敏感信息

加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

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.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.KILL_BACKGROUND_PROCESSES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
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_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VIDEO	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
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.NEARBY_WIFI_DEVICES	未知	Unknown permission	Unknown permission from android reference
android.permission.BLUETOOTH_CONNECT	未知	Unknown permission	Unknown permission from android reference
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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
android.permission.REORDER_TASKS	正常	重新排序正在运行的应用程序	允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前

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.BIND_VPN_SERVICE	合法		VpnService 必须要求,以确保只有系统可以绑定到它
android.permission.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
android.permission.QUERY_ALL_PACKAGES	正常		允许查询设备上的任何普通应用程序,无论清单声明如何

应用内通信