



ANDROID 静态分析报告



tiktok followers: 1.01155552

分析日期: 2025-05-20 12:59:40

i应用概览

文件名称:	tiktok followers v1.0 1155552.apk
文件大小:	3.9MB
应用名称:	tiktok followers
软件包名:	MrBOOND.com
主活动:	droid.child.MainActivity
版本号:	1.01155552
最小SDK:	14
目标SDK:	19
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	52/100 (中风险)
杀软检测:	28 个杀毒软件报毒
MD5:	0daf8011220cfe2bc8405607b3ec4ee4
SHA1:	3a507885ee0c2aef45e68abc5300647320388be6
SHA256:	3bd8a9661646f6c4b8ed9c8c2b119738c57c70044ccfef4e271983429a6d26f4

📊 分析结果严重性分布

🚨 高危	⚠️ 中危	ℹ️ 信息	✅ 安全	🔍 关注
1	5	0	1	0

📦 四大组件导出状态统计

Activity组件: 3个, 其中export的有: 0个
Service组件: 1个, 其中export的有: 0个
Receiver组件: 1个, 其中export的有: 1个
Provider组件: 0个, 其中export的有: 0个

应用签名证书信息

APK已签名

v1 签名: True

v2 签名: True

v3 签名: True

v4 签名: False

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

证书MD5: e89b158e4bcf988ebd09eb83f5378e87

证书SHA1: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81

证书SHA256: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc

证书SHA512:

5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccb6b34ec4233f5f6407035810376fea303977272d17958704d9b7711292a4569

公钥算法: rsa

密钥长度: 2048

指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75

共检测到 1 个唯一证书

权限声明与风险分级

权限名称	安全等级	权限内容	权限描述
android.permission.INTERNET	危险	完全互联网访问	允许应用程序创建网络套接字。
android.permission.VIBRATE	普通	控制振动器	允许应用程序控制振动器，用于消息通知振动功能。
android.permission.ACCESS_NETWORK_STATE	普通	获取网络状态	允许应用程序查看所有网络的状态。
android.permission.READ_EXTERNAL_STORAGE	危险	读取SD卡内容	允许应用程序从SD卡读取信息。
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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
android.permission.ACCESS_FINE_LOCATION	危险	获取精确位置	通过GPS芯片接收卫星的定位信息，定位精度达10米以内。恶意程序可以用它来确定您所在的位置。
android.permission.FOREGROUND_SERVICE	普通	创建前台Service	Android 9.0以上允许常规应用程序使用 Service.startForeground，用于podcast播放（推送悬浮播放，锁屏播放）
android.permission.ACCESS_WIFI_STATE	普通	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.READ_CALL_LOG	危险	读取通话记录	允许应用程序读取用户的通话记录
android.permission.WRITE_CALL_LOG	危险	写入通话记录	允许应用程序写入（但不读取）用户的通话记录数据。

android.permission.READ_CONTACTS	危险	读取联系人信息	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可借此将您的数据发送给其他人。
android.permission.RECEIVE_SMS	危险	接收短信	允许应用程序接收短信。恶意程序会在用户未知的情况下监视或删除。
android.permission.SEND_SMS	危险	发送短信	允许应用程序发送短信。恶意应用程序可能会不经您的确认就发送信息，给您带来费用。
android.permission.READ_SMS	危险	读取短信	允许应用程序读取您的手机或 SIM 卡中存储的短信。恶意应用程序可借此读取您的机密信息。
android.permission.MANAGE_EXTERNAL_STORAGE	危险	文件列表访问权限	Android11新增权限，读取本地文件，如简历，聊天图片。
android.permission.READ_LOGS	危险	读取系统日志文件	允许应用程序从系统的各日志文件中读取信息。这样应用程序可以发现您的手机使用情况，这些信息还可能包含用户个人信息或保密信息，造成隐私数据泄露。
android.permission.READ_PHONE_STATE	危险	读取手机状态和标识	允许应用程序访问设备的手机功能。有此权限的应用程序可确定此手机的号码和序列号，是否正在通话，以及对方的号码等。
android.permission.READ_PHONE_NUMBERS	危险	允许读取设备的电话号码	允许读取设备的电话号码。这是READ PHONE STATE授予的功能的一个子集，但对即时应用程序公开。
com.huawei.android.launcher.permission.CHANGE_BADGE	未知	未知权限	来自 android 引用的未知权限。

🔒 网络通信安全风险分析

序号	范围	严重程度	描述
----	----	------	----

📄 证书安全合规分析

高危: 0 | 警告: 1 | 信息: 1

标题	严重程度	描述信息
已签名应用	信息	应用已使用代码签名证书进行签名。

🔍 Manifest 配置安全分析

高危: 0 | 警告: 3 | 信息: 1 | 屏蔽: 0

序号	问题	严重程度	描述信息
1	应用已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用允许明文网络流量（如 HTTP、FTP 协议、DownloadManager、MediaPlayer 等）。API 级别 27 及以下默认启用，28 及以上默认禁用。明文流量缺乏机密性、完整性和真实性保护，攻击者可窃听或篡改传输数据。建议关闭明文流量，仅使用加密协议。

