南明离火
移动应用检测平台

ANDROID 静态分析报告

甘い言葉 • V4.8.2

分析日期: 2025-07-06 01:55:21

应用概览

文件名称:	fbce3c0fe076ba67.apk
文件大小:	30.23MB
应用名称:	甘い言葉
软件包名:	com.pfvvhd.lspifstr
主活动:	com.wind.im.MainActivity
版本号:	4.8.2
最小SDK:	21
目标SDK:	32
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	53/100 (中风险)
杀软检测:	AI评估：很危险，请谨慎安装
MD5:	6e5b89e90e6e923ac70412b819b6b8f4
SHA1:	3f60db0306e1c84fcac8e590ab00f3f9ada2f349
SHA256:	751fd737443dfa2f2c6269364d51ce5f25110a8fc80ec454bd14d8dd0c0b4000

分析结果严重性分布

高危	中危	信息	安全	关注
0	21	1	1	1

四大组件导出状态统计

Activity组件：113个，其中export的有： 4个
Service组件：15个，其中export的有： 5个
Receiver组件：17个，其中export的有： 5个
Provider组件：12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=rwiitbsa, ST=cPAMfWxP, L=mruAbjFg, O=vqStClwZ, OU=ScKjMKCg, CN=YYkfCAWo
签名算法: rsassa_pkcs1v15
有效期自: 2025-07-05 17:24:30+00:00
有效期至: 2035-07-03 17:24:30+00:00
发行人: C=rwiitbsa, ST=cPAMfWxP, L=mruAbjFg, O=vqStClwZ, OU=ScKjMKCg, CN=YYkfCAWo
序列号: 0xb57aaad036ed02e2
哈希算法: sha256
证书MD5: 6a513a1b5237fc55e7b34fa92bdbac7a
证书SHA1: 81eca665cdbf22d64ca7e1991924b238d460ede6
证书SHA256: c2bed6d932fdcaeb194aef0fa6e04ba72ead5b729d3dcd69f7a2a41ad742d36b
证书SHA512:
fd54155e46c86e8a680573bc7bcab0ff8060d7f2bda43574a61df00c58de7d9aff4e1d240dcc3636361d2d4c2f86a1cfa4f9fa53e5132[illegible]b8c87ab67384bc4

公钥算法: rsa
密钥长度: 2048
指纹: e1eb951c88bb6facc530d3c1280103633af3ea6680f07dbdd3d47113c7c61270
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.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.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.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.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.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.GET_TASKS	危险	检索当前运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。恶意应用程序可借此发现有关其他应用程序的保密信息。
android.permission.MODIFY_AUDIO_SETTINGS	危险	允许应用修改全局音频设置	允许应用程序修改全局音频设置，如音量。多用于消息语音功能。

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。
android.permission.BROADCAST_PACKAGE_ADDED	签名	接收新增APP的通知	它允许一个应用程序接收到其他应用程序添加新包（即新安装的可执行文件）的广播消息。
android.permission.BROADCAST_PACKAGE_CHANGED	签名	接收APP变化的通知	它允许一个应用程序接收到其他应用程序变化（安装、卸载、修改）的广播消息。
android.permission.BROADCAST_PACKAGE_INSTALL	签名	接收APP安装的通知	它允许一个应用程序接收到其他应用程序安装新包（即新安装的可执行文件）的广播消息。
android.permission.BROADCAST_PACKAGE_REPLACED	签名	接收APP替换的通知	它允许一个应用程序接收到其他应用程序被覆盖安装的广播消息。
android.permission.RESTART_PACKAGES	普通	重启进程	允许程序自己重启或重启其他程序
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.CHANGE_NETWORK_STATE	危险	改变网络连通性	允许应用程序改变网络连通性。
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.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）
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	普通	OPPO推送服务	OPPO推送服务正常工作所必需的，它允许应用接收来自OPPO推送系统的消息。
com.heytap.mcs.permission.RECIEVE_MCS_MESSAGE	普通	OPPO推送服务	OPPO推送服务正常工作所必需的，它允许应用接收来自OPPO推送系统的消息。
com.huawei.android.launcher.permission.CHANGE_BADGE	普通	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
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.SYSTEM_OVERLAY_WINDOW	未知	未知权限	来自 android 引用的未知权限。
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。
com.meir6bfivr.smknxy.permission.MIPUSH_RECEIVE	未知	未知权限	来自 android 引用的未知权限。
com.meizu.flyme.push.permission.RECEIVE	普通	魅族push服务权限	魅族push服务权限。
com.meir6bfivr.smknxy.push.permission.MESSAGE	未知	未知权限	来自 android 引用的未知权限。

