南明离火
移动应用检测平台

ANDROID 静态分析报告

Thanox Pro • v5.2.7

分析日期: 2025-04-03 02:38:17

应用概览

文件名称:	Thanox_Pro_v5.2.7-row_Patched_by_youarefinished.apk
文件大小:	22.67MB
应用名称:	Thanox Pro
软件包名:	github.tornaco.android.thanos.pro
主活动:	now.fortuitous.thanos.main.NavActivity
版本号:	5.2.7
最小SDK:	24
目标SDK:	35
加固信息:	未加壳
开发框架:	Xposed
应用程序安全分数:	49/100 (中风险)
跟踪器检测:	2/432
杀软检测:	经检测，该文件安全
MD5:	7162f7825c0c68c7adc6ce13af649ff7
SHA1:	649e7b467eb8f26a04cc1[illegible]d43e0c76fd055b0ab
SHA256:	82526f7e456092[illegible]b046de083a43fa4d73d3b4a04f3df87f5c339186535

分析结果严重性分布

高危	中危	信息	安全	关注
5	39	2	3	3

四大组件导出状态统计

Activity组件：111个，其中export的有： 9个
Service组件：17个，其中export的有： 8个
Receiver组件：13个，其中export的有： 3个
Provider组件：5个，其中export的有： 2个

应用签名证书信息

二进制文件已签名
v1 签名: False
v2 签名: True
v3 签名: True
v4 签名: False
主题: C=US, ST=California, L=LA, O=Google, OU=android, CN=youarefinished
签名算法: rsassa_pkcs1v15
有效期自: 2021-11-20 12:02:04+00:00
有效期至: 2046-11-14 12:02:04+00:00
发行人: C=US, ST=California, L=LA, O=Google, OU=android, CN=youarefinished
序列号: 0x6391bab
哈希算法: sha1
证书MD5: ffad74a28f9a8acc6c7aa33b964d303f
证书SHA1: 13501c91424608b5dca1ffc857abc173488b7784
证书SHA256: 7981162e75cd768fc2efacee773c924be0c52217a86d85c4d2a8304f2bf1c4b4
证书SHA512:
e04fa5d9c90984f0fb42e5fa17eb3e9cf1ae672dcdc431bd9b473a619f09707eec8bf8c1fb4fb47b5d53b25d0dd0019ea67e53ea96814ba43d1af8351e3ff203

公钥算法: rsa
密钥长度: 1024
指纹: 4b7fbf2fb7595cf0883c1c9cd470e3c788f4f31c097250738afe7db5a84abf7f
找到 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.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_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.READ_MEDIA_VIDEO	危险	允许从外部存储读取视频文件	允许应用程序从外部存储读取视频文件。
android.permission.READ_MEDIA_AUDIO	危险	允许从外部存储读取音频文件	允许应用程序从外部存储读取音频文件。
android.permission.READ_MEDIA_IMAGES	危险	允许从外部存储读取图像文件	允许应用程序从外部存储读取图像文件。
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.POST_NOTIFICATIONS	危险	发送通知的运行时权限	允许应用发布通知，Android 13 引入的新权限。
com.android.vending.CHECK_LICENSE	未知	未知权限	来自 android 引用的未知权限。
android.permission.QUERY_ALL_PACKAGES	普通	获取已安装应用程序列表	Android 11引入与包可见性相关的权限，允许查询设备上的任何普通应用程序，而不考虑清单声明。
android.permission.USE_FINGERPRINT	普通	允许使用指纹	此常量在 API 级别 28 中已弃用。应用程序应改为请求USE_BIOMETRIC
android.permission.USE_BIOMETRIC	普通	使用生物识别	允许应用使用设备支持的生物识别方式。
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.WAKE_LOCK	危险	防止手机休眠	允许应用程序防止手机休眠，在手机屏幕关闭后后台进程仍然运行。
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	普通	Google 定义的权限	由 Google 定义的自定义权限。
com.google.android.gms.permission.AD_ID	普通	应用程序显示广告	此应用程序使用 Google 广告 ID，并且可能会投放广告。
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	普通	允许应用程序访问广告服务归因	这使应用能够检索与广告归因相关的信息，这些信息可用于有针对性的广告目的。应用程序可以收集有关用户如何与广告互动的数据，例如点击或展示，以衡量广告活动的有效性。
android.permission.ACCESS_ADSERVICES_AD_ID	普通	允许应用访问设备的广告 ID。	此 ID 是 Google 广告服务提供的唯一、用户可重置的标识符，允许应用出于广告目的跟踪用户行为，同时维护用户隐私。
android.permission.RECEIVE_BOOT_COMPLETED	普通	开机自启	允许应用程序在系统完成启动后即自行启动。这样会延长手机的启动时间，而且如果应用程序一直运行，会降低手机的整体速度。
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.startForegroup，用于podcast播放（推送悬浮播放，锁屏播放）
github.tornaco.android.thanos.pro.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
moe.shizuku.manager.permission.API_V23	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

