南明离火
移动应用检测平台

ANDROID 静态分析报告

Logo

澳门金沙 • v3.7.1

分析日期: 2025-03-11 12:58:22

应用概览

文件名称:	amjx-master-ca-g-release-v3.7.1-20230425110836.apk
文件大小:	30.62MB
应用名称:	澳门金沙
软件包名:	com.tech.amjx.cash2
主活动:	com.tech.hope.lottery.LauncherActivity
版本号:	3.7.1
最小SDK:	22
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:	52/100 (中风险)
杀软检测:	AI评估：可能有安全隐患
MD5:	5dcf2f11c42b5a31587c95fb11f77551
SHA1:	80ae950190feb3a5529e287f57a[illegible]f184780ba9
SHA256:	d58e449dcf86a6bb673f21e[illegible]bfe6e97f8ee90

分析结果严重性

高危	中危	信息	安全	关注
2	1	2	2	1

四大组件信息

Activity组件：226个，其中export的有：3个
Service组件：3个，其中export的有：0个
Receiver组件：2个，其中export的有：0个
Provider组件：1个，其中export的有：0个

证书信息

二进制文件已签名
v1 签名: True

v2 签名: True
v3 签名: False
v4 签名: False
主题: C=china, ST=GuangDong, L=ShenZhen, OU=Hope, CN=LISA
签名算法: rsassa_pkcs1v15
有效期自: 2017-12-23 10:36:05+00:00
有效期至: 2042-12-17 10:36:05+00:00
发行人: C=china, ST=GuangDong, L=ShenZhen, OU=Hope, CN=LISA
序列号: 0x485f7530
哈希算法: sha256
证书MD5: c39cdd5feac53ec26f3051136838ddea
证书SHA1: 121ff5cc25cc4d82926918f36296d39f7be1e4cc
证书SHA256: e6d1472836067dcfbef8f1285f549591fe76fead5d362c279d1691edbaec8d76
证书SHA512:
6fcc8aacb091914d4bd213c8f18901a08bbef0c719d04e5b5ebca4594371d157b49967b9ec196b67ceb04e20ce3203c8a19a1d4f3b95343008a5d96ef74c897

公钥算法: rsa
密钥长度: 2048
指纹: 77b888d5ede0bf0ab9d2b0a28be160c709f3ffbb4d138b73119c0369c1bc91e1
找到 1 个唯一证书

☰ 应用权限

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.KILL_BACKGROUND_PROCESSES	普通	结束进程	允许应用程序结束其他应用程序的后台进程。
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	普通	在后台下载文件	这个权限是允许应用通过下载管理器下载文件，且不对用户进行任何提示。
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.REORDER_TASKS	危险	对正在运行的应用程序重新排序	允许应用程序将任务移至前端和后台。恶意应用程序可借此强行进入前端，而不受您的控制。
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.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.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.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.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.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。
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.SYSTEM_OVERLAY_WINDOW	未知	未知权限	来自 android 引用的未知权限。
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.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.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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。

网络通信安全

高危: **2** | 警告: **1** | 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。
2	*	警告	基本配置配置为信任系统证书。
3	*	高危	基本配置配置为信任用户安装的证书。

证书安全分析

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	应用程序使用代码签名证书进行签名

MANIFEST分析

高危: **0** | 警告: **4** | 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	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 (androidx.test.core.app.InstrumentationActivityInvoker$BootstrapActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
4	Activity (androidx.test.core.app.InstrumentationActivityInvoker$EmptyActivity) 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 (androidx.test.core.app.InstrumentationActivityInvoker$EmptyFloatingActivity) 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。

</> 安全漏洞检测

高危: **0** | 警告: **9** | 信息: **2** | 安全: **1** | 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
4	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
5	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
6	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
7	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

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	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
10	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
11	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
12	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

动态库分析

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	armeabi/liblbs.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	No RELRO high 此共享对象未启用 RELRO。整个 GOT（.got 和 .got.plt）都是可写的。如果没有此编译器标志，全局变量上的缓冲区溢出可能会覆盖 GOT 条目。使用选项 -z,relro,-z,now 启用完整 RELRO，仅使用 -z,relro 启用部分 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

