南明离火
移动应用检测平台

ANDROID 静态分析报告

Next Toppers • v21.6

分析日期: 2025-04-01 22:16:47

应用概览

文件名称:	Next Toppers v21.6.apk
文件大小:	14.36MB
应用名称:	Next Toppers
软件包名:	com.NextToppers.ABhi
主活动:	.MainActivity
版本号:	21.6
最小SDK:	24
目标SDK:	27
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	46/100 (中风险)
杀软检测:	4 个杀毒软件报毒
MD5:	3a6104b462284c14a482d05cb1c08249
SHA1:	e4bf3531ab5b1a2193d957c6405f00b3a686ff3f
SHA256:	ccb8f53ea6692a7fc0277cfd8d7af22587087d907b1ef9e94cc03d82c897c8a4

分析结果严重性分布

高危	中危	信息	安全	关注
4	1	2	2	0

四大组件导出状态统计

Activity组件：11个，其中export的有：1个
Service组件：3个，其中export的有：1个
Receiver组件：4个，其中export的有：3个
Provider组件：1个，其中export的有：1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=IN, ST=Leecher, L=Noob, O=Lover, OU=Andhbhakt, CN=CuteJiJa
签名算法: rsassa_pkcs1v15
有效期自: 2023-10-19 19:01:35+00:00
有效期至: 2048-10-12 19:01:35+00:00
发行人: C=IN, ST=Leecher, L=Noob, O=Lover, OU=Andhbhakt, CN=CuteJiJa
序列号: 0x1bb48620
哈希算法: sha512
证书MD5: 2225397c5e51d5a8d83605bc4039dac2
证书SHA1: 2807a1086da73e744d6245bc507d5c8600e78b75
证书SHA256: b1fb4da4fb0c260a02db954b062c5b2400ac670697a1e2389129a6c24844ba25
证书SHA512:
e9f7ee48b9cd7961d0417fbaf271ae9a4a0d852b52bf1800d9bae2298a6f682e2fbea4cac93a775a3fd998dc52573140fd998ac02eb19f64ab7452b514b36c3a

公钥算法: rsa
密钥长度: 2048
指纹: f40c41fcf9ec32b21e43c089a12bfa34e9dad4a109208b4091082659e02ec910
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.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.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.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.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。
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.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.c2dm.permission.RECEIVE	普通	接收推送通知	允许应用程序接收来自云的推送通知。
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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
net.dinglisch.android.tasker.PERMISSION_RUN_TASKS	未知	未知权限	来自 android 引用的未知权限。
android.permission.BLUETOOTH_ADMIN	危险	管理蓝牙	允许程序发现和配对新的蓝牙设备。
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.SYSTEM_ALERT_WINDOW	危险	弹窗	允许应用程序弹窗。 恶意程序可以接管手机的整个屏幕。
android.permission.CHANGE_WIFI_STATE	危险	改变Wi-Fi状态	允许应用程序改变Wi-Fi状态。

android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	普通	使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS 的权限	应用程序必须拥有权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
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.CAMERA	危险	拍照和录制视频	允许应用程序拍摄照片和视频，且允许应用程序收集相机在任何时候拍到的图像。
android.permission.BLUETOOTH	危险	创建蓝牙连接	允许应用程序查看或创建蓝牙连接。
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置方面的数据。恶意应用程序可借此破坏您的系统配置。
android.permission.READ_SETTINGS	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	严重级别	描述

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: **2** | 警告: **8** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用程序已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用程序打算使用明文网络流量，例如明文HTTP，FTP协议，DownloadManager和MediaPlayer。针对API级别27或更低的应用程序，默认值为“true”。针对API级别28或更高的应用程序，默认值为“false”。避免使用明文流量的主要原因是缺乏机密性，真实性和防篡改保护；网络攻击者可以窃听传输的数据，并且可以在不被检测到的情况下修改它。
2	应用程序数据可以被备份 [android:allowBackup=true]	警告	这个标志允许任何人通过adb备份你的应用程序数据。它允许已经启用了USB调试的用户从设备上复制应用程序数据。
3	Activity (.MainActivity) 容易受到 StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (27) 更新到 29 或更高版本以在平台级别修复此问题。