高危: **1** | 警告: **0** | 信息: **0** | 安全: **0**

序号	范围	严重级别	描述
1	*	高危	基本配置不安全地配置为允许到所有域的明文流量。

证书安全合规分析

高危: **0** | 警告: **0** | 信息: **1**

标题	严重程度	描述信息
已签名应用	信息	应用程序使用代码签名证书进行签名

Manifest 配置安全分析

高危: **0** | 警告: **30** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用程序具有网络安全配置 [android:networkSecurityConfig=@xml/network_security_config]	信息	网络安全配置功能让应用程序可以在一个安全的，声明式的配置文件中自定义他们的网络安全设置，而不需要修改应用程序代码。这些设置可以针对特定的域名和特定的应用程序进行配置。

2	Activity (now.fortuitous.thanos.process.v2.ProcessManageActivityV2) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
3	Activity设置了TaskAffinity属性 (now.fortuitous.thanos.process.v2.ProcessManageActivityV2Delegate)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
4	Activity (now.fortuitous.thanos.apps.AppDetailsActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
5	Activity (now.fortuitous.thanos.power.SmartFreezeActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
6	Activity设置了TaskAffinity属性 (now.fortuitous.thanos.power.ShortcutStubActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
7	Activity设置了TaskAffinity属性 (now.fortuitous.thanos.power.FreezeAllShortcutActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
8	Activity设置了TaskAffinity属性 (now.fortuitous.thanos.main.OneKeyBoostShortcutActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
9	Activity设置了TaskAffinity属性 (now.fortuitous.thanos.main.PrebuiltFeatureShortcutActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
10	Activity设置了TaskAffinity属性 (now.fortuitous.thanos.launchother.LaunchOtherAppAskActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
11	Activity (now.fortuitous.thanos.launchother.LaunchOtherAppAskActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
12	Activity设置了TaskAffinity属性 (now.fortuitous.thanos.launchother.LaunchOtherAppDenyActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名

13	Activity (now.fortuitous.thanos.launchother.LaunchOtherAppDenyActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
14	Activity (now.fortuitous.thanos.launchother.AllowListActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
15	Activity (now.fortuitous.thanos.recovery.RecoveryUtilsActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
16	Service (now.fortuitous.thanos.qs.QuickConfigAppTile) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_QUICK_SETTINGS_TILE [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
17	Service (now.fortuitous.thanos.qs.ShowCurrentActivityTile) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_QUICK_SETTINGS_TILE [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
18	Service (now.fortuitous.thanos.qs.ShowNetStatsTile) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_QUICK_SETTINGS_TILE [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
19	Service (now.fortuitous.thanos.qs.PrimaryOnOffTile) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_QUICK_SETTINGS_TILE [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
20	Service (now.fortuitous.thanos.qs.TrimmolineOnOffTile) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_QUICK_SETTINGS_TILE [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。

本报告由南明离火移动安全分析平台生成

21	Service (now.fortuitous.thanos.qs.OnyKeyClearTile) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_QUICK_SETTINGS_TILE [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
22	Service (now.fortuitous.thanos.service.SuSupportService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
23	Broadcast Receiver (now.fortuitous.thanos.infinite.InfiniteZDeviceAdminReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_DEVICE_ADMIN [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
24	Content Provider (io.github.libxposed.service.XposedProvider) 未被保护。 [android:exported=true]	警告	发现 Content Provider与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
25	Activity设置了TaskAffinity属性 (github.tornaco.practice.honeycomb.locker.ui.verify.VerifyActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
26	Activity (github.tornaco.practice.honeycomb.locker.ui.verify.VerifyActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
27	Content Provider (rikka.shizuku.ShizukuProvider) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.INTERACT_ACROSS_USERS_FULL [android:exported=true]	警告	发现一个 Content Provider被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
28	Service (androidx.work.impl.background.systemjob.SystemJobService) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。

29	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
30	Activity (androidx.compose.ui.tooling.PreviewActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
31	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。

代码安全漏洞检测

高危: **4** | 警告: **7** | 信息: **2** | 安全: **2** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	应用程序记录日志信息,不得记录敏感信息	信息	CWE: CWE-532: 通过日志文件的信息暴露 OWASP MASVS: MSTG-STORAGE-3	升级会员：解锁高级权限
2	文件可能包含硬编码的敏感信息，如用户名、密码、密钥等	警告	CWE: CWE-312: 明文存储敏感信息 OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	升级会员：解锁高级权限
3	此应用程序使用SSL Pinning 来检测或防止安全通信通道中的MITM攻击	安全	OWASP MASVS: MSTG-NETWORK-4	升级会员：解锁高级权限
4	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
5	应用程序使用带PKCS5/PKCS7填充的加密模式CBC。此配置容易受到填充oracle攻击。	高危	CWE: CWE-649: 依赖于混淆或加密安全相关输入而不进行完整性检查 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	升级会员：解锁高级权限