com.meizu.c2dm.permission.RECEIVE	普通	魅族push服务权限	魅族push服务权限。
com.meir6bfivr.smknxy.permission.C2D_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
android.permission.ACCESS_LOCATION_EXTRA_COMMANDS	普通	访问定位额外命令	访问额外位置提供程序命令，恶意应用程序可能会使用它来干扰GPS或其他位置源的操作。
android.permission.READ_CONTACTS	危险	读取联系人信息	允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.READ_EXTERNAL_STORAGE	危险	读取SD卡内容	允许应用程序从SD卡读取信息。
com.meir6bfivr.smknxy.permission.PROCESS_PUSH_MSG	未知	未知权限	来自 android 引用的未知权限。
com.meir6bfivr.smknxy.permission.PUSH_PROVIDER	未知	未知权限	来自 android 引用的未知权限。
android.permission.REQUEST_INSTALL_PACKAGES	危险	允许安装应用程序	Android8.0 以上系统允许安装未知来源应用程序权限。
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	未知	未知权限	来自 android 引用的未知权限。
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序装载和卸载可移动存储器的文件系统。
android.permission.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
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.meizu.flyme.permission.PUSH	未知	未知权限	来自 android 引用的未知权限。
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。
com.asus.msa.SupplementaryDID.ACCESS	普通	获取厂商oaid相关权限	获取设备标识信息oaid，在华硕设备上需要用到的权限。
freemme.permission.msa	未知	未知权限	来自 android 引用的未知权限。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.wind.im.MainActivity	Schemes: ii9tov://,
com.imacapp.common.WindCommTransitActivity	Schemes: xqchat://,
com.tencent.tauth.AuthActivity	Schemes: tencent111111://,

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: **0** | 警告: **16** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用已配置网络安全策略 [android:networkSecurityConfig=@7F160003]	信息	网络安全配置允许应用通过声明式配置文件自定义网络安全策略，无需修改代码。可针对特定域名或应用范围进行灵活配置。
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	Activity 设置了 TaskAffinity 属性 (com.imacapp.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）。
4	Activity (com.imacapp.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。
5	Service (com.vivo.push.sdk.service.CommandClientService) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。
6	Broadcast Receiver (com.tencent.wind.im.push.receiver.VivoPushMessageReceiverImpl) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。

7	Service (com.xiaomi.mipush.sdk.PushMessageHandler) 受权限保护，但应检查权限保护级别。 Permission: com.xiaomi.xmsf.permission.MIPUSH_RECEIVE [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
8	Broadcast Receiver (com.xiaomi.push.service.receivers.NetworkStatusReceiver) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
9	Broadcast Receiver (com.wind.im.push.receiver.XiaomiPushMessageReceiver) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
10	Broadcast Receiver (com.wind.im.push.receiver.MeizuPushServerMsgReceiver) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
11	Activity (com.imacapp.common.WindCommTransitActivity) 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。
12	Activity (com.tencent.tauth.AuthActivity) 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。
13	Service (com.meizu.cloud.pushsdk.NotificationService) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。
14	Broadcast Receiver (com.huawei.hms.support.api.push.PushMsgReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.mei.6ufi.vv.smknxy.permission.PROCESS_PUSH_MSG protectionLevel: signatureOrSystem [android:exported=true]	信息	检测到 Broadcast Receiver 已导出并受权限保护，但权限保护级别为 signatureOrSystem。建议使用 signature 级别，避免依赖系统安装位置。