4	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: com.google.android.c2dm.permission.SEND [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。
5	Content Provider (com.google.classes.DefaultProvider) 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。
6	Service (com.google.service.RemoteService) 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。
7	Broadcast Receiver (com.google.classes.DefaultProvider$DefaultReceiver) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
8	Activity (com.google.classes.DefaultProvider$MyActivity) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (27) 更新到 29 或更高版本以在平台级别修复此问题。
9	Activity (com.google.classes.DefaultProvider$MyActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
10	Broadcast Receiver (com.google.classes.FakeCamera$FakeCameraReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。

代码安全漏洞检测

高危: **1** | 警告: **2** | 信息: **1** | 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	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

3	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
4	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
5	启用了调试配置。生产版本不能是可调试的	高危	CWE: CWE-919: 移动应用程序中的弱点 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-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
00026	方法反射	反射	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
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
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
00013	读取文件并将其放入流中	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	5/30	android.permission.WAKE_LOCK android.permission.VIBRATE android.permission.SYSTEM_ALERT_WINDOW android.permission.CAMERA android.permission.WRITE_SETTINGS
其它常用权限	10/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.READ_EXTERNAL_STORAGE android.permission.ACCESS_WIFI_STATE com.google.android.c2dm.permission.RECEIVE android.permission.FLASHLIGHT android.permission.BLUETOOTH_ADMIN android.permission.CHANGE_WIFI_STATE android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS android.permission.BLUETOOTH

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
next-topper-bec4b-default-rtdb.firebaseio.com	安全	否	**IP地址:** 35.201.97.85 **国家:** 美国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099730 **经度:** -94.578568 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• https://next-topper-bec4b-default-rtdb.firebaseio.com	自研引擎-S

Firebase 配置安全检测

标题	严重程度	描述信息

Firebase数据库未授权访问	危险	位于 https://next-topper-bec4b-default-rtdb.firebaseio.com/.json 的 Firebase 数据库在没有任何身份验证的情况下暴露在互联网上。响应内容如下所示：
		{
		"test": {
		"-OJ-7HHsgqeUwxGiOC0W": {
		"email": "mr-k0anti@wearehackerone.com",
		"message": "this firebase has been found unprotected by mr-k0anti",
		"username": "mr-k0anti"
		}
		}
		}

Firebase远程配置已禁用	安全	Firebase远程配置URL （ https://firebaseremoteconfig.googleapis.com/v1/projects/908552751484/namespaces/firebase:fetch?key=AIzaSyCk5TlIHg2tfxZ49NZpV2UN81XnZTEUK-c ） 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

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。
Jetpack Media	[Google]()	与其他应用共享媒体内容和控件。已被 media2 取代。
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，获享更强健的数据库访问机制。

🔑 敏感凭证泄露检测

可能的密钥
"firebase_database_url" : "https://next-topper-bec4b-default-rtdb.firebaseio.com"
"google_api_key" : "AIzaSyCk5TlIHg2tfxZ49NZpV2UN81XnZTEUK-c"
"google_app_id" : "1:908552751484:android:729d69900910af242a7cf9"
n4EPbNtXMNgNzgO0pJjfLc54Q9QnnUoOaUIYAPh3WtjkGkOhzM+wXdSDCxzgR/iipbLkIXQNuy2sY
NjsrA1QwNTBHXTs6aEALIGwiQk87OClMXDAm
n5cgy1k4ASf3A5cAFuJXKKaF9KpBPgDvM7KP4g1olGkCMADcBJwb2p8KOMvMPoUaCCBpALgfmBba
n+ZGkpzrId6ak3RlpLm1xz5kePn0QOiZ5A3H9GIMf80wHeZ+l7QZo6Qh7HwFWh45t3iCsKEiATkXo
ATwvXhgTMSdZTScxZkRLdTopWRgUOCpCTzAwaAMWdHVmFxE=
GzsyDW0lMCdZXTE0H0nMe3poAxl0dHwAEA==
Y29tLmFwcGxpc2RvLmFwcGNsb25lci5jbGFzc2VzLnNlY29uZGFyeQ==
PSAyXUtve2lMWj09IVhKIGVyHhYyPTjFT7oL0IXFAdrYG0ZAA97fQcHAwBoAns=
PDArA1E7ICNfVjAgaElXIjoqQlkxeitMVjQzI18=
DDszDVA0IiNDHyF0FlkKNjwnM0xdAdDQXUWJ1IbPXQfSEx7emcMGG98
PDArA1E7ICNfVjAgaElXIjoqQlkxeitMVjQzI18WJTgzXg==
njY7OJr0nLOpwiHpt4BgUi6Q3PCZi8h1SSjpR0vaM9LxEkHSMh69dMRHz7agGfUSlhqhzKG50dHiJ
nJBUhcameExFCkEhow4NEJCIST32oW4TEg3ogbg+NklAaSl1KFG2lNGlJimqU0/P3sGZ0nLNn9qx9
n+AxcP7sT90e4wsx2lRLoVkh6KOeOs1Z8IekeSce3yWOWpL9T0tglaWGb+w/x8OmdyoJXQPCPkDTc

