南明离火
移动应用检测平台

ANDROID 静态分析报告

夜猫麻将 • v24.1.1

分析日期: 2025-10-15 14:42:21

应用概览

文件名称:	pkg.apk
文件大小:	70.7MB
应用名称:	夜猫麻将
软件包名:	com.yemao.yemao2024
主活动:	com.yemao.yemao2024.MainActivity
版本号:	24.1.1
最小SDK:	21
目标SDK:	30
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	37/100 (高风险)
跟踪器检测:	2/432
杀软检测:	AI评估：可能有安全隐患
MD5:	32062b3e4880633f956f722d66c3b4ea
SHA1:	e6ac81059b852e63242db1775cffdca89f61d62c
SHA256:	5dd07e60c125a9c389c55bc2f613e387b4e0ac433e4f81a9c385fc893d95a31

分析结果严重性分布

高危	中危	信息	安全	关注
4	12	2	0	0

四大组件导出状态统计

Activity组件：10个，其中export的有： 1个
Service组件：1个，其中export的有： 0个
Receiver组件：0个，其中export的有： 0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: False
v4 签名: False
主题: CN=yemao
签名算法: rsassa_pkcs1v15
有效期自: 2023-12-19 11:03:22+00:00
有效期至: 2048-12-12 11:03:22+00:00
发行人: CN=yemao
序列号: 0x1
哈希算法: sha256
证书MD5: 9bf4f399039e8114c657165bbb9f399f
证书SHA1: 404ad38d77137e262b544c73685e9616145d4570
证书SHA256: a7e7bf04819c8f682866877762caa6bf0b452cebb55edd7682fe452a0fbc3995
证书SHA512:
3c171dd95a851e58772264c060b4cfa2da27b53f5973c574e7f791e707ce1f53436a9e43a943ed4c456e39f528d55c008d543a54888721c77cfb0a8057f57fa5

公钥算法: rsa
密钥长度: 2048
指纹: 83470a00247aa9f4b56d8b9023d84310141c5633aa55e89a59d7e8be184426e5
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.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.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.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_COARSE_LOCATION	危险	获取粗略位置	通过WiFi或移动基站的方式获取用户粗略的经纬度信息，定位精度大概误差在30~1500米。恶意程序可以用它来确定您的大概位置。
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.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.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.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_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.CAPTURE_VIDEO_OUTPUT	普通	允许捕获视频输出	允许应用程序捕获视频输出。
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。

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: **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: **1** | 警告: **4** | 信息: **0** | 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	应用可被调试 [android:debuggable=true]	高危	应用开启了可调试标志，攻击者可轻易附加调试器进行逆向分析，导出堆栈信息或访问调试相关类，极大提升被攻击风险。
3	应用数据存在泄露风险 未设置[android:allowBackup]标志	警告	建议将 [android:allowBackup] 显式设置为 false。默认值为 true，允许通过 adb 工具备份应用数据，存在数据泄露风险。
4	Activity 设置了 TaskAffinity 属性 (com.yemao.yemao2024.wxapi.WXEntryActivity)	警告	设置 taskAffinity 后，其他应用可读取发送至该 Activity 的 Intent。为防止敏感信息泄露，建议保持默认 affinity（包名）。
5	Activity (com.yemao.yemao2024.wxapi.WXEntryActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。

代码安全漏洞检测

高危: **3** | 警告: **7** | 信息: **2** | 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	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	可能存在跨域漏洞。在 WebView 中启用从 URL 访问文件可能会泄漏文件系统中的敏感信息	警告	CWE: CWE-200: 信息泄露 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
4	SSL的不安全实现。信任所有证书或接受自签名证书是一个关键的安全漏洞。此应用程序易受MITM攻击	高危	CWE: CWE-295: 证书验证不恰当 OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	升级会员：解锁高级权限
5	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
6	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
7	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
8	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
9	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

10	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
11	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
12	不安全的Web视图实现。可能存在WebView任意代码执行漏洞	警告	CWE: CWE-749: 暴露危险方法或函数 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	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 CANAR(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/libclinkapi-lib.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: ['__FD_ISSET_chk', '__vsprintf_chk', '__memmove_chk', '__memcpy_chk', '__FD_SET_chk', '__vsnprintf_chk', '__strlen_chk']	True info 符号被剥离
2	arm64-v8a/libgmesdk.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: ['__FD_ISSET_chk', '__FD_SET_chk', '__strchr_chk', '__strrchr_chk', '__memcpy_chk', '__strlen_chk', '__vsnprintf_chk', '__vsprintf_chk', '__read_chk', '__strncat_chk', '__memset_chk', '__memmove_chk']	True info 符号被剥离