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
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
00054	从文件安装其他APK	反射	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
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
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
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
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
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
00091	从广播中检索数据	信息收集	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

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
00036	从 res/raw 目录获取资源文件	反射	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
00191	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00034	查询当前数据网络类型	信息收集 网络	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
00134	获取当前WiFi IP地址	WiFi 信息收集	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
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
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
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
00033	查询IMEI号	信息收集	升级会员：解锁高级权限

敏感权限分析

类型	匹配	权限
恶意软件常用权限	6/30	android.permission.VIBRATE android.permission.SYSTEM_ALERT_WINDOW android.permission.REQUEST_INSTALL_PACKAGES android.permission.READ_PHONE_STATE android.permission.CAMERA android.permission.GET_TASKS
其它常用权限	8/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.REORDER_TASKS android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.ACCESS_WIFI_STATE android.permission.FOREGROUND_SERVICE 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。

域名检测

域名	状态	中国境内	位置信息
zhj.huabaoqiaoshifu.com	安全	是	**IP地址:** 58.220.73.244 **国家:** 中国 **地区:** 江苏 **城市:** 扬州 **纬度:** 32.397221 **经度:** 119.435600 **查看:** 高德地图
zhj.17zbmf.com	安全	否	No Geolocation information available.
whatismyip.akamai.com	安全	否	**IP地址:** 184.28.81.217 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图

URL链接分析

URL信息	源码文件
• javascript:isreadyforpulldown • javascript:isreadyforpullup	com/handmark/pulltorefresh/library/extras/PullToRefreshWebView2.java
• javascript:window.gettoken • javascript:window.is_token • javascript:window.serverurl	com/tech/hope/lottery/firstpage/luckymoney/LuckyMoneyActivity.java
• http://whatismyip.akamai.com	p4/a.java
• javascript:window.gettoken • javascript:window.is_token • javascript:window.serverurl	com/tech/hope/lottery/mine/login/LoginActivity.java
• https://%s/api/v2/android/%s/%s	va/a.java
• javascript:window.gettoken • javascript:window.is_token • javascript:window.serverurl	com/tech/hope/lottery/mine/login/FindPasswordStepActivity.java
• javascript:window.gettoken • javascript:window.is_token • javascript:window.serverurl	com/tech/hope/lottery/mine/login/RegisterActivity.java
• javascript:window.gettoken • javascript:window.is_token	com/tech/pay/ui/main/FindPasswordByMoblieActivity.java
• 127.0.0.1	com/netease/LDNetDiagnoService/a.java
• https://%s/api/v2/android/%s/%s	va/q.java
• https://zhj.huabaoqiaoshifu.com:8443/ • https://zhj.17zbmf.com:8443/	com/tech/hope/lottery/LauncherActivity.java

• https://github.com/tootallnate/java-websocket/wiki/lost-connection-detection	mc/a.java

第三方SDK

SDK名称	开发者	描述信息
Jetpack Camera	Google	CameraX 是 Jetpack 的新增库。利用该库，可以更轻松地向应用添加相机功能。该库提供了很多兼容性修复程序和解决方法，有助于在众多设备上打造一致的开发者体验。
腾讯浏览服务（TBS）	Tencent	腾讯浏览服务，依托 X5 内核强大的能力，致力于提供优化移动端浏览体验的整套解决方案。
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。
android-gif-drawable	koral--	android-gif-drawable 是在 Android 上显示动画 GIF 的绘制库。
Jetpack Test	Google	在 Android 中进行测试。
PictureSelector	LuckSiege	一款针对 Android 平台下的图片选择器，支持从相册获取图片、视频、音频 & 拍照，支持裁剪(单图 or 多图裁剪)、压缩、主题自定义配置等功能，支持动态获取权限&适配 Android 5.0+ 系统的开源图片选择框架。
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。
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 Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。
FileDownloader	LingoChamp	Android 文件下载引擎，稳定、高效、灵活、简单易用。

