南明离火
移动应用检测平台

ANDROID 静态分析报告

51禁域 • v1.2.3

分析日期: 2024-05-26 22:14:46

应用概览

文件名称:	51禁域.apk
文件大小:	17.89MB
应用名称:	51禁域
软件包名:	com.sgsewreyvb.ertrthjtyj
主活动:	com.sgsewreyvb.ertrthjtyj.SplashActivity
版本号:	1.2.3
最小SDK:	21
目标SDK:	32
加固信息:	未加壳
应用程序安全分数:	44/100 (中风险)
杀软检测:	10 个杀毒软件报毒
MD5:	21d0776d976f31c7b9fd406d1d37af29
SHA1:	d3318d57b6212bc6db07dd7e0d943267106d0db5
SHA256:	2b4071f47233e50c1573982ef0144f3f1b3ba399a2fdf21a8ab8e39f7a1cd0548

分析结果严重性分布

高危	中危	信息	安全	关注
6	9	1	3	6

四大组件导出状态统计

Activity组件：12个，其中export的有：0个
Service组件：3个，其中export的有：1个
Receiver组件：0个，其中export的有：0个
Provider组件：4个，其中export的有：0个

应用签名证书信息

二进制文件已签名
v1 签名: True
v2 签名: True
v3 签名: False

本报告由南明离火移动安全分析平台生成

v4 签名: False
主题: CN=sf, OU=sf, O=sf, L=sf, ST=sf
签名算法: rsassa_pkcs1v15
有效期自: 2023-06-06 09:41:57+00:00
有效期至: 2048-05-30 09:41:57+00:00
发行人: CN=sf, OU=sf, O=sf, L=sf, ST=sf
序列号: 0x1
哈希算法: sha256
证书MD5: f02106816835524d47e3ffe0db9b4499
证书SHA1: 02de49ec59e0db20f2b30d692ee5ef7721c45eb1
证书SHA256: eca5bdef6a6919fd67bc823ef7863085ec9f20bf61f437e655e92d2961bd3043
证书SHA512:
c681216661b0acdac56aea48818a511ec47242661ebe1dba6b5fd2764367c63a8b2b4ced056ce4c7601bcfec3bfb97f976e819a5f8805d17fd881187195a243e5

公钥算法: rsa
密钥长度: 2048
指纹: d3d2bbb1139b12ceb0028531e818dc6b3fd579688daa7375ea0dd16d06be3432
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.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.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.ACCESS_DOWNLOAD_MANAGER	签名(系统)	访问下载管理器	这个权限是允许应用访问下载管理器，以便管理大型下载操作
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.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.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.REQUEST_DELETE_PACKAGES	普通	请求删除应用	允许应用程序请求删除包。
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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
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。

网络通信安全风险分析

高危: **1** | 警告: **0** | 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。

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	应用程序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: **2** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用程序可以安装在有漏洞的已更新 Android 版本上 Android 5.0-5.0.2, [minSdk=21]	信息	该应用程序可以安装在具有多个未修复漏洞的旧版本 Android 上。这些设备不会从 Google 接收合理的安全更新。支持 Android 版本 => 10，API 29 以接收合理的安全更新。
2	应用程序具有网络安全配置 [android:networkSecurityConfig=@xml/jz_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。
3	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。
4	Service (com.sgsewreyvb.ertrthjtyj.CompressAndUpdateService) 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。

代码安全漏洞检测

高危: **5** | 警告: **6** | 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
2	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
3	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

4	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
5	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
6	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
7	应用程序在加密算法中使用ECB模式。ECB模式是已知的弱模式，因为它对相同的明文块[UNK]产生相同的密文	高危	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	升级会员：解锁高级权限
8	该文件是World Readable。任何应用程序都可以读取文件	高危	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
9	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
10	WebView域控制不严格漏洞	高危	CWE: CWE-73: 外部控制文件名或路径	升级会员：解锁高级权限
11	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
12	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

本报告由南明离火移动安全分析平台生成

13	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
14	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 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/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。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会对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: ['__strrchr_chk', '__vsnprintf_chk', '__memcpy_chk', '__strchr_chk', '__vsprintf_chk', '__strncpy_chk']	False warning 符号可用

