南明离火
移动应用检测平台

ANDROID 静态分析报告

Pesohere - v1.0.5

分析日期: 2025-08-29 15:38:18

应用概览

文件名称:	Pesohere_1.0.5.apk
文件大小:	4.64MB
应用名称:	Pesohere
软件包名:	com.pesohere.android
主活动:	com.cow.here.uicowhereanddto.acowherectivity.WeCowHerelcomeActivity
版本号:	1.0.5
最小SDK:	21
目标SDK:	33
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	63/100 (低风险)
跟踪器检测:	4/432
杀软检测:	经检测，该文件安全
MD5:	d40fe85e09a6fccb461661622dbc12a4
SHA1:	0f998a3bfb218abece94ab07727ccaf8d8309285
SHA256:	599a0910ba36e59a53ba472f1257174a1fe8c71407a87f981ef66f80001a0977

分析结果严重性分布

高危	中危	信息	安全	关注
0	13	1	3	0

四大组件导出状态统计

Activity组件：14个，其中export的有： 1个
Service组件：16个，其中export的有： 0个
Receiver组件：4个，其中export的有： 1个
Provider组件：2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=Google Inc., OU=Android, CN=Android
签名算法: rsassa_pkcs1v15
有效期自: 2023-01-11 11:17:44+00:00
有效期至: 2053-01-11 11:17:44+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0xea85ee4e338ef6e477ffe9b977c380d033c762a0
哈希算法: sha256
证书MD5: 4ffe4ecb3468d695d5fad3ddaf36eb78
证书SHA1: 00763c48cfb8169ebb1d67dfc0fa0a09671f6d91
证书SHA256: 84d9c7638a365c96f824c1585593dd98b5b4b5c1c8458bcf7db8ffc26a4d3e18
证书SHA512:
c5da593092520a4d58954cd03d68aac5dc61652e9fc4ec63e71a31dad82598a81fc2288415f89da[illegible]53974d524f867829f91a1572154fdb24ee40e1a356877

公钥算法: rsa
密钥长度: 4096
指纹: a27297dec08b4d34e8327794ed687e3153ec300732750231876f8cacb07aac4[illegible]
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.ACCESS_WIFI_STATE	普通	查看WiFi状态	允许应用程序查看有关Wi-Fi状态的信息。
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.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.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.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.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.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.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_PRI	未知	未知权限	来自 android 引用的未知权限。
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
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.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.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。
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。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.cow.here.uicowhereanddto.acowherectivity.MoreDataCowHereActivity	Schemes: pesohere://, Hosts: main.app, Paths: /page,

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: **3** | 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	Activity (com.cow.here.uicowhereanddto.acowherectivity.MoreDataCowHereActivity) 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。
3	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.google.android.c2dm.permission.SEND [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: **8** | 信息: **1** | 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	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	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
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
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	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
8	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
9	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
10	IP地址泄露	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MSTG-CODE-2	升级会员：解锁高级权限
11	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

应用行为分析

编号	行为	标签	文件
00077	读取敏感数据（短信、通话记录等）	信息收集 短信 通话记录 日历	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
00002	打开相机并拍照	相机	升级会员：解锁高级权限
00183	获取当前相机参数并更改设置	相机	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
00173	获取 AccessibilityNodeInfo 屏幕中的边界并执行操作	无障碍服务	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
00191	获取短信收件箱中的消息	短信	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
00013	读取文件并将其放入流中	文件	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
00067	查询IMSI号码	信息收集	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
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
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
00009	将游标中的数据放入JSON对象	文件	升级会员：解锁高级权限
00011	从 URI 查询数据（SMS、CALLLOGS）	短信 通话记录 信息收集	升级会员：解锁高级权限
00010	读取敏感数据（SMS、CALLLOG）并将其放入 JSON 对象中	短信 通话记录 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
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
00130	获取当前WIFI信息	WiFi 信息收集	升级会员：解锁高级权限