15	Broadcast Receiver (com.huawei.hms.support.api.push.PushReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.meir6bfivr.smknxy.permission.PROCESS_PUSH_MSG protectionLevel: signatureOrSystem [android:exported=true]	信息	检测到 Broadcast Receiver 已导出并受权限保护，但权限保护级别为 signatureOrSystem。建议使用 signature 级别，避免依赖系统安装位置。
16	Service (com.huawei.hms.support.api.push.service.HmsMsgService) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。
17	Content Provider (com.huawei.hms.support.api.push.PushProvider) 受权限保护，但应检查权限保护级别。 Permission: com.meir6bfivr.smknxy.permission.PUSH_PROVIDER protectionLevel: signatureOrSystem [android:exported=true]	信息	检测到 Content Provider 已导出并受权限保护，但权限保护级别为 signatureOrSystem，建议使用 signature 级别，避免依赖系统安装位置。
18	Activity (com.xiaomi.mipush.sdk.NotificationClickedActivity) 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。
19	Service (androidx.work.impl.background.systemjob.SystemJobService) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
20	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 受权限保护，但应检查权限保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。

代码安全漏洞检测

高危: **0** | 警告: **4** | 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	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
3	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
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	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

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/libapksadfsalkwes.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金丝雀值，以便在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', '__write_chk', '__vsnprintf_chk', '__strlen_chk']	True info 符号被剥离

2	arm64-v8a/librtmp-jni.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	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
3	arm64-v8a/libtxm.com.axss.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	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
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
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	12/30	android.permission.VIBRATE android.permission.RECORD_AUDIO android.permission.CAMERA android.permission.READ_PHONE_STATE android.permission.GET_TASKS android.permission.MODIFY_AUDIO_SETTINGS android.permission.WAKE_LOCK android.permission.RECEIVE_BOOT_COMPLETED android.permission.SYSTEM_ALERT_WINDOW android.permission.READ_CONTACTS android.permission.REQUEST_INSTALL_PACKAGES android.permission.WRITE_SETTINGS
其它常用权限	11/46	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_NETWORK_STATE android.permission.CHANGE_WIFI_STATE android.permission.FOREGROUND_SERVICE android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS android.permission.ACCESS_LOCATION_EXTRA_COMMANDS android.permission.READ_EXTERNAL_STORAGE android.permission.FLASHLIGHT

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

appgallery.cloud.huawei.com	安全	是	**IP地址:** 49.4.35.16 **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

URL 链接安全分析

URL信息	源码文件
• https://appgallery.cloud.huawei.com/app/ • https://play.google.com/store/apps/details?id= • https://appgallery.cloud.huawei.com • https://play.google.com/store	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息
OpenSSL	OpenSSL	OpenSSL 是用于传输层安全性协议（TLS）和安全套接字层（SSL）协议的功能强大的，商业级且功能齐全的工具包。
IJKPlayer	Bilibili	IJKPlayer 是一款基于 FFmpeg 的轻量级 Android/iOS 视频播放器，具有 API 易于集成、编译配置可裁剪、支持硬件加速解码、DanmakuFlameMaster 架构清晰、简单易用等优势。
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。
移动统计分析	Umeng	U-App 作为一款专业、免费的移动统计分析产品。在日常业务中帮您解决多种数据相关问题，如数据采集与管理、业务监测、用户行为分析、App 稳定性监控及实现多种运营方案等。助力互联网企业充分挖掘用户行为数据价值，找到产品更新迭代方向，实现精细化运营，全面提升业务增长效能。
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。