3	arm64-v8a/libmain.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	Partial RELRO warning 此共享对象启用了部分 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在部分 RELRO 中，GOT 部分的非 PLT 部分是只读的，但 .got.plt 仍然是可写的。使用选项 -z,relro,-z,now 启用完整的 RELRO。	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	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	True info 符号被剥离

应用行为分析

编号	行为	标签	文件
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
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
00191	获取短信收件箱中的消息	短信	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
00012	读取数据并放入缓冲流	文件	升级会员：解锁高级权限
00056	修改语音音量	控制	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
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
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
00153	通过 HTTP 发送二进制数据	http	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
00054	从文件安装其他APK	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
00076	获取当前WiFi信息并放入JSON中	信息收集 WiFi	升级会员：解锁高级权限
00016	获取设备的位置信息并将其放入 JSON 对象	位置 信息收集	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
00072	将 HTTP 输入流写入文件	命令 网络 文件	升级会员：解锁高级权限
00094	连接到 URL 并从中读取数据	命令 网络	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
00102	将手机扬声器设置为打开	命令	升级会员：解锁高级权限
00023	从当前应用程序启动另一个应用程序	反射 控制	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
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
00085	获取ISO国家代码并将其放入JSON中	信息收集 电话服务	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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	6/30	android.permission.RECORD_AUDIO android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.VIBRATE android.permission.CAMERA android.permission.READ_PHONE_STATE

本报告由南明离火移动安全分析平台生成

其它常用权限	6/46	android.permission.ACCESS_NETWORK_STATE android.permission.INTERNET android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_WIFI_STATE com.google.android.gms.permission.AD_ID

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
www.mostonetech.com	安全	是	**IP地址:** 140.249.88.239 **国家:** 中国 **地区:** 中国山东 **城市:** 济南 **纬度:** 36.651216 **经度:** 117.12 **查看:** 高德地图
ssgw.updrips.com	安全	否	**IP地址:** 154.215.122.55 **国家:** 香港 **地区:** 香港,香港 **城市:** 柴湾 **纬度:** 22.2678103 **经度:** 114.2360778 **查看:** Google 地图
api.open.mostonetech.com	安全	是	**IP地址:** 39.106.13.203 **国家:** 中国 **地区:** 中国北京 **城市:** 北京 **纬度:** 39.904211 **经度:** 116.407395 **查看:** 高德地图
sandcash.mixienet.com.cn	安全	是	**IP地址:** 203.107.86.172 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.274085 **经度:** 120.15507 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件
• http://www.infotiger.com • http://www.girafa.com • http://www.unwrap.jp • http://www.herz-power.de/technik.html • http://buytaert.net/crawler • http://help.yahoo.com/help/us/ysearch/slurp • http://www.majestic12.co.uk/bot.php	

- https://buy.itunes.apple.com/verifyReceipt
- http://www.sync2it.com/susie
- http://hilfe.acont.de/bot.html
- http://holmes.ge
- http://wiki.creativecommons.org/Metadata_Scraper
- http://browsers.garykeith.com
- http://www.kapere.com
- http://www.newzcrawler.com
- http://ponderer.org
- http://www.catchbot.com
- http://www.feedhub.com
- http://www.cipinet.com/bot.html
- http://www.answerbus.com
- http://www.scrubtheweb.com/abs/meta-check.html
- http://scripts.sil.org/OFL
- http://botw.org
- https://api.weixin.qq.com/sns/auth
- http://www.twingly.com
- http://www.displaydetails.com
- http://www.tecomi.com/bot.htm
- http://www.sqwidge.com/bot
- http://www.kosmix.com/html/crawler.html
- http://www.scifihifi.com/cocoalicious
- http://www.whizbang.com/crawler
- http://www.strategicboard.com
- http://www.bestwhois.net
- http://www.scoutjet.com
- http://www.coriolis.ch
- http://www.entireweb.com
- http://bookmarkbase.com
- http://reader.livedoor.com
- http://minutillo.com/steve/feedonfeeds
- http://www.google.com/feedfetcher.html
- http://MapoftheInternet.com
- http://gnomit.com
- http://doc.php.net
- http://Anonymouse.org
- http://knight.zook.in
- http://www.domaincrawler.com/domains/view
- http://www.simpy.com/?ref=bot
- http://www.google.com/bot.html
- http://www.ascendercorp.com
- http://www.ascendercorp.com/typedesigners.html
- http://subtextproject.com
- http://www.briansmodelcars.com/links
- http://www.yama.info.waseda.ac.jp
- http://8.136.102.190/arks/yemaoMJ.apkhttp
- http://www.kinja.com
- http://net-promoter.com
- http://search.thunderstone.com/texis/websearch/about.html
- http://www.google.com/adsbot.html
- http://www.dotnetdotcom.org
- http://www.mojeek.com/bot.html
- http://www.SiteSpider.com
- http://www.yoow.eu
- http://herbert.groot.jebbink.nl/?app=rssImages
- http://www.envolk.com/envolk
- http://www.europarchive.org
- http://www.businverse.com/bot.php
- http://www.googlebot.com/bot.html
- http://www.runnk.com
- http://www.diffbot.com
- http://www.html2jpg.com
- http://babelserver.org/rix