00083	查询IMEI号	信息收集 电话服务	升级会员：解锁高级权限
00062	查询WiFi信息和WiFi Mac地址	WiFi 信息收集	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
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
00189	获取短信内容	短信	升级会员：解锁高级权限
00188	获取短信地址	短信	升级会员：解锁高级权限
00200	从联系人列表中查询数据	信息收集 联系人	升级会员：解锁高级权限
00201	从通话记录中查询数据	信息收集 通话记录	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
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
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
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
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
00091	从广播中检索数据	信息收集	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
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
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
00195	设置录制文件的输出路径	录制音视频 文件	升级会员：解锁高级权限
00199	停止录音并释放录音资源	录制音视频	升级会员：解锁高级权限
00198	初始化录音机并开始录音	录制音视频	升级会员：解锁高级权限
00194	设置音源（MIC）和录制文件格式	录制音视频	升级会员：解锁高级权限

00197	设置音频编码器并初始化录音机	录制音视频	升级会员：解锁高级权限
00007	Use absolute path of directory for the output media file path	文件	升级会员：解锁高级权限
00196	设置录制文件格式和输出路径	录制音视频 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.RECEIVE_BOOT_COMPLETED android.permission.SYSTEM_ALERT_WINDOW android.permission.ACCESS_COARSE_LOCATION android.permission.CAMERA android.permission.READ_SMS android.permission.WAKE_LOCK
其它常用权限	7/46	android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.INTERNET android.permission.FOREGROUND_SERVICE com.google.android.gms.permission.AD_ID com.google.android.c2dm.permission.RECEIVE com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_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
sonelink.s	安全	否	No Geolocation information available.
sstats.s	安全	否	No Geolocation information available.
simpression.s	安全	否	No Geolocation information available.
sapp.s	安全	否	No Geolocation information available.
sviap.s	安全	否	No Geolocation information available.
scdn-settings.s	安全	否	No Geolocation information available.
sgcdsdk.s	安全	否	No Geolocation information available.
slaunches.s	安全	否	No Geolocation information available.
sinapps.s	安全	否	No Geolocation information available.

sars.s	安全	否	No Geolocation information available.
smonitorsdk.s	安全	否	No Geolocation information available.
sadrevenue.s	安全	否	No Geolocation information available.
sattr.s	安全	否	No Geolocation information available.
sdlsdk.s	安全	否	No Geolocation information available.
ssdk-services.s	安全	否	No Geolocation information available.
scdn-testsettings.s	安全	否	No Geolocation information available.
sconversions.s	安全	否	No Geolocation information available.
sregister.s	安全	否	No Geolocation information available.
svalidate.s	安全	否	No Geolocation information available.

URL 链接安全分析

URL信息	源码文件
• https://firebase.google.com/support/privacy/init-options	f/e/c/x/h.java
• https://%sapp.%s	com/appsflyer/internal/AFf1ySDK.java
• https://%scdn-settings.%s/android/v1/%s/settings • https://%smonitorsdk.%s/remote-debug?app_id= • https://%scdn-testsettings.%s/android/v1/%s/settings • https://%sonelink.%s/shortlink-sdk/v2 • https://%sgcdsdk.%s/install_data/v5.0/ • https://%sviap.%s/api/v1/android/validate_purchase?app_id= • https://%sars.%s/api/v2/android/validate_subscription?app_id=	com/appsflyer/internal/AFc1vSDK.java
• https://%simpression.%s	com/appsflyer/share/CrossPromotionHelper.java
• https://%s/%s/%s/	f/e/c/x/s/c.java
• https://%sdlsdk.%s/v1.0/android/	com/appsflyer/internal/AFb1mSDK.java
• https://%sviap.%s/api/v1/android/validate_purchase?app_id=	com/appsflyer/internal/AFd1xSDK.java
• https://%sadrevenue.%s/api/v2/generic/v6.9.4/android?app_id= • https://%sstats.%s/stats • https://%sinapps.%s/api/v • https://%sattr.%s/api/v • https://%sconversions.%s/api/v • https://%slaunches.%s/api/v	com/appsflyer/internal/AFb1zSDK.java
• 127.0.0.1	f/f/a/h/p.java