2	应用数据允许备份 [android:allowBackup=true]	警告	该标志允许通过 adb 工具备份应用数据。启用 USB 调试的用户可直接复制应用数据，存在数据泄露风险。
3	Broadcast Receiver (droid.child.MainActivity\$ArabWareSMS) 未受保护。存在 intent-filter。	警告	检测到 Broadcast Receiver 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Broadcast Receiver 被显式导出，存在安全风险。

</> 代码安全漏洞检测

高危: 1 | 警告: 2 | 信息: 0 | 安全: 0 | 屏蔽: 0

序号	问题	等级	参考标准	文件位置
1	应用程序使用不安全的随机数生成器	警告	CWE: CWE-330: 使用不充分的随机数 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	升级会员: 解锁高级权限
2	应用程序可以读取/写入外部存储器，任何应用程序都可以读取写入外部存储器的数据	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	升级会员: 解锁高级权限
3	默认情况下，调用Cipher.getInstance("AES")将返回AES ECB模式。众所周知，ECB模式很弱，因为它导致相同明文块的密文相同。	高危	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	升级会员: 解锁高级权限

应用行为分析

编号	行为	标签	文件
00193	发送短信	短信	升级会员: 解锁高级权限
00192	获取短信收件箱中的消息	短信	升级会员: 解锁高级权限
00055	查询短信内容及电话号码来源	短信 信息收集	升级会员: 解锁高级权限
00063	隐式意图（查看网页、拨打电话等）	控制	升级会员: 解锁高级权限
00091	从广播中检索数据	信息收集	升级会员: 解锁高级权限

00048	查询短信内容	短信 信息收集	升级会员：解锁高级权限
00049	查询短信发送者的电话号码	短信 信息收集	升级会员：解锁高级权限
00191	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00128	查询用户账户信息	信息收集 账号	升级会员：解锁高级权限
00054	从文件安装其他APK	反射	升级会员：解锁高级权限
00022	从给定的文件绝对路径打开文件	文件	升级会员：解锁高级权限

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	10/30	android.permission.VIBRATE android.permission.RECORD_AUDIO android.permission.ACCESS_FINE_LOCATION android.permission.READ_CALL_LOG android.permission.WRITE_CALL_LOG android.permission.READ_CONTACTS android.permission.RECEIVE_SMS android.permission.SEND_SMS android.permission.READ_SMS android.permission.READ_PHONE_STATE
其它常用权限	6/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.FOREGROUND_SERVICE android.permission.ACCESS_WIFI_STATE

常用: 已知恶意软件广泛滥用的权限。

其它常用权限: 已知恶意软件经常滥用的权限。

🔍 恶意域名威胁检测

域名	状态	中国境内	位置信息
api.telegram.org	安全	否	IP地址: 149.154.167.220 国家: 大不列颠及北爱尔兰联合王国 地区: 英格兰 城市: 伦敦 纬度: 51.508530 经度: -0.125740 查看: Google 地图

postimg.cc	安全	否	IP地址: 149.154.167.220 国家: 法国 地区: 上法兰西岛 城市: 鲁拜克斯 纬度: 50.693710 经度: 3.174439 查看: Google 地图
------------	----	---	---

URL 链接安全分析

URL信息	源码文件
<ul style="list-style-type: none"> https://kd1s.com 	自研引擎-A
<ul style="list-style-type: none"> https://postimg.cc/ctn7rfdl https://api.telegram.org/bot https://www.google.com 	droid/child/MainActivity.java

第三方 SDK 组件分析

SDK名称	开发者	描述信息
File Provider	Android	FileProvider 是 ContentProvider 的特殊子类。它通过创建 content://Uri 代替 file:///Uri 以促进安全分享与应用程序关联的文件。

敏感凭证泄露检测

可能的密钥
Telegram_Bot_API_Key: 7700971570:AAHCrWwFKuoB2pExmmXPqHDnBzrNjxAIUqQ

免责声明及风险提示:

本报告由南明离火移动安全分析平台自动生成，内容仅供参考，不构成任何法律意见或建议。本平台对使用本产品及其内容所引发的任何直接或间接损失概不负责。本报告内容仅供网络安全研究，不得违反中华人民共和国相关法律法规。如有任何疑问，请及时与我们联系。

南明离火移动安全分析平台是一款专业的移动端恶意软件分析和安全评估框架。它能够执行静态分析和动态分析，深入扫描软件中中潜在的漏洞和安全隐患。

© 2025 南明离火 - 移动安全分析平台自动生成