nnEP6ewBXAAflTa7oYJUhwJEetmtGlXCvCL+m3LNYblk7NznmCXnpivcDfARoGWQz+wH3PlZaTRjs
n78C8qoIPewXwOcK9V1kHzIi2qlRGLEB3LDSVx3KgP3rEWSlxHzAZt8OgljPjEvkcWGJmr4dyoA/A
nYfAXeebVnyGCJC3JuHeGh1/vFx2nMjvh++m8iTvax9jMPgHOBv5OMXlE0tICyhR86SYXchted46h
NDoiX1c8MGhdXSc5L15LPDsoA2gaBxJydhoAD2txFhUSZHcbBw==
GztmZFYhMTRDXSF0BUJWOzElWVE6OmgDFg==
nbmhoaGhoaMig8M5S0hTgENxxYMk8kg9v+nAPg34ys79CB6GnkDt8Q5KGon97Er8nPxu1LWU8UsbB
BjsrSEw9PShKGAIxKFkYAiYpQ197emcMGG98
MzsoWUt6JilPVyE7GUBdMT0zQGc7IStPXScnaFlMMw==
MzsoWUt6JitIXDwhK0RMNDgvThYhICA=
Fjs2RF0xdBVYWzYxNV5eIDgqVBhvfQ==
PSAyXUtve2ldVDQtaEpXOjMqSBY2OysCSyE7NEgXNCQ2XhcxMTJMUTkneURcaD0iQBY8OjJISjsxMgNcOi[illegible]oQVc0MGhAWTs1IUhK
GztmQ10hIylfU3U3KUNWMDcyRFc7dCdbWTw4J09UMHpoAxl0
NjsrA0s+MTJOUCI1NEgWJzErQlx7FQV5cRoaGWN9AgsCaHoAExlhdxI=
nZWtL6D4gxleEjTgRsiZreZ8nNC9qRwx6BC0WIWuyNpCzY/YJalfUgLEw4LPgFs0T[illegible]J4BOD
MzsoWUt6MylCXzkxJEJUMTsqSRYhICA=
PSAyXUtve2lZFjgxaWBZMQsebHo9PQ==
NDoiX1c8MGhdXSc5L15LPDsoA2oQFQJyfQ0AA392FBgZfmw[illegible]BgdqfQ==
NDoiX1c8MGhEViExKFkWNDcyRFc7ehBkfQI=
PSAyXUtve2lMWj09IVhKIGVyHhYyPTJFTTd6L0i[illegible]YG[illegible]ZAA97fQcHAwBo[illegible]SEAhACldSDAmBExMNjwjXhc=
n2olwU2SXZdN1AtzmEfwtI+49oSQRs[illegible]T9EUqAMoahx3rYvpW8M[illegible]wFzglxT7WyQ97eOMmX0M
noCasBeYxdhEKpQwBfJ50pb7[illegible]abgN[illegible]ki7C4F0QoQ4DC2[illegible]lIh[illegible]Fm4VchWLJb0nGeaa3F9QicidEUf
FBEVAnsXF2l9cxYHc31ZM[illegible]AvQ[illegible]8=
nd7qkHRn2vssM[illegible]VdE3[illegible]Vka86jITBsDMNu[illegible]GM[illegible]mj[illegible]a9lhqhj7ifnqmsbvLfG5CH0PGDUkNXMvqV4
AQYHbnN1PShL[illegible]U6KVkYNCInRFQ0Nj[illegible]
MzsoWUt6[illegible]YSjwxNHJWMCMZT1c5M[illegible]ZTDM=
nCXBIWXMAAC4jAAAuIwF4pT9[illegible]AA[illegible]Hk0lEQVR42u2dW6wdUxjHf98pirqURElc6tIihKZOL0rqLiEl
nJ2k5MBi65DXhQ6iwE[illegible]BH[illegible]BP6FLXhB3AUWa2u5ImSNKdNMFPcp2Z7YYKaoCkmcDa0CWuCVuBu8zs
nzHYAd4WOR[illegible]A[illegible]1sxkhgw8jJi6SHgPuC+lQifwMvAu8ZGavhnYmptVM+CLc4RUzgEm42eiehP2E
nsw0N[illegible]Q0FUesnYpIOBE4BTsKt2ewLTEyYDCfK0MfeUYzYO8ROjmQsca3o2lrYFJm2AXuAL81s
GTshSl0ndCdBSjA1IlQYJyEoQ1E7Mw==

