MoGua

Tiktok 3.0.3.APK 分析报告

APP名称:	Tiktok

包名:	com.jKFEG.DUeZd
域名线索:	23条
URL线索:	21条
邮箱线索:	1条
分析日期:	2024年10月18日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 4_base.apk
文件大小: 12.15MB
MD5值: 65d47a84da26d5f51fd4683d227e0857
SHA1值: 839914d4023083fecff29767154f8d6138e1f103
SHA256值: 9f20460b4054e6b0371ad27c79f0e5badb667240fdd20bd0db3f0b3ccc95651f

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: 3.0.3
安卓版本: 303

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**: 17.253.87.200 **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
lh3-dz.googleusercontent.com	**IP**: 172.217.163.33 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
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**: 3.165.16.35 **所属国家**: United States of America **地区**: Washington **城市**: Seattle **纬度**: 47.627499 **经度**: -122.346199
googlehosted.l.googleusercontent.com	**IP**: 172.217.163.33 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
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**: 103.235.47.188 **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**: 110.242.68.4 **所属国家**: China **地区**: Hebei **城市**: Baoding **纬度**: 38.851109 **经度**: 115.490280
media.tenor.com	**IP**: 142.251.43.10 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
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
	IP: 13.35.51.93 **所属国家**: Japan **地区**: Tokyo

d3cd3rn5299ol7.cloudfront.net	**城市**: Tokyo **纬度**: 35.689499 **经度**: 139.692322
c.tenor.com	**IP**: 66.220.147.11 **所属国家**: United States of America **地区**: California **城市**: Menlo Park **纬度**: 37.436935 **经度**: -122.193604

URL线索

URL信息	Url所在文件
https://t.me/+jhSYhvKRxBw2MmM1	com/yyds/b_uiCommonWidget/popup/LineCheckPopup.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://exoplayer.dev/issues/player-accessed-on-wrong-thread	j1/i0.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://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
https://x</LA_URL>	n1/s.java
https://x	n1/s.java
http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	n1/t.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://aomedia.org/emsg/ID3	f2/a.java
https://developer.apple.com/streaming/emsg-id3	f2/a.java
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
play.googleapis.com	摸瓜V3引擎
lh3-dz.googleusercontent.com	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://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
googlehosted.l.googleusercontent.com	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
media.tenor.com	摸瓜V3引擎
http://stackoverflow.com/a/4410331	摸瓜V3引擎
c.tenor.com	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
15061706271	com/yyds/e_utils/secret/AESEncryptUtil.java
15061706271	com/yyds/e_utils/secret/AESEncryptUtilNew.java
18190904013	com/yyds/e_utils/upload_old/FURVideo.java
18190904013	com/yyds/e_utils/upload_old/UploadResp.java
19110415070	com/yyds/e_utils/upload_old/UploadVideoResponse.java
17041105110	com/yyds/e_utils/download/DownloadUtil.java
18081300002	com/yyds/g_model/splash/UserInfo2.java
13023308131	com/yyds/g_model/splash/UserInfo2.java
13022302131	com/yyds/g_model/splash/UserInfo2.java
15020831011	com/yyds/g_model/splash/HXConfigBean.java
14003102111	com/kongzue/baseframework/BaseFragment.java
14003102111	com/kongzue/baseframework/BaseActivity.java

17512775099	o3/a.java
18400208085	widget/recharge/AddBankAccountPopup.java
13212621320	widget/recharge/RechargeBottomPopup$onCreate$1.java
15064909041	ando/file/core/FileDirectory.java
15080006490	ando/file/core/d.java
18190904014	ando/file/core/FileMimeType.java
15460319001	ando/file/core/FileMimeType.java
19041526131	ando/file/core/FileMimeType.java
15061121070	ando/file/core/FileGlobal.java
13401402021	ando/file/core/FileUri.java
14460405081	ando/file/core/FileSizeUtils.java
19170440050	ando/file/core/FileSizeUtils.java
15061706271	ando/file/core/FileUtils.java
19041526131	ando/file/core/FileUtils.java
15460319001	ando/file/core/FileUtils.java
16071604040	ando/file/core/FileUtils.java
18170034071	ando/file/core/MediaStoreUtils.java

15011332171	util/pageUtils/UIController.java
18190904012	util/pageUtils/UIController.java
13020406071	util/pageUtils/UIController.java
19040015330	util/pageUtils/UIController.java

签名证书

APK已签名
v1 签名: True
v2 签名: False
v3 签名: False
找到 1 个唯一证书
主题: C=cn
签名算法: rsassa_pkcs1v15
有效期自: 2019-02-04 06:04:42+00:00
有效期至: 2049-03-28 06:04:42+00:00
发行人: C=cn
序列号: 0x5a25e464
哈希算法: sha1
md5值: 34b68d2b3043b3612d99edf1b6a22d0c
sha1值: 166073937926629f3ffe054be80850b7f4ceffeb
sha256值: 0905f4115d5025c1cc09f729282553f7062f9bb082219afc3d918e86b5008053
sha512值: 381a60be0aa6b96bb50826b53735088c7d36db5893426679231e0024b969c20ca574a33481ba5fd10cf2e38e9e61f0d31d1fc240bbd797c3ece38ac1d00c2fa2

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

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.tencent.tauth.AuthActivity	Schemes: tencent1106779540://,

---