自研引擎-A

• http://misc.yahoo.com.cn/help.html • http://www.sync2it.com/bms/susie.php • http://otc.dyndns.org/webscan • https://api.weixin.qq.com/sns/oauth2/refresh_tokenhttps • http://www.dontbuylists.com • http://www.dead-links.com • http://www.rojo.com/corporate/help/agg • http://www.kyluka.com/crawl.html • http://www.tumblr.com • http://www.bloglines.com • http://www.skycomp.ca • http://www.youdao.com/help/webmaster/spider • http://www.pagebull.com • http://www.inktomi.com/slurp.html • http://www.goforit.com/about • http://www.activetourist.com • http://www.jadynave.com/robot • http://www.live.com • http://corp.infocious.com/tech_crawler.php • http://search.msn.com/msnbot.htm • http://www.searchengineworld.com/validator • http://www.lipperhey.com • http://tinyurl.com/64t5n • http://tailrank.com/robot • http://www.healthdash.com • http://herbert.groot.jebbink.nl/?app=WebImages • http://www.inetbot.com/bot.html • http://www.meta-spinner.de • http://liferea.sf.net • http://www.inclue.com • http://browsers.garykeith.com/sitemail/contact-me.asp • http://www.avantbrowser.com • http://www.ximian.com • http://www.opentagger.com/opentaggerbot.htm	
• https://sandcash.mixienet.com.cn/gateway/v2/order/linkcodepayment • https://sandcash.mixienet.com.cn/gateway/v2/order/mixedpay • https://sandcash.mixienet.com.cn/pay/sdk? • https://sandcash.mixienet.com.cn • https://sandcash.mixienet.com.cn/gateway/v2/order/quickpayment	com/pay/paytypelibrary/base/PayUtil.java
• javascript:window.nativebridge.receiveEvent	com/unity3d/services/ads/webplayer/WebPlayerView.java
• http://www.mostonetech.com/download	com/mostone/share/sdk/ui/MLifeWebActivity.java
• https://api.open.mostonetech.com	com/mostone/open/sdk/a/a/f.java
• https://sgw.updrips.com/oauth2/check/appinfo	org/xianliao/im/sdk/net/model/LoginInfoRequest.java
• http://120.24.210.161:52234/gateway/red/dispatcher	org/xianliao/im/sdk/net/model/GetBilldIRequest.java
• data:%u,sendavgr,vnd:%u	lib/arm64-v8a/libgmesdk.so

第三方 SDK 组件分析

SDK名称	开发者	描述信息

GME	Tencent	游戏多媒体引擎（Game Multimedia Engine）是一个专门针对游戏场景定制的实时游戏音视频 SDK，覆盖了休闲社交类、MOBA 类、MMORPG 等多种游戏类型，提供了包括多人实时语音、实时视频、语音消息、语音转文本等功能。功能完备，接入门槛低，一个 SDK 即可满足多样化的游戏音视频诉求。
Unity	Unity Technologies	Unity 游戏使用 Il2Cpp 后端时产生的游戏代码。
百度 LBS	Baidu	百度地图 Android SDK 是一套基于 Android 4.0 及以上版本设备的应用程序接口。 您可以使用该套 SDK 开发适用于 Android 系统移动设备的地图应用，通过调用地图 SDK 接口，您可以轻松访问百度地图服务和数据，构建功能丰富、交互性强的地图类应用程序。
阿里云游戏盾	Aliyun	游戏盾是通过封装登录器隐藏真实 IP，需要修改业务IP换成游戏盾 IP，然后在后台添加源IP 和转发业务端口，玩家通过下载封装好的登录器进入游戏。是采用多机房集群部署模式，节点切换无感知，加密所有连接，实现 CC 零误封，避免源 IP 泄漏，免疫 CC 与 DDOS 攻击。
Unity Ads	Unity Technologies	Unity Ads SDK 由领先的移动游戏引擎创建，无论您是在 Unity、xCode 还是 Android Studio 中进行开发，都能为您的游戏提供全面的变现服务框架。
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。

第三方追踪器检测

名称	类别	网址
Baidu Location		https://reports.exodus-privacy.eu.org/trackers/97
Unity3d Ads	Advertisement	https://reports.exodus-privacy.eu.org/trackers/121

敏感凭证泄露检测

可能的密钥
百度地图的=> "com.baidu.lbsapi.API_KEY" : "aiHH6GVg3sbU9GfA8Sxj5DtGGJvfmnN"

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。