6	此应用程序将数据复制到剪贴板。敏感数据不应复制到剪贴板，因为其他应用程序可以访问它	信息	OWASP MASVS: MSTG-STORAGE-10	升级会员：解锁高级权限
7	应用程序使用SQLite数据库并执行原始SQL查询。原始SQL查询中不受信任的用户输入可能会导致SQL注入。敏感信息也应加密并写入数据库	警告	CWE: CWE-89: SQL命令中使用的特殊元素转义处理不恰当（'SQL 注入'） OWASP Top 10: M7: Client Code Quality	升级会员：解锁高级权限
8	MD5是已知存在哈希冲突的弱哈希	警告	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-4	升级会员：解锁高级权限
9	SHA-1是已知存在哈希冲突的弱哈希	警告	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-4	升级会员：解锁高级权限
10	该文件是World Writable。任何应用程序都可以写入文件	高危	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
11	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，因为它将两个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
12	如果一个应用程序使用WebView.loadDataWithBaseURL方法来加载一个网页到WebView，那么这个应用程序可能会遭受跨站脚本攻击	高危	CWE: CWE-79: 在Web页面生成时对输入的转义处理不恰当（'跨站脚本'） OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-6	升级会员：解锁高级权限
13	此应用程序可能具有Root检测功能	安全	OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限

14	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
15	应用程序创建临时文件。敏感信息永远不应该被写进临时文件	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

Native 库安全加固检测

序号	动态库	NX(堆栈禁止执行)	PIE	STACK CANARY(栈保护)	RELRO	RPATH（指定SO搜索路径）	RUNPATH（指定SO搜索路径）	FORTIFY(常用函数加强检查)	SYMBOLS STRIPPED(裁剪符号表)
1	arm64-v8a/libtn.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 （ROP） 攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或RPATH	None info 二进制文件没有设置RUNPATH	True info 二进制文件有以下加固函数: ['__memmove_chk', '__vsnprintf_chk', '__read_chk', '__strlen_chk']	True info 符号被剥离

应用行为分析

编号	行为	标签	文件
00013	读取文件并将其放入流中	文件	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
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
00019	从给定的类名中查找方法，通常用于反射	反射	升级会员：解锁高级权限
00026	方法反射	反射	升级会员：解锁高级权限
00001	初始化位图对象并将数据（例如JPEG）压缩为位图对象	相机	升级会员：解锁高级权限
00033	查询IMEI号	信息收集	升级会员：解锁高级权限
00065	获取SIM卡提供商的国家代码	信息收集	升级会员：解锁高级权限
00066	查询ICCID号码	信息收集	升级会员：解锁高级权限
00067	查询IMSI号码	信息收集	升级会员：解锁高级权限
00104	检查给定路径是否是目录	文件	升级会员：解锁高级权限
00025	监视要执行的一般操作	反射	升级会员：解锁高级权限
00043	计算WiFi信号强度	信息收集 WiFi	升级会员：解锁高级权限
00130	获取当前WIFI信息	WiFi 信息收集	升级会员：解锁高级权限
00139	获取当前WiFi id	信息收集 WiFi	升级会员：解锁高级权限
00051	通过setData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
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限
00108	从给定的 URL 读取输入流	网络 命令	升级会员：解锁高级权限
00014	将文件读入流并将其放入 JSON 对象中	文件	升级会员：解锁高级权限
00005	获取文件的绝对路径并将其放入 JSON 对象	文件	升级会员：解锁高级权限
00112	获取日历事件的日期	信息收集 日历	升级会员：解锁高级权限
00024	Base64解码后写入文件	反射 文件	升级会员：解锁高级权限
00078	获取网络运营商名称	信息收集 电话服务	升级会员：解锁高级权限

00038	查询电话号码	信息收集	升级会员：解锁高级权限
00132	查询ISO国家代码	电话服务 信息收集	升级会员：解锁高级权限
00012	读取数据并放入缓冲流	文件	升级会员：解锁高级权限
00162	创建 InetSocketAddress 对象并连接到它	socket	升级会员：解锁高级权限
00163	创建新的 Socket 并连接到它	socket	升级会员：解锁高级权限
00096	连接到 URL 并设置请求方法	命令 网络	升级会员：解锁高级权限
00030	通过给定的 URL 连接到远程服务器	网络	升级会员：解锁高级权限
00121	创建目录	文件 命令	升级会员：解锁高级权限
00125	检查给定的文件路径是否存在	文件	升级会员：解锁高级权限
00004	获取文件名并将其放入 JSON 对象	文件 信息收集	升级会员：解锁高级权限
00114	创建到代理地址的安全套接字连接	网络 命令	升级会员：解锁高级权限
00109	连接到 URL 并获取响应代码	网络 命令	升级会员：解锁高级权限
00147	获取当前位置的时间	信息收集 位置	升级会员：解锁高级权限
00075	获取设备的位置	信息收集 位置	升级会员：解锁高级权限
00115	获取设备的最后已知位置	信息收集 位置	升级会员：解锁高级权限
00187	查询 URI 并检查结果	信息收集 短信 通话记录 日历	升级会员：解锁高级权限
00089	连接到 URL 并接收来自服务器的输入流	命令 网络	升级会员：解锁高级权限
00175	获取通知管理器并取消通知	通知	升级会员：解锁高级权限
00177	检查是否授予权限并请求	权限	升级会员：解锁高级权限
00204	获取默认铃声	信息收集	升级会员：解锁高级权限