• https://%ssdk-services.%s/validate-android-signature • https://%svalidate.%s/api/v	com/appsflyer/internal/AFa1fSDK.java
• https://%sregister.%s/api/v	com/appsflyer/internal/AFd1dSDK.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/804122745191/namespaces/firebase:fetch?key=AIzaSyASp0fwIUzBnPPTPsYvDCdcy4X3vy3OaAU ） 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 云顶提供的最新信息。
AndPermission	yanzhenjie	Android 平台上的权限管理器。
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。
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。
Google Analytics	Google	提供各种 API，可帮助您收集、配置和报告用户与您的在线内容进行互动的数据。
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分析数据。

第三方追踪器检测

名称	类别	网址
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105

敏感凭证泄露检测

可能的密钥
友盟统计的=> "UMENG_CHANNEL" : "googlePlay"
"changecowherepwd_btn" : "Confirm"
"google_api_key" : "AIzaSyASp0fwIUzBnPPTPsYvDCdcy4XBvy3OaAU"
"google_app_id" : "1:804122745191:android:4c21dd798a5617a023f7c2"
"google_crash_reporting_api_key" : "AIzaSyASp0fwIUzBnPPTPsYvDCdcy4XBvy3OaAU"
GQkbGEUVA1MFCRMTSwEAHAxLJwQBBgYCW0sKBAYpHAAVAEcLDRMXHgQGQg==
FwkTKAoDOBYdDRE9Cwg1Gx8JEQ==
DA8WGQodFF0fDRcfDB4SGwQLWjEwLC02ITojJCY8KiY7LDw8JCYg
DA8WGQodFF0fDRcfDB4SGwQLWjEwLC02ITorKDwuOjg/MC48LD0r
BRUGGxZOX1wYHxJcFQgSHQMABhVdDAcIXRUIEh1EFQYZBQ4LAF0MAwcCA0ocFQEk
AxQeB0UXER0BBxFSBwhBEQoWAFAHAEgLHQtADwcHCVQECh8NRRMLCRMaAgdaBhoKH0skDAgWNRkKAQA=
VjlfKDc7IyBCKSI3KzlMMwUBBh8aC1MkAhU7BAAYDBseXA==
Dg4cHwAMBF0bAAAfAEMOEB8EHR4gGxEJkOXLBBMZJhsHOwoADgBBBUmDh0AXFNfREVCTA==
CwgcDzMdFQQtESwWTT9PGw9LFx8dGw0LBiYCFjoOFxlZ
DA8WGQodFF0fDRcfDB4SGwQLWiI2Liw6MSoiNTMoMSc=
E3F9E1E0CF99D0E56A055BA65E241B3399F7CFA524326B0CDD6EC1327EDDFDC1
CRUdKAo3HwQnDRcXFgJPFQ4RNx8EJwQXFzodBAEEOgECH0dB
M0lNSj5EXUoyQ0FbTVJAKQpIDjFeNTVOVkw2UV9SJFkqEkISDAlTQVNCFkE=
PhUTHwA3HwQnDRcXWwQEBUsIAQMHTwAEBAMAFIdBBgZF08EBAsKGBUgDhYbBQEMDQ==
DA8WGQodFF0fBhEKCxlPEwgRHR8dQTg5MS4=
DA8WGQodFF0fDRcfDB4SGwQLWjEwLC02ITouLjM5NjEvPyArJCYsIi8=
3BAF59A2E5331C30675FAB3EFF5FFF0D116142D3D4664F1C3CB804068B40614F
Dg4fGxcRAwAsBxI6AD8EOwYEExUnACocBgAeLx04BhUcFkcODB4APQAGA0lUSENfQQ==
CBMABBdcMQMGLR0RAC4OBSMABhUDGwEKkOXLQ15LRxARBw5IDAFFAxQeB0dYUBkcBwtbTA==
NwkTPxIbNA0bARELJgIWOg4XET8dCkAQEQADFRcZKgMFTg==
ACIdHC0RAhYLCRUGAB9PBAgmGwc7ChoAJAYoFVNKSwAVCxs=