敏感凭证泄露检测

可能的密钥
vivo推送的=> "local_iv" : "MzMsMzQsMzUsMzYsMzcsMzgsMzksNDAsNDEsMzIsMzgsMzcsMzYsMzUsMzQsMzMsI0AzNCwzMiwzMywzNywzMywzNCwzMiwzMywzMywzMywzNCw0MSwzNSwzNSwzMiwzMiwjQDMzLDM0LDM1LDM2LDM3LDM4LDM5LDQwLDQxLDMyLDM4LDM3LDMzLDM1LDM0LDMzLCNAMzQsMzIsMzMsMzcsMzMsMzQsMzIsMzMsMzMsMzMsMzQsNDEsMzUsMzIsMzIsMzI"
凭证信息=> "APP_ID" : "com.meir6bfivr.smknxy"
openinstall统计的=> "com.openinstall.APP_KEY" : "ii9tov"
aFg5QGs7ZT1sO1tlbDhfJFNefU9RZGJETU56

aEF9f21OX15tOlt8aDhPOVNRfUdrZGVC
aDhHOmg7YV5LTjx4XF9iRWtuOENTXmFbX19xeU1BbWZoO34
aE59R2hePD5eXnF4aH5hYlNRfUdoOz1HW1FQ
aGVPe147PHtrOzxlW159amtuOEZoOGJEazhxZU1IYWteT1NDa0g
U15hQ2o7eWZfUUNlbE9fVmhRYXNrXnlmTU9i
aH5xU2hOYWZKT3F6X2VPfWhebkBtTnF7b0g
QGs7fT1LTn15aEF9YmtPT39qXnFebUg
a2RuTGhOZXtqOjx4bE9PYmg7fg
jufli9HdAS7UionNSfEQPscsQXTXApOwdaElQ0Fe588=
aDphR2tecV5aX315bDoweGg7bkxqZGU
a245RGhebkRsOHFlXFFHe2tnfTpoZDxeSlg
a244Q29kYV5NTltmTU4wZWhnfVtTXmVbS089
aGVPf2o7YT5NTl98bEhhemtucT0
aEF6QGo7YkddUW16TV9Pa2hOekBqfg
aDphT287eXtdXmV4aH5hZmhkfV9qTnleW19i
aE9Tc15eYWZKTzx8TVw4bGhebkxvZH1C
aGVQRFNOeWZdXmVmaH5beVNYOUBrO1xES09I
aE9TT2tOeWZKTm15aH5hbFNfU0NqTlxHbEJ
U159f207cWZdXjx5XF9lUGhkfU9TO2HXWFI
aDhHR1NeekZdUU98TU9lfGhnfUdrXmFbazt9fG9I
aGR9c287YVtTO3F6aDM4O2hfT19rWA
a25xZ1NOfkddUWVbDhfamg4T3NTTl9bZtQ
aGdhT1N3eVtoOkN5XFw4emg4U1tjZHk
U1hxW2g7XEdKTzx8aE9fcGhoYTpnOY9o
U19MTGpOX2ZNTl9GTWhlRFNYOEdvZDxmS0FA
aGVQRGg7cV5dXFlmDk4a2hfUEBTfg
aGd9VmNeWVtfUW1mbEFteFNYcT5tZHkx
aEF6RGtePGZfXjhlaDswOWtOYV9TO31mS04x
aGVPX2o7YkdfXmVlTUw4cGhIOFtsWA

aGR9W29kfkdsO2V7bH5bbGhfUExeO3FmbTtY
aEFhc15eYkRrOk98bDowbGg4TERTO2FbXG4
aGd9e2s7eWZfUUN8aExlcGtlT0dqTmV7U0g
aGVPe147PHtrOzxlW159amtuOEZoOGFbX144Zl9ucXxoWDg6WjtuR1xfYXhcWFw
aEhxe15OekRrO2FlaEhxOmg6YTpsXmF7W14x
aFhxT2heeXtoOGFlbDhfYmtucVZvO25HbTpi
a2dhT15OfWZdUUd6TV9PemhkfWdqXjxmXG4
aDthW2xeekRNQVNlTU59eGhYcXtvZF9C
aEg4R2tOPHtoO316XFhbfWhkfVNrZF9C
aFhxe1M7XEdNTm14bDhlf2hIcT5oSA
aDphOl5ObkRoOzhmTVw4fGhlUEBqZGE9bDox

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。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。