密钥凭证

可能的密钥
YW5kcm9pZC5oYXJkd2FyZS5jbHVidC9vdGg=
L3N5c3RlbS9ldGMvZXRjbHVnZWQtaW5wdXQtZGV2aWNlcy54bWw=
L3N5c3RlbS9iaW4vbmVtdVZNLXByb3A=
L3N5c3RlbS9iaW4vbWljcm92aXJ0LXByb3A=
L3N5c3RlbS9iaW4vZ2VueW1vdGlvbi12Ym94LXNm
L3N5c3RlbS9iaW4vZHJvaWQ0eGFwcm9w
YW5kcm9pZC5oYXJkd2FyZS5jYW1lcmEuZmxhc2g=
LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tDQpNSUlGVnpDQ0JEK2dBd0lCQWdJUUtjYm45SDRZRHlrcU1nNmZuYjVuMmpBTkJna3Foa2lHOXcwQkFRc0ZBRENCQ0pBRVVMTUFrR0ExVUVCaE1DUjBJeEd6QVpCZ05WQkFnVEVlZHlaV0YwWlhJZ1RXRnVZMmhsYzNSbGNqRVFNQTRHDQpBMVVFQnhNSFUyRnNabTl5WWkFYU1CZ0dBMVVFQ2hNUlEwOU1UFJQSUVOQklFeHBiV2wwWldReE5qQTBCZ05WDQpCQU1UTFVQ0UFRVOUVUeUJTVTBFZ1JHOXRZV2x1SUSZaaGJHbGtZWFJwYjI0Z1UyVmpkWEpsaUJEDQpRVEFFlRncweE56QXpNVFl3TURBd01EQmFGdzB4T0RBek1UWXlNelU1TlRsYU1GMHhJVEFmQmdOVkJBc1RHRVJ2DQpiV0ZwYmlCRGIyNTBjblZsUZaaGJHbGtZWFJsWkRFZE1Cc0dBMVVFQ3hNVVVHOXphWFJwZG1WVFUwd2dWMmxzDQpaR05oY21ReEdUQVhCZ05WQkFNTUVDb3ViM0JsYm1sdWMzUmhiR3d1YVc4d2dnRWlNQTBHQ1NxR1NJYjNEUUVCDQpBQUVBQTRJQkR3QXdnZ0VLQW9JQkFRQzNLMW9Ld1dQTENEdFM2bnZiQzE5ZEt0TmFJYU1PVU1sSkJQRzd4WVBTDQp1OWNiNmdWUXdPdCtZbEcwTkg1VVNUNDdpU21Va