GQkXSxMdFQRPARZSCwIVUhkAEgIWHABFHgQUDgcfWlQGGgofRU9F
CBMABBdcMwYcHAofIBUCFx8MGx4wAB8tkOXLABwPCREzHBggAAAAKBkRDhUAGRwBQBFbTA==
AxQeB0UXER0BBxFSBwhBEQoWAFAHAEgLHQtADwcHCVQECh8NRRMLCRMdAgFaEQMfRisdEQQHGwgEABkcASUEHAQKBAA=
AxQeB0UXER0BBxFSBwhBEQoWAFAHAEgLHQtADwcHCVQECh8NRRMLCRMdAgFaBBYXHEsxCQQREAQEBhQ+DgYEFQAf
PhUTHwA3HwQnDRcXMwQEBUsIAQMHTwAEBABNAFIFChpdHRoECVIzBAQFLBcbBQNPHgwXEj0AAA4LAA==
QhILGEoQFQUGCwABSh4YAR8AGV8QHx1KERUYUV0IFQEWAQoZSgEGDA0bBQIrEwYdNwMAABw=
BA8GDgsAXhcOHARTREMGFx80ARUBFjgEAAQABAYOF1xSAw4PADsBT0hTSg==
CgQGOBEGGR0IQDdcFhkTGwUCWgIWCAEWBgAfAh0cDRECFh0NAhsWGQQANBEdBB8KQQ==
BxQBH01cFAcARgYdEjIJFxkAKxQSGwk6CwQACFJUX1RSUU8JFlIxREg=
DA8WGQodFF0cDREGDAMGAUUkJCA/JiskJiwiLy0vICAxOiM7OiEgOTU7JSIn
NwkTJAsRMxwYIAAAAEUbGgomGwc7ChoABioDBCQKCQEVTg==
ACIdHC0RAhYLCRUGAB9PAhwBNx8EJw0XFzUaBTcfRFVeBwoQEQ==
LxQbBwERAlsbAAwBSU0CGgoLGhUfJgxMkOXLFRcFET0eBwoGEVoVCA8WAgsTQR0bDQsGTA==
CwgcDzMdFQQtESwWTT9PGw9LFxEdDA0JMQoaKRcZAF0=
BRUGGxZOX1wYHxJcFQgSHQMABhVdDAcIXRUIEh1EFQYfBwALCh1AQggcDRUcXxsKGgA=
DA8WGQodFF0fDRcfDB4SGwQLWjMyIi03Mw==
DA8WGQodFF0fDRcfDB4SGwQLWiA8PDw6PCo5KBQijUkCiAmNg==
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
CgQGOBEGGR0IQDdcFhkTGwUCWgABCgsKBQ0IExcCAREeBwYOCBEEGQgdBToAGQcDDUw=
GQkbGEUVA1MFCRMTSwEAHAxLJwQBBgYCkOXLCBwMTQcEEh0cLBwBCBleSwAaFDoBDAAKTA==
CBMABBdcMQMGLR0KAC4OBSMABhUDGwEKkOXLEhU0HBUdGkEHFzcIHRULQ0xYUBkcBwtbTA==
CwgcDzMdFQQtESwWTT9PGw9LEBUVBgYAMQoaKRcZAF0=
AxQeB0UXER0BBxFSBwhBEQoWAFAHAEgLHQtADwcHCVQECh8NRRkKGQ0bBUsyHBwOHA==
DA8WGQodFF0GBhEXCxlPEwgRHR8dQSwsMyk=
CBMABBdcMQMGLR0KAC4OBSMABhUDGwEKkOXLQVBJSVQVXRsHNgYXBA8VQ0xYUBkcBwtbTA==
ACIdHC0RAhYLCRUGAB9PAgMKGhUwAB8tFxcINxEuEVVRXRsNHQY=
BRUGGxZOX1wYHxJcFQgSHQMABhVdDAcIXQ==
AxQeB0UXER0BBxFSBwhBEQoWAFAHAEgLHQtADwcHCVQECh8NRRMLCRMdAgFaHBwMCREbCgNPPgQGFQQaAAYoEwsMBhcZ
DA8WGQodFF0fDRcfDB4SGwQLWiI2Liw6Nz05JCAlJDgvIDsnNzMiKA==