敏感权限滥用分析

类型	匹配	权限

本报告由南明离火移动安全分析平台生成

恶意软件常用权限	2/30	android.permission.WAKE_LOCK android.permission.RECEIVE_BOOT_COMPLETED
其它常用权限	10/46	android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.READ_MEDIA_VIDEO android.permission.READ_MEDIA_AUDIO android.permission.READ_MEDIA_IMAGES android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE com.google.android.gms.permission.AD_ID android.permission.FOREGROUND_SERVICE

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
goo.gl	安全	否	**IP地址:** 142.250.72.174 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 潘杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
goo.gle	安全	否	**IP地址:** 67.199.248.13 **国家:** 美国 **地区:** 纽约 **城市:** 纽约市 **纬度:** 40.750134 **经度:** -73.997009 **查看:** Google 地图
app-measurement.com	安全	是	**IP地址:** 180.163.150.38 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.468948 **查看:** 高德地图
tornaco.github.io	安全	否	**IP地址:** 185.199.110.153 **国家:** 美国 **地区:** 宾夕法尼亚 **城市:** 加利福尼亚 **纬度:** 40.065647 **经度:** -79.891724 **查看:** Google 地图

www.paypal.me	安全	否	**IP地址:** 185.199.110.133 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
pagead2.googlesyndication.com	安全	是	**IP地址:** 180.163.150.38 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.46894 **查看:** 高德地图
t.me	安全	否	**IP地址:** 149.154.167.99 **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
raw.githubusercontent.com	安全	否	**IP地址:** 185.199.110.133 **国家:** 美国 **地区:** 宾夕法尼亚 **城市:** 加利福尼亚 **纬度:** 40.065647 **经度:** -79.891724 **查看:** Google 地图
projectlombok.org	安全	否	**IP地址:** 104.21.64.1 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
psdev.de	安全	否	No Geolocation information available.
thanox.emui.tech	安全	是	**IP地址:** 124.220.71.112 **国家:** 中国 **地区:** 北京 **城市:** 北京 **纬度:** 39.907501 **经度:** 116.397102 **查看:** 高德地图
jira.codehaus.org	安全	否	No Geolocation information available.
youtrack.jetbrains.com	安全	否	**IP地址:** 67.199.248.13 **国家:** 爱尔兰 **地区:** 都柏林 **城市:** 都柏林 **纬度:** 53.344151 **经度:** -6.267249 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• https://www.paypal.me/tornaco	now/fortuitous/app/donate/DonateActivity.java
• https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	thfxxp/akjwdoa/hatag/w2b.java
• https://play.google.com/store/apps/details?id=github.tornaco.android.thanos.pro • https://t.me/thanox_mod • https://tornaco.github.io/thanox-docs/zh/guide/profile.html • http://thanox.emui.tech/api/ • https://tornaco.github.io/thanox-docs • https://tornaco.github.io/thanox-docs/zh/guide/launch_other_app.html • https://tornaco.github.io/thanox-docs/zh/guide/bg_start.html • https://raw.githubusercontent.com/tornaco/thanox/master/	github/tornaco/android/thanos/BuildProp.java
• http://jira.codehaus.org/browse/mvel	org/mvel2/optimizers/impl/asm/ASMAccessorOptimizer.java
• www.google.com	github/tornaco/android/thanos/core/push/PushMessage.java
• https://www.paypal.me/tornaco	thfxxp/akjwdoa/hatag/a4a.java
• http://psdev.de/licensesdialog	thfxxp/akjwdoa/hatag/fd5.java
• https://youtrack.jetbrains.com/issue/kt-55980	thfxxp/akjwdoa/hatag/nl7.java
• https://app-measurement.com/a • https://app-measurement.com/s/d	thfxxp/akjwdoa/hatag/fgb.java
• https://www.paypal.me/tornaco	thfxxp/akjwdoa/hatag/hs2.java
• https://www.google.com • https://goo.gl/naoooi • www.google.com	thfxxp/akjwdoa/hatag/fib.java
• https://app-measurement.com/a • https://app-measurement.com/s	thfxxp/akjwdoa/hatag/u4b.java