敏感权限滥用分析

类型	匹配	权限

本报告由南明离火移动安全分析平台生成

恶意软件常用权限	6/30	android.permission.REQUEST_INSTALL_PACKAGES android.permission.RECORD_AUDIO android.permission.CAMERA android.permission.MODIFY_AUDIO_SETTINGS android.permission.VIBRATE android.permission.GET_TASKS
其它常用权限	5/46	android.permission.INTERNET android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE 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
exoplayer.dev	安全	否	**IP地址:** 185.199.108.153 **国家:** 美利坚合众国 **地区:** 宾夕法尼亚 **城市:** 加利福尼亚 **纬度:** 40.065647 **经度:** -79.891724 **查看:** Google 地图
www.ikb66.com	安全	是	**IP地址:** 61.160.148.90 **国家:** 中国 **地区:** 江苏 **城市:** 台州 **纬度:** 32.492168 **经度:** 119.910767 **查看:** 高德地图
jojolive-test.s3.ap-southeast-1.amazonaws.com	安全	是	**IP地址:** 61.160.148.90 **国家:** 中国 **地区:** 江苏 **城市:** 台州 **纬度:** 32.492168 **经度:** 119.910767 **查看:** 高德地图
52kbhl.com	安全	是	**IP地址:** 61.160.148.90 **国家:** 中国 **地区:** 江苏 **城市:** 台州 **纬度:** 32.492168 **经度:** 119.910767 **查看:** 高德地图
d379lwrm6sjtq.cloudfront.net	安全	是	**IP地址:** 61.160.148.90 **国家:** 中国 **地区:** 江苏 **城市:** 台州 **纬度:** 32.492168 **经度:** 119.910767 **查看:** 高德地图

s3.ap-east-1.amazonaws.com	安全	是	**IP地址:** 52.95.160.69 **国家:** 中国 **地区:** 香港 **城市:** 香港 **纬度:** 22.285521 **经度:** 114.157692 **查看:** 高德地图
aomedia.org	安全	是	**IP地址:** 61.160.148.90 **国家:** 中国 **地区:** 江苏 **城市:** 台州 **纬度:** 32.492168 **经度:** 119.910767 **查看:** 高德地图
ai1mo8.com	安全	否	No Geolocation information available.

URL 链接安全分析

URL信息	源码文件
• javascript:document.body.style.margin=	app/a/module_comic/ArticleActivity$startObserve$1$2.java
• https://52kbhl.com/	com/caoliu/module_im/ImRepository.java
• https://s3.ap-east-1.amazonaws.com	com/caoliu/module_im/adapter/ChatNewAdapter.java
• https://s3.ap-east-1.amazonaws.com	com/caoliu/module_im/adapter/ChatRoomAdapter.java
• https://52kbhl.com/front/	com/caoliu/module_im/Cif.java
• https://52kbhl.com/	com/caoliu/lib_common/repository/FileRepository.java