3JPMmJ3WkozRWlGRFBQVmRuN0JHb25qUE9KeHQxdUlCUEN0DQphME1sK2hBKzF1Z2ZMY2wvcHl2OERYbWZEU2lTZFJFZ1VpdW9sU0d3ck53cUxPM
2c4d0pDMTUrTkdoU3lhOThvDQpwdmJRWlFqS0JJSWtDSStkdTBVRUJ1QVZTYWJicVhPRHdUV0hXSHZFMzFVSW4yaG1yd0pGM3d2MEpOTlBuUS8yDQ
p2blpNSG0zb0ZuOFpRYlYzeGNPUlRBL1ZBdnpxSlZ6anhWZitRQUVYTlJ5cFBsRCtocDc4cTJvVnBjbDhjUVFvDQoxeTVCL1d5Z3JrL1ZKMTFVNjY5SXhrMGl
rSmNFUmN6WWtZV1FwY0hGSlF4VEFnTUJBQUdqZ2dIZE1JSUIyVEFmDQpCZ05WSFNNRUdEQVdnQlNRcjJvNmxGb0wySkRxRWxaejMwTzBPaWphNXp
BZEJnTlZIUTRFRmdRVVgrcFFXYkJ5DQpGc2h6WHlBelo0MVZzd1ZHRjlzd0RnWURWUjBQQVFIL0JBUURBZ1dnTUF3R0ExVWRFd0VCL3dRQ01BQXdIUVlE
DQpWUjBsQkJZd0ZBWUlLd1lCQlFVSEF3RUdDQ3NHQVFVRkJ3TUNNRThHQTFVZElBUklNRVl3T2dZTEt3WUJCQUd5DQpNUUVDQWdjd0t6QXBCZ2dyQ
mdFRkJRY0NBUllkYUhSMGNITTZMeTl6WldOMWNtVXVZMjl0YjJSdkxtTnZiUzlEDQpVRk13Q0FZR1o0RU1BUUlCTUZRR0ExVWRId1JOTUVzd1NhQkhvR
VdHUTJoMGRIQTZMeTlqY213dVkyOXRiMlJ2Y2EpZMkV1WTI5dEwwTlBUVTlFVDFKVFFVUnZiV0ZwYmxaaGJHbGtZWFJwYjI1VFpXTjFjbVZUWlhKMlpYS
kRRUzVqDQpjbXd3Z1lVR0NDc0dBUVVGQndFQkJIa3dkekJQQmdnckJnRUZCUVdN3QW9aRGFlUjBjRG92TDJOeWRDNWpiMjF2DQpaRzlqWVM1amIyM
HZRMDlOVDBSUFVsTkJSRzl0WVdsdVZtRnNhV1JoZEdsdmJsTmxZM1Z5WlZObGNuWmxja05CDQpMbU55ZERBa0JnZ3JCZ0VGQlFjd0FZWVlhSFIwY0R
vdkwyOWpjM0F1WTI5dGIyUnZZMkV1WTI5dE1Dc0dBMVVkDQpFUVFrTUNLQ0VDb3ViM0JsYm1sdWMzUmhiR3d1YVcrQ0RtOXdaVzVwYm5OMFlXeH
NMbWx2TUEwR0NTcUdTSWIzDQpEUUVCQ3dVQUE0SUJBUUEyZ0lSQXMwQnVkZHdJV0g4MVo4Q1p3cm9pQ3NHNEVMSUJ6OHNuV[illegible]HxWndiRHFZaU
VnDQp1dnl1bTFVVzdOdS95aHlVZE9lZlMrM1phejExQUhWak54Q3RmRkluQmp6WjI1dXNHcEo3cjY3RHRMWFhEVDFLDQpLNFAzW[illegible]MmFweUhvM
HlUUVJrdjQ5YVBzNmlRcXU3eVQySnJiTmFDUnFwTjkrR29SOUJYanZ5VlRBNStsM1Z6DQp0ZFhoQWhnSjVlZTIzTEtzc3hsNDZGRllaY[illegible]N1pCUDFUR
lA1WXB2MmFGZHBraGxXbk1OK082K0hRaHBtDQpHSHpVcWtzcWhvRXBFN2w4QmxUTTFTVVhYMmJVbExvdEdqeW5wU2[illegible]TR3Nza3V4dkFp
SldaMTVOWkkzDQo4RUFYamttT1I1SVdJTlZJZGxqUnlFNDZHUHJvb1pTN1doQTlNCi0tLS0tRU5EIENFUlRJRklDQVRFLS0tLS[illegible]tLS0tQkVHSU4gQ0VS
VElGSUNBVEUtLS0tLQ0KTUlJR0NEQ0NBL0NnQXdJQkFnSVFLeTV1NnRsMU5td1VpbTdibzN5TUJ6QU5CZ2txaGtpRzl3[illegible]QURDQg0KaFRFTE1Ba