• https://github.com/shahroz16/material-searchview • https://github.com/miguelcatalan/materialsearchview • https://github.com/izacus/fuzzydateformatter • https://github.com/hyb1996/auto.js-apkbuilder • https://github.com/svenwiegand/time-duration-picker • https://github.com/amrdeveloper/codeview • https://projectlombok.org/ • https://github.com/rovo89/xposed • https://github.com/matrixxun/materialbadgetextview • https://github.com/timusus/recyclerview-fastscroll • https://github.com/hsiafan/apk-parser • https://github.com/j-easy/easy-rules • https://github.com/vic797/android_native_code_view • https://github.com/topjohnwu/libsu • https://github.com/zhanghai/materialprogressbar • https://github.com/elvishew/xlog • https://github.com/spacecowboy/nononsense-filepicker	thfxxp/akjwdoa/hatag/q1b.java
• https://api.github.com	thfxxp/akjwdoa/hatag/vc6.java
• https://goo.gle/compose-feedback	thfxxp/akjwdoa/hatag/kca.java
• https://firebase.google.com/support/privacy/init-options	thfxxp/akjwdoa/hatag/lg3.java
• https://raw.githubusercontent.com/libcheck/rulibchecker-rules/master	thfxxp/akjwdoa/hatag/j05.java

Firebase 配置安全检测

标题	严重程度	描述信息

Firebase远程配置已禁用	安全	Firebase远程配置URL（ https://firebaseremoteconfig.googleapis.com/v1/projects/907184698911/namespaces/firebase:fetch?key=AIzaSyDA9rPKCSnxweegzsgadUZ9Qv6rjb6Q7TA ）已禁用。响应内容如下所示：
		{
		"state": "NO_TEMPLATE"
		}

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Jetpack Graphics	Google	利用多个 Android 平台版本中的图形工具降低画面延迟。

Jetpack DataStore	Google	Jetpack DataStore 是一种数据存储解决方案，允许您使用协议缓冲区存储键值对或类型化对象。DataStore 使用 Kotlin 协程和 Flow 以异步、一致的事务方式存储数据。
MMKV	Tencent	MMKV 是基于 mmap 内存映射的 key-value 组件，底层序列化/反序列化使用 protobuf 实现，性能高，稳定性强。
xCrash	iQIYI	xCrash 能为安卓 app 提供捕获 Java 崩溃，native 崩溃和 ANR 的能力。不需要 root 权限或任何系统权限。
Jetpack Compose	Google	Jetpack Compose 是用于构建原生 Android 界面的新工具包。Jetpack Compose 使用更少的代码、强大的工具和直观的 Kotlin API 简化并加快了 Android 上的界面开发。
Google Play Service	Google	借助 Google Play 服务，您的应用可以利用由 Google 提供的最新功能，例如地图、Google+ 等，并通过 Google Play 商店以 APK 的形式分发自动平台更新。 这样一来，您的用户可以更快地接收更新，并且可以更轻松地集成 Google 必须提供的最新信息。
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。
Jetpack App Startup	Google	App Startup 库提供了一种直接，高效的方法来在应用程序启动时初始化组件。库开发人员和应用程序开发人员都可以使用 App Startup 来简化启动顺序并显式设置初始化顺序。App Startup 允许您定义共享单个内容提供程序的组件初始化程序，而不必为需要初始化的每个组件定义单独的内容提供程序。这可以大大缩短应用启动时间。
Jetpack WorkManager	Google	使用 WorkManager API 可以轻松地调度即使在应用退出或设备重启时仍应运行的可延迟异步任务。
Firebase	Google	Firebase 提供了分析、数据库、消息传递和崩溃报告等功能，可助您快速采取行动并专注于您的用户。
Shizuku	RikkaW	Shizuku 可以帮助普通应用借助一个由 app_process 启动的 Java 进程直接以 adb 或 root 特权使用系统 API。
Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
Firebase Analytics	Google	Google Analytics（分析）是一款免费的应用衡量解决方案，可提供关于应用使用情况和用户互动度的统计数据。
Jetpack AppCompat	Google	Allows access to new APIs on older API versions of the platform (many using Material Design).
Jetpack Room	Google	Room 持久性库在 SQLite 的基础上提供了一个抽象层，让用户能够在充分利用 SQLite 的强大功能的同时，获享更稳健的数据库访问机制。

邮箱地址敏感信息提取

EMAIL	源码文件
thanox@163.com	github/tornaco/android/thanos/BuildProp.java
mahmoud.benhassine@icloud.com	thfxxp/akjwdoa/hatag/q1b.java