DA8WGQodFAtBHgwXEh0AFQ4XWgcaCw8ABks7CBccNRUXFh0=
CgQGOBEGGR0IQDdcFhkTGwUCWhMbDgYCFwYCFhoOFxEABAs3ERsRAQRb
CgQGKhUEHBoMCREbCgNJW0UCEQQwAAYRFwsZMxcYChgGFh1ATA==
NwkTPxIbNR0bARELJgIWOg4XESQEAEALFxIOCwUEJhsHFgZV
AxQeB0UXER0BBxFSBwhBEQoWAFAHAEgLHQtADwcHCVQECh8NRRMLCRMdAgEMXhAABhYGFwwIHB8JFQkcGhxLBQwJBhcfSzcfHRwcFxMMAxU+ChwbBQdBJAQLChgVIgoXFR0A
LxQbBwERAltGYkVSRU1BUktFVFBTT0hFkOXLa1JLRVRQU09IRVJFTUFSS0VaEgYGBAFaTA==
CgQGIgsHBBIBCwBaTEMGFx8kBAAAKQQcFxc4KDZDERwZAEZJRA==
QhEXGAoyBR1AHRVdAQgXGwgAPBUBCjgNGwsLDl0=
CwgcDzMdFQQtESwWTT9PGw9LABkHAw0mHRIlBAAOTA==
CA8RBAERJBw8HBcbCwpJGBhLAB8xFhwAMxcfAAtDTFhQMQ4bAERRQzQgJzonMTUqQQ==
CgIZXwc8Oz1bABcHEjgjFQk3AR0/OA==
AxQeB0UXER0BBxFSBwhBEQoWAFAHAEgLHQtADwcHCVQECh8NRRkKGQ0bBUsXHx8DDQYGDAIPAUUpHQMHDzxFHQNNAh0GSxcfBEEAAAAAQw8XHwYbBxsKGgAFCh8KXDkAAAIcCQERMQkEBBwfSwQfABs6AAMQCBIGTwkVHRELCUhBWw==
GQkbGEUVA1MFCRMTSwEAHAxLJwQBBgYCW0sZDj4EEhECMA4bAFpM
CgQGPhcdNhwdLgweAEUVGgIWND0cHQ0hkOXLKDZLTlRSXQkBURc1Hw4EAgERAlFDSAwGTA==
DA8WGQodFF0GBhEXCxlPEwgRHR8dQT4sNzI=
DA8WGQodFF0fDRcfDB4SGwQLWiI2Liw6Ii0iLzc0NiAxJyo=
DA8WGQodFF0CDQEbBEMAER8MGx5dJiUkNSAyIjM7MSEiNg==
QhILGEoQFQUGCwABSh4YAR8AGV8QHx1KERUYUV0IFQEWAQoZShEVGAgcDQorHRIXNwMAABw=
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
AxQeB0UXER0BBxFSBwhBEQoWAFAHAEgLHQtADwcHCVQECh8NRRkKGQ0bBUs1AgEOEVkmRQIHUgAKABwaAUYGHQkBBBEfDBseAEEpFwAEFBI5HzorMQEdCRwBLzssOR9LAB8nFhgAFiOfExM5Vw==
Cw4ABgQAXhoAGggTEUUlEx8AXCMKHBwAHUsOFAAZABoEJwYFAD8MAQ0bGE1dWVo=
KBMABBc3HwQnDRcXIRkOWggKAy8bGhoALQAfEx0ZOg0RHgZV
QhILGEoQFQUGCwABSh4YAR8AGV8QHx1KERUYUV0IFQEWAQoZShEVGAgcDQorHRoBNwMAABw=
GQkXSxMdFQRPDAoXFk0PHR9FHBEFCkgVExcIDwZHRQIZFhhIWFI=

免责声明及风险提示:

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。