0dBMVVFQmhNQ1IwSXhHekFaQmdOVkJBZ1RFa2R5WldGMFpYSWdUV0Z1WTJobGMzUmxjakVRTUE0Rw0KQTFVR[illegible]MkZzWm05eVpERWFNQ
mdHQTFVRUNoTVJRMDlOVDBSUElFTkJJRXhwYldsMFpXUXhLekFwQmdOVg0KQkFNVElrTlBUVTlFVHlCU1Uw[illegible]EdsbWFXTmhkR2x2YmlCQm
RYUm9iM0pwZEhrd0hoY05NVFF3TWpFeQ0KTURBd01EQXdXaGNOTWprd01qRXhNak0xT1RVNVdqQ0JrRE[illegible]R0ExVUVCaE1DUjBJeEd6QVpCZ05
WQkFnVA0KRWtkeVpXRjBaWElnVFdGdVkyaGxjM1JsY2pFUU1BNEdBMVVFQnhNSFUyRnNabTl5WkRFY[illegible]VFQ2hNUg0KU[illegible]TlQwUlBJRU5C
SUV4cGJXbDBaV1F4TmpBMEJnTlZCQU1UTFVOUFRVOUVUeUJTVTBFZ1JHOXRZV2x1SUZaaA0KYkdsa[illegible]BiMjRnVTJWamRYSm[illegible]abGNpQk
RRVENDQVNJd0RRWUpLb1pJaHZjTkFRRUJCUUFEZ2dFUA0KQURDQ0FRb0NnZ0VCQUk3Q0Fobmhv[illegible]MWpTejlBZERUU2[illegible]3dGlCVVVXT
3FpZ3dBd0NmeDNNMjhTaA0KYlhjRG93K0crZU1HbkQ0TGdZcWJTUnV0QTc3NlM5dU1JTzNW[illegible]NE5yMHpDc0xk[illegible]VJSkdTMA0KU
WE0QWwvZStaOTZlMEhxblU0QTdmSzMxbGxWdmwwY0tmSVdMSXBlTnM0VGdsbGZRY0JoZ[illegible]MUWVUbmFHNg0K[illegible]rbkVLcG9vSVpGTm
l1SlBKYVh5ZWpYZEp0eEdwZENzV1RXTS8wNlJRMUEvV1pNZWJGRWg3bGdVcS81MQ0K[illegible]QWNoaFA2YTVp[illegible]b1ZTM0FPVEpCaHV5
eWRSUmVadzNpVkRwQTNoU3FYdHRuN0l6VzN1TGgwbg0KYzEzY1JUQ0FxdU95UVF1d[illegible]cm5sRzUxL3J1V0Z[illegible]XdFQUFhT0NBV1V3Z2dG
aE1COEdBMVVkSXdRWQ0KTUJhQUZMdXZmZ0k5K3FieFBJU09yZTQ0bU96Wk1q[illegible]TFVZERnUVdCQ[illegible]Gb0wySkRxRWxaeg0KMzBP
ME9pamE1ekFPQmdOVkhROEJBZjhFQkFNQ0FZWXdFZ1lEVlIwVEFRSC9CQWd3[illegible]SUJBREFkQmdOV[illegible]NVRUZqQVVCZ2dyQmdFRkJRY0RB
UVlJS3dZQkJRVUhBd0l3R3dZRFZSMGdCQlF3RWpBR0JnUlZIU0FBTUFnRw0KQm[illegible]BRUNBVEJNQmdOVkhS[illegible]VEJETUVHZ1A2QTloanRvZEhSd09
pOHZZM0pzTG1OdmJXOWtiMk5oTG1Odg0KYlM5RFQwMVBSRTlTVTBGR[illegible]pwWTJGMGFX[illegible]YwYUc5eWFYUjVMbU55YkRCeEJnZ3JCZ
0VGQlFjQg0KQVFSbE1HTXdPd1lJS3dZQkJRVUhNQUtHTDJoMGRIQTZMe[illegible]dVkyOXRiMlJ2WT[illegible]OXRMME5QVFU5RQ0KVDFKVFFVRmtaRlJ5
ZFhOMFEwRXVZM0owTUNRR0NDc0dBUVVGQnpBQmhoaG9kSFJ[illegible]dm[illegible]Qzl[illegible]JIxdg0K[illegible]WpiMjB3RFFZSktvWklodmNOQVFFTUJRQU