第三方追踪器检测

名称	类别	网址
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27

Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

敏感凭证泄露检测

可能的密钥
"key_app_feature_config_s_manage" : "key_app_feature_config_s_manage"
"key_app_feature_config_resident" : "key_app_feature_config_resident"
"key_rss_e" : "key_rss_e"
"key_feature_toggle" : "key_feature_toggle"
"key_icon_maker" : "key_icon_maker"
"key_patch_info" : "key_patch_info"
"key_app_feature_config_app_to_disable" : "key_app_feature_config_app_to_disable"
"key_developer" : "key_developer"
"key_smart_standby_bypass_if_has_n" : "key_smart_standby_bypass_if_has_n"
"key_theme_attr_preview" : "key_theme_attr_preview"
"key_launch_other_app_allow_list_settings" : "key_launch_other_app_allow_list_settings"
"key_cheat_field_imei_slot_" : "key_cheat_field_imei_slot_"
"key_app_feature_config_app_lock" : "key_app_feature_config_app_lock"
"key_build_info_app" : "key_build_info_app"
"key_app_feature_config_task_clean_up" : "key_app_feature_config_task_clean_up"
"key_cheat_field_device_id" : "key_cheat_field_device_id"
"key_about" : "key_about"
"key_cheat_field_imei_slot_1" : "key_cheat_field_imei_slot_1"
"key_ignore_system_app" : "key_ignore_system_app"
"key_app_feature_config_op_remind" : "key_app_feature_config_op_remind"
"key_cheat_field_net_country_iso" : "key_cheat_field_net_country_iso"
"key_app_stability_upkeep_enabled" : "key_app_stability_upkeep_enabled"
"key_cheat_field_line1_num" : "key_cheat_field_line1_num"
"key_bg_screen_off_clean_up_skip_fg" : "key_bg_screen_off_clean_up_skip_fg"
"key_smart_standby_stop_service" : "key_smart_standby_stop_service"
"key_original_field_net_op_" : "key_original_field_net_op_"

本报告由南明离火移动安全分析平台生成

"module_profile_pref_key_rule_engine_date_time" : "module_profile_pref_key_rule_engine_date_time"
"key_app_feature_config_app_info_detailed" : "key_app_feature_config_app_info_detailed"
"key_enable_toast_info" : "key_enable_toast_info"
"key_app_feature_config_block_uninstall" : "key_app_feature_config_block_uninstall"
"key_app_list_item" : "key_app_list_item"
"key_enable_nr_t" : "key_enable_nr_t"
"module_locker_key_re_verify_on_app_switch" : "key_re_verify_on_app_switch"
"key_strategy" : "key_strategy"
"key_app_feature_config_block_clear_data" : "key_app_feature_config_block_clear_data"
"key_original_field_android_id" : "key_original_field_android_id"
"module_profile_pref_key_rule_engine_from_shortcut" : "module_profile_pref_key_rule_engine_from_shortcut"
"key_original_field_meid_slot_3" : "key_original_field_meid_slot_3"
"key_smart_freeze_tips" : "key_smart_freeze_tips"
"key_original_field_net_op_1" : "key_original_field_net_op_1"
"module_profile_pref_key_rule_engine_danmu" : "module_profile_pref_key_rule_engine_danmu"
"key_app_feature_config_smart_freeze" : "key_app_feature_config_smart_freeze"
"key_cheat_field_sim_op_name" : "key_cheat_field_sim_op_name"
"key_original_field_sim_op_1" : "key_original_field_sim_op_1"
"key_smart_standby_bypass_if_has_visible_windows" : "key_smart_standby_bypass_if_has_visible_windows"
"key_cheat_field_android_id" : "key_cheat_field_android_id"
"key_enable_battery_drain_app_reminging" : "key_enable_battery_drain_app_reminging"
"key_original_field_sim_op_name_1" : "key_original_field_sim_op_name_1"
"key_config_template_category" : "key_config_template_category"
"key_original_field_sim_op_3" : "key_original_field_sim_op_3"
"google_app_id" : "1:907184698911:android:534d97f74ea89a81b8872a"
"key_original_field_line1_num" : "key_original_field_line1_num"
"badge_app_idle" : "idle"
"key_restore_default" : "key_restore_default"
"key_open_source_license" : "key_open_source_license"
"key_original_field_meid_slot_2" : "key_original_field_meid_slot_2"

"key_app_feature_config_privacy_cheat" : "key_app_feature_config_privacy_cheat"
"key_smart_freeze_screen_off_clean_up" : "key_smart_freeze_screen_off_clean_up"
"key_original_field_sim_serial" : "key_original_field_sim_serial"
"module_profile_pref_key_rule_engine_automation" : "module_profile_pref_key_rule_engine_automation"
"key_app_feature_config_recent_task_blur" : "key_app_feature_config_recent_task_blur"
"module_profile_pref_key_rule_engine_push" : "module_profile_pref_key_rule_engine_push"
"module_locker_key_re_verify_on_task_removed" : "key_re_verify_on_task_removed"
"key_recent_task_blur_mode" : "key_recent_task_blur_mode"
"key_crash" : "key_crash"
"key_smart_standby_block_bg_service_start" : "key_smart_standby_block_bg_service_start"
"com.google.firebase.crashlytics.mapping_file_id" : "1aa0f9ebf79448e8aea05b303215eda7"
"key_app_feature_config_start_restrict" : "key_app_feature_config_start_restrict"
"key_bg_screen_off_clean_up_skip_recent_task" : "key_bg_screen_off_clean_up_skip_recent_task"
"key_app_feature_config_ops" : "key_app_feature_config_ops"
"key_cheat_field_sim_serial" : "key_cheat_field_sim_serial"
"key_original_field_imei_slot_" : "key_original_field_imei_slot_"
"key_original_field_net_op_name_" : "key_original_field_net_op_name_"
"key_bg_screen_off_clean_up_delay" : "key_bg_screen_off_clean_up_delay"
"key_enable_logging" : "key_enable_logging"
"key_app_feature_config_bg_restrict" : "key_app_feature_config_bg_restrict"
"key_app_feature_config_a_manage" : "key_app_feature_config_a_manage"
"key_cheat_field_net_op" : "key_cheat_field_net_op"
"key_bg_screen_off_clean_up_skip_audio" : "key_bg_screen_off_clean_up_skip_audio"
"key_bg_restrict_show_notification" : "key_bg_restrict_show_notification"
"key_feedback" : "key_feedback"
"key_show_net_stat" : "key_show_net_stat"
"module_locker_key_verify_method" : "module_locker_key_verify_method"
"key_app_feature_config_p_manage" : "key_app_feature_config_p_manage"
"google_crash_reporting_api_key" : "AIzaSyDA9rPKCSnxweegzsgadUZ9Qv6rjb6Q7TA"
"key_original_field_device_id" : "key_original_field_device_id"