• http://8.136.101.204/v/饺子挺住.jpg • http://8.136.101.204/v/饺子还年轻.jpg • http://8.136.101.204/v/饺子偷人.mp4 • http://8.136.101.204/v/饺子真会.jpg • http://8.136.101.204/v/饺子星光.mp4 • http://8.136.101.204/v/饺子有活.jpg • http://8.136.101.204/v/饺子高兴.jpg • http://8.136.101.204/v/饺子你听.jpg • http://8.136.101.204/v/饺子高冷.mp4 • http://8.136.101.204/v/饺子汪汪.jpg • http://8.136.101.204/v/饺子你听.mp4 • http://8.136.101.204/v/饺子起飞.mp4 • http://8.136.101.204/v/饺子真萌.mp4 • http://8.136.101.204/v/饺子真萌.jpg • http://8.136.101.204/v/饺子真会.mp4 • http://8.136.101.204/v/饺子偷人.jpg • http://8.136.101.204/v/饺子有活.mp4 • http://8.136.101.204/v/饺子好妈妈.mp4 • http://8.136.101.204/v/饺子想吹.mp4 • http://8.136.101.204/v/饺子还小.mp4 • http://8.136.101.204/v/饺子可以.mp4 • http://8.136.101.204/v/饺子堵住了.jpg • http://8.136.101.204/v/饺子跳.mp4 • http://8.136.101.204/v/饺子可以了.mp4 • http://8.136.101.204/v/饺子起飞.jpg • http://8.136.101.204/v/饺子打电话.mp4 • http://8.136.101.204/v/饺子都懂.jpg • http://8.136.101.204/v/饺子还小.jpg • http://8.136.101.204/v/饺子不服.mp4 • http://8.136.101.204/v/饺子不服.jpg • http://8.136.101.204/v/饺子高兴.mp4 • http://8.136.101.204/v/饺子想吹.jpg • http://8.136.101.204/v/饺子主动.jpg • http://8.136.101.204/v/饺子运动.mp4 • http://8.136.101.204/v/饺子三位.jpg • http://8.136.101.204/v/饺子受不了.jpg • http://8.136.101.204/v/饺子堵住了.mp4 • http://8.136.101.204/v/饺子可以.jpg • http://8.136.101.204/v/饺子高冷.jpg • http://8.136.101.204/v/饺子受不了.mp4 • http://8.136.101.204/v/饺子还年轻.mp4 • http://8.136.101.204/v/饺子运动.jpg • http://8.136.101.204/v/饺子星光.jpg • http://8.136.101.204/v/饺子主动.mp4 • http://8.136.101.204/v/饺子挺住.mp4 • http://8.136.101.204/v/饺子都懂.mp4 • http://8.136.101.204/v/饺子可以了.jpg • http://8.136.101.204/v/饺子汪汪.mp4 • http://8.136.101.204/v/饺子跳.jpg • http://8.136.101.204/v/饺子打电话.jpg • http://8.136.101.204/v/饺子好妈妈.jpg • http://8.136.101.204/v/饺子三位.mp4 • http://8.136.101.204/v/饺子想吹.mp4	z/Cif.java
• javascript:document.body.style.margin=0	com/caoliu/module_main/square/detail/DynamicDetailActivity$setNormalUi$3.java
• https://image.baidu.com/it/u=2900823425,1993445529&fm=253&app=138&size=w931&n=0&f=jpeg&fmt=auto?sec=1670605200&t=ab67a73ef1605f3131b7c5c43ada799	com/caoliu/lib_common/dialog/ShareDialog.java
• https://d379lwrmf6sjrq.cloudfront.net/sf16/domain/5aylwdc3	com/caoliu/lib_common/base/BaseViewModel$tryCatch$2.java
• https://d379lwrmf6sjrq.cloudfront.net/sf16/domain/app.version	com/sgsewreyvb/ertrthjtyj/MainViewModel$getVersion$1.java
• https://d379lwrmf6sjrq.cloudfront.net/sf16/domain/app.version	com/caoliu/module_mine/mine/MineViewModel$postVersionCheck$1.java
• file:///assets/	com/opensource/svgaplayer/Cbreak.java

• https://jojolive-test.s3.ap-southeast-1.amazonaws.com/vip/2022-02-25/14/4c053e1ca87d459ea9d19b73d7297a0f.mp4	com/caoliu/lib_jzvideo/tiktok/TikTokRecyclerViewAdapter.java
• https://d379lwrmf6sjrq.cloudfront.net/sf16/domain/app.version • http://8.136.101.204/v/饺子还年轻.jpg • https://www.ikb66.com • http://8.136.101.204/v/饺子偷人.mp4 • http://8.136.101.204/v/饺子挺住.jpg • http://8.136.101.204/v/饺子真会.jpg • http://8.136.101.204/v/饺子星光.mp4 • http://8.136.101.204/v/饺子有活.jpg • http://8.136.101.204/v/饺子高兴.jpg • http://8.136.101.204/v/饺子你听.jpg • 127.0.0.1 • http://8.136.101.204/v/饺子高冷.mp4 • https://github.com/vinc3m1 • http://8.136.101.204/v/饺子汪汪.jpg • http://8.136.101.204/v/饺子真萌.jpg • http://8.136.101.204/v/饺子真萌.mp4 • http://8.136.101.204/v/饺子起飞.mp4 • http://8.136.101.204/v/饺子你听.mp4 • http://8.136.101.204/v/饺子真会.mp4 • http://8.136.101.204/v/饺子偷人.jpg • http://8.136.101.204/v/饺子有活.mp4 • https://aomedia.org/emsg/id3 • http://8.136.101.204/v/饺子好妈妈.mp4 • https://s3.ap-east-1.amazonaws.com • http://8.136.101.204/v/饺子想吹.mp4 • http://8.136.101.204/v/饺子还小.mp4 • https://d379lwrmf6sjrq.cloudfront.net/sf16/domain/5aylwdc3 • http://8.136.101.204/v/饺子可以.mp4 • http://8.136.101.204/v/饺子堵住了.jpg • http://8.136.101.204/v/饺子跳.mp4 • http://8.136.101.204/v/饺子可以了.mp4 • javascript:document.body.style.margin= • http://8.136.101.204/v/饺子起飞.jpg • http://8.136.101.204/v/饺子都懂.jpg • http://8.136.101.204/v/饺子打电话.mp4 • http://8.136.101.204/v/饺子还小.jpg • https://github.com/vinc3m1/roundedimageview • https://52kbhl.com/front/ • http://8.136.101.204/v/饺子堵住了.mp4 • https://ai1mo8.com/front/ • http://8.136.101.204/v/饺子不服.jpg • http://8.136.101.204/v/饺子不服.mp4 • http://8.136.101.204/v/饺子高兴.mp4 • http://8.136.101.204/v/饺子想吹.jpg • http://8.136.101.204/v/饺子主动.jpg • http://8.136.101.204/v/饺子想听.mp4 • http://8.136.101.204/v/饺子可以.jpg • http://8.136.101.204/v/饺子受不了.jpg • http://8.136.101.204/v/饺子三位.jpg • https://52kbhl.com/ • http://8.136.101.204/v/饺子运动.mp4 • http://8.136.101.204/v/饺子高冷.jpg • http://8.136.101.204/v/饺子受不了.mp4 • http://8.136.101.204/v/饺子还年轻.mp4 • http://8.136.101.204/v/饺子运动.jpg • https://developer.apple.com/streaming/emsg-id3 • http://8.136.101.204/v/饺子星光.jpg • http://8.136.101.204/v/饺子主动.mp4 • https://exoplayer.dev/issues/player-accessed-on-wrong-thread • file:///assets/ • http://8.136.101.204/v/饺子挺住.mp4	自研引擎-S