RnZ0lCQUU0cmRrK1NIR0kyaWJwM3dTY0Y5QnpXUkoycA0KbW[illegible]m1BVDdxU2VhaU5[illegible]WanBrMW1BNDJHSFd4M2QxUWNueXUzSGVJe
mcvM2tDREtvMmN1SDFaLw0KZStGRTZrS1Z4RjBOQVZCR0Zm[illegible]XQyTThSS2h[illegible]NFN6UjdKenNJdEc4a08zS2RZM1JZUEJwcw0KUD
AvSEVacklxUFcxTis4UVJjWnMyZUJlbFNhejY2Mmp1ZTUvR[illegible]ZlZRTdsM1lwaExH[illegible]GRvbHRNWQ0KZFZFVkFCdDBpTjNoeHpnRVF5anBGd
jNaQmRSZFJ5ZGcxdnM0TzJ4eW9wVDRRaHJmN1c4R[illegible]CZ0NxNU9qYw0KM[illegible]M5aVBjMGQxc2pocVBwZXBVZkphM3cvNVZqbzFKWH
Z4a3U4OCt2WmJyYWMyLzRFanhZb0lRNVF4Rw0K[illegible]KzNHSDVRRmxr[illegible]NjgrUFVxNE5DTmsrcUtCUjZjR0hkTlhKOTNTckxsUDd1M3I3b
CtMNA0KSHlhUHM5S2c0RGRiS0RzeDVRNVhMV[illegible]Qm1HcVc1cHJVN[illegible]Ly91K2Flbi9lN0tKRDJBRnNRWA0KajRyQllLRU1ybHREUjVGTD
Fab1hYL25VaDhlQ2pMZm40Zzh3R1RlR3J[illegible]ZHJ2MFBKRkdV[illegible]MGZ4UThBTkFlNGhaN1E3ZHJOSjNnalRjQnBVQzJKRDVMZW8z
MVJwZzBHY2cxOWhDQzBXdmdtamUzV1[illegible]bEJsR0dTVzRnTm[illegible]Zb2FrUndKaU5pcVorR2I3KzZrSERTVm5lRmVPL3FKYWtYemxCeWpBQT
ZxdVBiWXpTZg0KK0FaeEFlS0NJTlQrY[illegible]S1FTkQgQ0VSV[illegible]VEUtLS0tLQ0KLS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tDQpNSUlGZER
DQ0JGeWdBd0lCQWdJUUoyYnVWd[illegible]cjEzQ2kvSVRlSW[illegible]Foa2lHOXcwQkFRd0ZBREJ2DQpNUXN3Q1FZRFZRUUdFd0pUUlRFVU1CSUdB
MVVFQ2hNTFFXUmtWSEoxYzNRZ1[illegible]akFrQmdOVkJBc1[illegible]paRlJ5ZFhOMElFVjRkR1Z5Ym1Gc0lGUlVVQ0JPWlhSM2IzSnJNU0l3SUFZRFZR
UURFeGxCWkdSVWNuVnpkQ[illegible]JsY201aGJDQkRR[illegible]I5ME1CNFhEVEF3TURVek1ERXdORGd6T0ZvWERUSXdNRFV6TURFd05EZ3pPRm93D
QpnWVV4Q3pBSkJnTlZCQVl[illegible]Q01Sc3dHUVlEVl[illegible]khjbVZoZEdWeUlFMWhibU5vWlhOMFpYSXhFREFPDQpCZ05WQkFjVEIxTmhiR1p2Y21R
eEdqQVlCZ05WQkFvV[illegible]FVHlCRFFTQk1h[illegible]01Tc3dLUVlEDQpWUVFERXlKRFQwMVBSRThnVWxOQklFTmxjblJwWm1sallYUnBiMjRn
UVhWMGFHOXlhWF[illegible]QU5CZ2txDQpo[illegible]QkFRRUZBQU9DQWc4QU1JSUNDZ0tDQWdFQWtlaFVrdElLVnJHc0RTVGR4YzlFWjNTWkt6Z
