



头条成人版 2.0.0.APK 分析报告



APP名称:

头条成人版

包名:	dark.syutt.SfUYY
域名线索:	8条
URL线索:	7条
邮箱线索:	1条
分析日期:	2025年6月21日
分析平台:	摸瓜APK反编译平台

文件名: 头条成人版.apk
文件大小: 23.75MB
MD5值: 1f2fb406ea4927a1b1889025e4f82ff1
SHA1值: 2c004fe1b07b4095001fa4e822d8bb76f6be903e
SHA256值: 77cccf67e2b24c666dee931afc1da2dfd662902c2672928c86874074e395d973

i APP 信息

App名称: 头条成人版
包名: dark.syutt.SfUYY
主活动Activity: com.tiktok.MainActivity
安卓版本名称: 2.0.0
安卓版本: 1

🔍 域名线索

域名	服务器信息
picsum.photos	IP: 104.26.4.30 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
developer.mozilla.org	IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568
journeyapps.com	IP: 18.65.168.24 所属国家: Japan 地区: Tokyo

	城市: Tokyo 纬度: 35.689499 经度: 139.692322
www.jsdelivr.com	IP: 104.21.23.24 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
dartbug.com	IP: 216.239.36.21 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
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
www.w3.org	IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
api.flutter.dev	IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514

URL信息	Url所在文件
https://journeyapps.com/	摸瓜V1引擎
https://github.com/journeyapps/zxing-android-embedded	摸瓜V1引擎
https://www.jsdelivr.com/using-sri-with-dynamic-files	摸瓜V2引擎
https://github.com/apvarun/toastify-js	摸瓜V2引擎
https://github.com/nodeca/pica	摸瓜V2引擎
https://github.com/richtr/NoSleep.js/issues/15	摸瓜V2引擎
https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released	摸瓜V2引擎
https://picsum.photos/200/200?random=1	摸瓜V2引擎
https://picsum.photos/167/300	摸瓜V2引擎
https://picsum.photos/200/200?random=2	摸瓜V2引擎
https://picsum.photos/200/200?random=3	摸瓜V2引擎
https://picsum.photos/200/200?random=4	摸瓜V2引擎
https://picsum.photos/200/200?random=5	摸瓜V2引擎
https://picsum.photos/200/200?random=6	摸瓜V2引擎
https://picsum.photos/200/200?random=7	摸瓜V2引擎

https://picsum.photos/200/200?random=8	摸瓜V2引擎
https://picsum.photos/200/200?random=9	摸瓜V2引擎
https://picsum.photos/200/200?random=10	摸瓜V2引擎
https://picsum.photos/200/200?random=11	摸瓜V2引擎
https://github.com/flutter/flutter/issues.	lib/arm64-v8a/libflutter.so
https://dartbug.com/52121.	lib/arm64-v8a/libflutter.so
https://api.flutter.dev/flutter/material/Scaffold/of.html	lib/arm64-v8a/libapp.so

 邮箱线索

邮箱地址	所在文件
appro@openssl.org	lib/arm64-v8a/libflutter.so

 手机线索

 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='中国', ST='北京', L='北京', O='北京', OU='北京', CN='中国'
签名算法: rsassa_pkcs1v15
有效期自: 2025-04-27 14:11:38+00:00
有效期至: 2035-04-25 14:11:38+00:00
发行人: C='中国', ST='北京', L='北京', O='北京', OU='北京', CN='中国'
序列号: 0x1cee2ef5
哈希算法: sha256
md5值: 827be03cb50d01cf3bea14cb111b062e
sha1值: 28b517d25c56ff04dbf1c731c80b97173da4ee24
sha256值: 01e9f45bd59635d4769ce840cc29cde68a20a0c4f6fdeb20acccf0edd6d48ca4
sha512值: eb58994597acfcaf0e1a4c842c8616dbca41ca6a007c1dbbef2f499dda70858cc453f8daf984acbf50cc80de54638e3ec1f469875c501dda806b90fcab04bf4
公钥算法: rsa
密钥长度: 2048
指纹: ba33d04ba6a66b61a3000496816723ff01fbbdae169c2c9accbc4b52a2652615

硬编码敏感信息

可能的敏感信息
"library_zxingandroidembedded_author" : "JourneyApps"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"

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.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_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.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_AUDIO	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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.READ_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference
dark.syutt.SfUYY.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference
android.permission.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
freemme.permission.msa	未知	Unknown permission	Unknown permission from android reference

应用内通信