- http://8.136.101.204/v/饺子都懂.mp4
- https://img0.baidu.com/it/u=2900833435,993445529&fm=253&app=138&size=w931&n=0&f=jpeg&fmt=auto?sec=1670605200&t=ab677a736f1605f3131b7c5c43ada799
- http://8.136.101.204/v/饺子汪汪.mp4
- www.baidu.com
- http://8.136.101.204/v/饺子跳.jpg
- http://8.136.101.204/v/饺子好妈妈.jpg
- http://8.136.101.204/v/饺子打电话.jpg
- https://github.com/vinc3m1/roundedimageview.git
- 223.5.5.5
- http://8.136.101.204/v/饺子可以了.jpg
- https://exoplayer.dev/issues/cleartext-not-permitted
- http://8.136.101.204/v/饺子三位.mp4
- https://jojolive-test.s3.ap-southeast-1.amazonaws.com/vip/2022-02-25/14/4c053e1ca87d459ea9d19b73d7297a0f.mp4
- http://8.136.101.204/v/饺子想听.jpg

第三方 SDK 组件分析

SDK名称	开发者	描述信息
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。
RenderScript	Android	RenderScript 是用于在 Android 上以高性能运行计算密集型任务的框架。RenderScript 主要用于数据并行计算，不过串行工作负载也可以从中受益。RenderScript 运行时可在设备上提供的多个处理器（如多核 CPU 和 GPU）间并行调度工作。这样您就能够专注于表达算法而不是调度工作。RenderScript 对于执行图像处理、计算摄影或计算机视觉的应用来说尤其有用。
AndroidUtilCode	Blankj	AndroidUtilCode 是一个强大易用的安卓工具类库，它合理地封装了安卓开发中常用的函数，具有完善的 Demo 和单元测试，利用其封装好的 API，可以大大提高开发效率。
AgentWeb	Justson	AgentWeb 是一个基于的 Android WebView，极度容易使用以及功能强大的库，提供了 Android WebView 一系列的问题解决方案，并且轻量和极度灵活。
XPopup	li-xiaojun	内置几种了常用的弹窗，十几种良好的动画，将弹窗和动画的自定义设计的极其简单。
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相关的文件。
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。
OkDownload	LingoChamp	可靠，灵活，高性能以及强大的下载引擎。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。

敏感凭证泄露检测

可能的密钥
"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"
ab677a736f1605f3131b7c5c43ada799
3uGkvLPCenxYndKwVJHfEVGTs8CjqVY5

本报告由南明离火移动安全分析平台生成

4c053e1ca87d459ea9d19b73d7297a0f
GcgzsKdDZTumABNz7uujrCfPIk9TQ355

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患。