WpmU053DQpB[illegible]NqMHQvRU[illegible]Qnl0MkYveVVzUEY2Yzk0N0FFWWU3L0VaZkg5SVkrQ3ZvK1hQbVQ1alI2DQoyUlJyNTV5emhhQ
0NlbmF2Y1pE[illegible]EtZdlQzK1pmN1g4WjBOeXZRd0Exb25yDQpheXpUN1krWUhCU3JmdVhqYnZ6WXFPU1NKTnBEY
TJLNFZmM3[illegible]VFZ3dSZFd0DQo0UTA4UldEOE1wWlJKN3hudzhvdXRtdnFSc2ZISUtDeEgyWGVTQWk2cEU2cDhvTkd
ONFRyN[illegible]bUbklxDQptMX[illegible]lN1NybU5udTRGR0R3d2xHVG0wK21mcVZGOXA4TTFkQlBJMVI3UXUyWEs4c1l4cmZWOGcvDQp2T2
xkeEp1d[illegible]MW9rdExxcFZqM1B[illegible]ZpKzhLai85TGl0NlRmN3VyajBDenI1NkVOQ0hvblloTXNUDQo4ZG03NFlsZ3VJd29WcXdVSFp3SzUzSHJ6dz
dkUGFtV2[illegible]nZXhXTy9iVG91SmJ0N0lFDQpJbEtWZ0pOcDZJNU1aZkdSQXkxd2RBTHFpMmNWS1dsU0FydlgzMUJxVlVhL29LT
W9ZWDl3ME1PaXFpd2hxa2[illegible]dHUlhhL2doZ250Tld1dE10UTVtdjBUSVp4TU9tbTN4YUc0TmovUU4zNzBFS0lmNk16T2k1Y0hrRVJnV1BPDQpHS
EZySyt5bWlyY3hYRHB[illegible]ldJQnF2OG1xWXFuSzhWMHJTUzUyN0VQeXdURUhsN1IwOVhpaWRuTXkvDQpzMUhhcDBmbGhGTUNBd0VBQWF
PQjlEQ0I4VEFmQmdO[illegible]HREFXZ0JTdHZaaDZOTFFtOS9yRUpsVHZBNzNnDQpKTXRVR2pBZEJnTlZIUTRFRmdRVXU2OStBajM2cHZFOGhJNnQ3a
mlZN05reU10U[illegible]UEFRSC9CQVFEQpBZ0dHTUE4R0ExVWRFd0VCL3dRRk1BTUJBZjh3RVFZRFZSMGdCQW93Q0RBR0JnUlZIU0FBTUVRR0ExV
WRId1E5DQp[illegible]EBM29EV0dNMmgwZEhBNkx5OWpjbXd1ZFhObGNuUnlkWE4wTG1OdmJTOUJaR1JVY25WemRFVjRkR1Z5DQpibUZzUTBGU2Iy
OTBMbU55YkR[illegible]3JCZ0VGQlFjQkFRUXBNQ2N3SlFZSUt3WUJCUVVITUFHR0dXaDBkSEE2DQpMeTl2WTNOd0xuVnpaWEowY25WemRDNWpiMjB
3RFFZSkt[illegible]dmNOQVFFTUJRQURnZ0VCQUdTL2cvRmZtb1hRDQp6YmloS1ZjTjZGcjMwZWsrOG5ZRWJ2RlNjTHNlUFA5TkRYUnF6SUdDSmRQRG9Dc
GRUUF[illegible]dHhGUUpkY2ZqDQpKdzVkaEhrM1FCTjM5YlNzSE5BN3F4Y1MxdTgwR0g0cjZYblRxMWRGREs4byt0RGI1VkNWaUx2ZmhWZHBmWkxZD
QpVc3B6Z[illegible]YzgrYTRibVlSQmJNZWxDMS9rWldTV2ZGTXpxT1JjVXg4Und3N0N4bjJvYkZzaGo1Y3FzUXVnc3Y1DQpCNWE2U0UyUThwVElxWE9pNndaN
0k1M2Vvdk5OVlo5NllVV1lHR2pIWGtCckkvVjVldStNdFd1THQyOUc5SHZ4DQpQVXNFMkpPQVdWcmdRU1Fkc284VllGaEgyKzl1UnYwVjlkbGZtclBiMkxxq
a1FMUE5sem11aGJzZGpyemNoNXZSDQpwdS94TzI4UU9HOD0NCi0tLS0tRU5EIENFUlRJRklDQVRFLS0tLS0=

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。