"key_general" : "key_general"
"key_settings_record_viewer" : "key_settings_record_viewer"
"google_api_key" : "AIzaSyDA9rPKCSnxweegzsgadUZ9Qv6rjb6Q7TA"
"key_app_list_item_show_version" : "key_app_list_item_show_version"
"key_open_source" : "key_open_source"
"key_sensor_off" : "key_sensor_off"
"key_cheat_field_meid_slot_2" : "key_cheat_field_meid_slot_2"
"key_app_feature_config_r_manage" : "key_app_feature_config_r_manage"
"key_cheat_field_imei_slot_2" : "key_cheat_field_imei_slot_2"
"key_original_field_sim_country_iso" : "key_original_field_sim_country_iso"
"key_app_feature_config_screen_on_notification" : "key_app_feature_config_screen_on_notification"
"key_enable_global_white_list" : "key_enable_global_white_list"
"key_smart_standby_unbind_service" : "key_smart_standby_unbind_service"
"key_persist_all_apps" : "key_persist_all_apps"
"key_original_field_net_country_iso" : "key_original_field_net_country_iso"
"key_donate" : "key_donate"
"key_original_field_sim_op_name_3" : "key_original_field_sim_op_name_3"
"key_power" : "key_power"
"key_app_ui" : "key_app_ui"
"key_original_field_imei_slot_2" : "key_original_field_imei_slot_2"
"key_enable_power_save" : "key_enable_power_save"
"key_original_field_net_op_3" : "key_original_field_net_op_3"
"key_app_feature_config_smart_standby" : "key_app_feature_config_smart_standby"
"key_original_field_net_op_name_3" : "key_original_field_net_op_name_3"
"module_locker_key_verify_method_custom_pattern" : "module_locker_key_verify_method_custom_pattern"
"key_original_field_sim_op_name_" : "key_original_field_sim_op_name_"
"key_bg_screen_off_clean_up_skip_notification" : "key_bg_screen_off_clean_up_skip_notification"
"key_original_field_meid_slot_1" : "key_original_field_meid_slot_1"
"key_smart_freeze_dol_tips" : "key_smart_freeze_dol_tips"
"key_app_icon_pack" : "key_app_icon_pack"

本报告由南明离火移动安全分析平台生成

"key_smart_freeze_method" : "key_smart_freeze_method"
"key_original_field_net_op_name_2" : "key_original_field_net_op_name_2"
"key_cheat_field_meid_slot_" : "key_cheat_field_meid_slot_"
"module_locker_key_re_verify_on_screen_off" : "key_re_verify_on_screen_off"
"key_original_field_net_op_2" : "key_original_field_net_op_2"
"key_original_field_net_op_name_1" : "key_original_field_net_op_name_1"
"key_original_field_sim_op_2" : "key_original_field_sim_op_2"
"key_cheat_field_meid_slot_3" : "key_cheat_field_meid_slot_3"
"key_cheat_field_sim_op" : "key_cheat_field_sim_op"
"key_nr_apps" : "key_nr_apps"
"key_smart_standby_set_inactive" : "key_smart_standby_set_inactive"
"key_contributors" : "key_contributors"
"module_profile_pref_key_rule_engine_custom_su" : "module_profile_pref_key_rule_engine_custom_su"
"key_app_theme" : "key_app_theme"
"key_process_manage_ui_v2" : "key_process_manage_ui_v2"
"key_app_feature_config_enable_package_on_launch" : "key_app_feature_config_enable_package_on_launch"
"key_build_info_server" : "key_build_info_server"
"key_launch_other_app" : "key_launch_other_app"
"key_cheat_field_installed_apps" : "key_cheat_field_installed_apps"
"key_data_restore" : "key_data_restore"
"key_recent_task_exclude_settings" : "key_recent_task_exclude_settings"
"key_original_field_meid_slot_" : "key_original_field_meid_slot_"
"key_app_feature_config_app_to_enable" : "key_app_feature_config_app_to_enable"
"module_profile_pref_key_rule_engine_su" : "module_profile_pref_key_rule_engine_su"
"key_original_field_sim_op_" : "key_original_field_sim_op_"
"key_smart_freeze_enable_on_launch_by_default" : "key_smart_freeze_enable_on_launch_by_default"
"user" : "User"
"key_email" : "key_email"
"key_data_backup" : "key_data_backup"
"key_cheat_field_sim_country_iso" : "key_cheat_field_sim_country_iso"