aScrTFQ5amZtdTQwGXV5FzwvDUQpdGVjeRQZZnl3dQcTY3l1HAlqeWl7NUBZOTh4
NiYjTEwwGSNJUTQHKVhKNjFmeFYmITZdVycgl0kYIS02SAJ1
nEWYD347Bz/VmtmYM96cSWoCWRCLMJVsE38naNXQ+k30gdExyI+kVj3Z1fpu0Jssdnp1GWxEkHSTp
BTgjTEswdAxCUTt0CVhKdQAjQV0yJidAGBY8J0NWMDhmWVd1EyNZGBsxMQ1tJTAnWV17emcMGG99Zg==
dXlmT0F1FAtMXA0VJEVRGjIgRFs8NSoDSDEy
ATwvXhgTMSdZTScxZkRLdRopWRgUOCpCTzAwaAMWdHVmFxE=
NjsrA3YwLDJ5VyUkI19LexUERVE=
GTshSl0ndCFCTHU/L0FUMDBoDWowJzJMSiE9KEoW
lTkjXks0MyNeGDE9NV1UNC1mXlEvMWYQGA==
nlwr5ETjezBRsKULS6ZJWAU8xvolPcBxwGQRaC5l0iNvycX7oSARkPgQQQNKjwHJgQugIBGYiVLwY
n6lLXhSq+P2Ae7qslh4HV0REDDQ314F/QQmVQhaYmuwAAAABJRU5ErkJggg==
PDArA1E7ICNfVjAgaElXIjoqQIkxeitMVjQzI18WNDArA1Q8ICM=
ADoqQls+dDNDVDw5L1ldMXQqSFknOi9DX3R0DEJRO3QpWEp1EClaVjk7J0kYEiYpWEh1ZkNKTQnL0FBdTApWlY5OyUgGCE8L14YOTElWU0nMWZMVjF0K0JKMHpoAxl0
nbz2PpFXK5obQPvYskh5WPqaG9rXnkDRR0q6cAjxZdP59oQNQA84ADshpC6WozBsB4DAP2/2KzrwR
HHMrDUs6JjRUGDM7NA1MPT01DU07MT5dXTYgl0kYNiYnXlB7dBZDXlQnIV1KMCQpX0x1PTINTDp0ek8GTRknSWcNFQRFUWl7JBMYOjpmeV05MSFfWTh4ZllQMHQiSE4wOCldXScnZkJedSAuREt1FTZdFnUNKVhKdTljSFw3NS5bQCI9KkEYPTEqXRg8OTZfVyMxZllQMHQnXUh7
nxtAB6Dkkzc+55W9DaF97Fkkv5BBgPHxbUjgkvZgS+F2Sbgzt/10o9cGJpAXA1cB03BOr94DlZZT
nAP7xsB0qOvNGAL+5klrOvBGghKD60AgQmEYAONbD9oSiM98ndOlrwNdAPL4fi77GUKyedoX+C60

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隐患。