本报告由南明离火移动安全分析平台生成

"key_enable_nr_clip" : "key_enable_nr_clip"
"key_original_field_imei_slot_3" : "key_original_field_imei_slot_3"
"key_cheat_field_net_op_name" : "key_cheat_field_net_op_name"
"key_use_round_icon" : "key_use_round_icon"
"key_original_field_sim_op_name_2" : "key_original_field_sim_op_name_2"
"key_smart_freeze_screen_off_clean_up_delay" : "key_smart_freeze_screen_off_clean_up_delay"
"module_locker_key_white_list_components" : "module_locker_key_white_list_components"
"key_data" : "key_data"
"key_enable_nr_n" : "key_enable_nr_n"
"key_original_field_imei_slot_1" : "key_original_field_imei_slot_1"
"key_app_list_item_show_pkg" : "key_app_list_item_show_pkg"
"key_cheat_field_show_cheated_app_notifications" : "key_cheat_field_show_cheated_app_notifications"
"key_cheat_field_imei_slot_3" : "key_cheat_field_imei_slot_3"
"key_cheat_field_meid_slot_1" : "key_cheat_field_meid_slot_1"
b8d7f823f339009301257bd69cb446c7
5593437D-7F24-42F2-8D17-3345775D3FC6
99c71a2d575e9f2c2c83e3ffd586a3b6
86254750241babac4b8d52996a675549
fbb0fffe49334e78f6f901c2a144314f
D2B275BF-53AC-4DCB-9144-467CB2D989AF
A92E8A9A743FE6648E2E4743F0A089E9EB4A568F
39A5DC32-B10D-4370-A896-A9A309256885
db5475a77c9685744ac9616fad38ed
8B62FB022B2ABB5DFCAD97BCFD8118EE
51480c4c32f346553bc1cf03fd8435e7
D78A8F3D-0FC2-4A45-A913-280DC73598E0
622e5271bafc9fcab7b2f78695caa5cb
b0ff815d681ccd468040c27a4cffcae5
E686ED30-C7A4-4D49-8BFF-8E4D7B4B1CF0
470fa2b4ae81cd56ecbcda9735803434cec591fa

82D094AC-95B1-40C9-B037-8A88F8309AE6
25cc0926b09a6e73798de05977c420f7
7E4BEEE5A92DCDDD48B5B7798CDEC79A
58bf0894-aa4c-4d70-b5b1-93e4f55ce578
58BCDEF326ABAF65A98AF7B881FA9C059752002E
B75F00CB-D413-4E35-BBA1-80BB6DD0ADBB
E8EB535E-A0D9-42D9-A73F-496B1EB0B9E7
Y29tLmFuZHJvaWQudmVuZGluZy5saWNlbnNpbmcuSUxpY2Vuc2luZ1NlcnZpY2U=
2C318A629B22F56EA6665AC81F0210CB
5f50452607bfbf8ec389f86233827ef0
5bb3d89b653a4cebe626d5bd5a5ec548
D878029F-1D75-42EF-9DEA-48B552172C3D
9d94be6a253e25a9855afd3c92d0f1b4
878dff329d1d60c12c9240751ae84dec
6E132918-0B02-43DA-8B33-A2BB62643EF2
C60FC34B-DC18-4087-845F-1D6AAE118D16
74EC7A26-5597-4C37-BD3C-A827A074EC02
16d5c7e8d44ba3546f725b156a925cdb
57487bf00923e37ac3620f8724e16e2b
a-95ed6082-b8e9-46e8-a73f-ff56f00f59d
8a70d3db86047d5900f6784b2 f79181

Google Play 应用市场信息

标题: Thanox Pro

评分: 4.31 **安装:** 5,000+ **价格:** 4.59 **Android版本支持:** **分类:** 工具 **Play Store URL:** github.tornaco.android.thanos.pro

开发者信息: Tornaco, Tornaco, 北京昌平回龙观, https://tornaco.github.io/Thanox/, thanox@163.com,

发布日期: None **隐私政策:** Privacy link

关于此应用:

Beta计划已支持Android 13+，请随意加入！ Thanox是一个系统管理工具，在系统隐私和系统优化方便提供了便利的功能。包含应用的权限管理，后台启动管理，后台运行管理，以及强大的情景模式和独特新奇的移花接木功能。 玩机小白不建议使用！ 不能接受Magisk、Xposed模块的不稳定性的，不建议使用！ 更新之前建议做好救砖无法启动的准备。

免责声明及风险提示: