南明离火
移动应用检测平台

ANDROID 静态分析报告

亲朋打僵尸 • v1.0

分析日期: 2024-02-26 18:19:09

应用概览

文件名称:	qpdjs_itmop.com.apk
文件大小:	14.7MB
应用名称:	亲朋打僵尸
软件包名:	com.moon.zombie
主活动:	com.moon.zombie.Launcher
版本号:	1.0
最小SDK:	9
目标SDK:	9
加固信息:	未加壳
应用程序安全分数:	47/100 (中风险)
杀软检测:	8 个杀毒软件报毒
MD5:	027c73d6bc1ac0a24f96eaed77a689a4
SHA1:	86b1cd30dd260f5acd0f179b6b6f404d374bcfa9
SHA256:	705d99025bf3a2b5b0d36ef09[illegible]946d747adc4e3200[illegible]67af5a229d1ec63a

分析结果严重性分布

高危	中危	信息	安全	关注
5	1	2	3	6

四大组件导出状态统计

Activity组件：7个，其中export的有：0个
Service组件：0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

二进制文件已签名
v1 签名: True

v2 签名: False
v3 签名: False
v4 签名: False
主题: ST=guangdong, L=shenzhen, O=vkings, OU=vkings, CN=lizs
签名算法: rsassa_pkcs1v15
有效期自: 2016-08-11 13:38:56+00:00
有效期至: 2116-07-18 13:38:56+00:00
发行人: ST=guangdong, L=shenzhen, O=vkings, OU=vkings, CN=lizs
序列号: 0x7b87c210
哈希算法: sha256
证书MD5: c1b5cb01128ad251ea2ccf7d8544d160
证书SHA1: 27ac44ec2e0a0be8c5bf01fc78b9406c6c3bc566
证书SHA256: b97bfac73be769a102c208c5b8df8838144b9fe42ee34e9f3ed9d25fd75784c6
证书SHA512:
14112de30d50e181ff532cf3ce8a0160bada1e22377d1ac16cadb8d5729ffa253fdf704b40f7216830c81574e5743f6741e930a2b57020c8ffcc1263d848e70

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.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_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.SEND_SMS	危险	发送短信	允许应用程序发送短信。恶意应用程序可能会不经您的确认就发送信息，给您带来费用。
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_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.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.BATTERY_STATS	普通	修改电池统计	允许对手机电池统计信息进行修改
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.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。
com.android.launcher.permission.INSTALL_SHORTCUT	签名	创建快捷方式	这个权限是允许应用程序创建桌面快捷方式。
com.android.launcher.permission.READ_SETTINGS	危险	读取桌面快捷方式	这种权限的作用是允许应用读取桌面快捷方式的设置。
android.permission.MANAGE_DOCUMENTS	签名	允许管理文档访问，通常在选择器中	允许应用程序管理对文档的访问，通常作为文档选取器的一部分。
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.webkit.permission.PLUGIN	未知	未知权限	来自 android 引用的未知权限。
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。

cn.swiftpass.wxpay.permission.MMOAUTH_CALLBACK	未知	未知权限	来自 android 引用的未知权限。
cn.swiftpass.wxpay.permission.MM_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
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错略的经纬度信息，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.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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
xvtian.gai.receiver	未知	未知权限	来自 android 引用的未知权限。
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。

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: **1** | 警告: **0** | 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
应用程序存在Janus漏洞	高危	应用程序使用了v1签名方案进行签名，如果只使用v1签名方案，那么它就容易受到安卓5.0-8.0上的Janus漏洞的攻击。在安卓5.0-7.0上运行的使用了v1签名方案的应用程序，以及同时使用了v2/v3签名方案的应用程序也同样存在漏洞。

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 2.3-2.3.2 [minSdk=9]	警告	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	应用程序数据存在被泄露的风险 未设置[android:allowBackup]标志	警告	这个标志 [android:allowBackup]应该设置为false。默认情况下它被设置为true，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。

代码安全漏洞检测

高危: **4** | 警告: **8** | 信息: **2** | 安全: **2** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	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
2	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
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	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
5	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
6	SHA-1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
7	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
8	此应用已使用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	应用程序可以写入应用程序目录。敏感信息应加密	信息	CWE: CWE-276: 默认权限不正确 OWASP MASVS: MSTG-STORAGE-14	升级会员：解锁高级权限
10	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
11	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
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
13	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
14	应用程序使用带PKCS5/PKCS7填充的加密模式CBC。此配置容易受到填充oracle攻击。	高危	CWE: CWE-649: 依赖于混淆或加密安全相关输入而不进行完整性检查 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	升级会员：解锁高级权限
15	不安全的Web视图实现。WebView忽略SSL证书错误并接受任何SSL证书。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
16	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

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)	SYMBOLSSTRIPPED(裁剪符号表)
1	armeabi/libcasdkjni.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	No 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	False warning 符号可用

2	armeabi/libidentifyapp.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	False warning 符号可用
3	armeabi/libplugin_phone.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	False warning 符号可用

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.READ_PHONE_STATE android.permission.SEND_SMS android.permission.VIBRATE android.permission.ACCESS_COARSE_LOCATION android.permission.CAMERA android.permission.SYSTEM_ALERT_WINDOW

本报告由南明离火移动安全分析平台生成

其它常用权限	9/46	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_WIFI_STATE android.permission.BATTERY_STATS android.permission.ACCESS_NETWORK_STATE com.android.launcher.permission.INSTALL_SHORTCUT android.permission.CHANGE_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
api.ipaynow.cn	安全	是	**IP地址:** 103.244.232.20 **国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看:** 高德地图
zhifu.dev.swiftpass.cn	安全	否	No Geolocation information available.
pay.swiftpass.cn	安全	是	**IP地址:** 111.230.118.187 **国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看:** 高德地图
posp.ipaynow.cn	安全	是	**IP地址:** 211.154.166.174 **国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看:** 高德地图
gw.tenpay.com	安全	否	No Geolocation information available.
example.com	安全	否	**IP地址:** 93.184.216.34 **国家:** United States of America **地区:** Virginia **城市:** Ashburn **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
huangjun.dev.swiftpass.cn	安全	否	No Geolocation information available.

ospd.mmarket.com	安全	是	**IP地址:** 120.197.235.71 **国家:** China **地区:** Guangdong **城市:** Guangzhou **纬度:** 23.127361 **经度:** 113.264252 **查看:** 高德地图
paya.swiftpass.cn	安全	是	**IP地址:** 193.112.234.72 **国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397231 **查看:** 高德地图
www.zhifuka.net	安全	否	No Geolocation information available.
da.mmarket.com	安全	是	**IP地址:** 120.232.188.83 **国家:** China **地区:** Guangdong **城市:** Guangzhou **纬度:** 23.127361 **经度:** 113.264252 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件
• https://msp.alipay.com/x.htm	com/alipay/android/Constant.java
• https://mobilegw.alipay.com/mgw.htm	com/alipay/mobilesecuritysdk/face/a.java
• http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:feedback	com/chinaMobile/k.java
• http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:getapplatameter&appkey= • 10.0.0.172 • http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:postactlog • http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:posterrlog • http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:posteventlog • http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:postsyslog	com/chinaMobile/MobileAgent.java
• https://pay.swiftpass.cn/ • http://huangjun.dev.swiftpass.cn/	com/switfpass/pay/MainApplication.java
• http://huangjun.dev.swiftpass.cn/pay/gateway	com/switfpass/pay/activity/AsyncTaskC0022e.java
• https://api.weixin.qq.com/cgi-bin/token?grant_type=client_credential&appid=%s&secret=%s • http://zhifu.dev.swiftpass.cn/spay/notify	com/switfpass/pay/activity/PayPlugin.java
• https://gw.tenpay.com/gateway/normalorderquery.xml?	com/switfpass/pay/utils/Constants.java
• http://211.154.151.196:8081/tenpay/payment/notifyCallBackUrl	com/switfpass/pay/utils/Util.java

• http://www.zhifuka.net/gateway/mbphonepay/mbphonepay.asp? • http://www.zhifuka.net/gateway/mbphonepay/mbphonepay.asp?customerid= • https://paya.swiftpass.cn/pay/gateway	com/xqt/now/paysdk/XqtPay.java
• http://ospd.mmarket.com:80/taac • http://ospd.mmarket.com:80/trust • http://ospd.mmarket.com:80/trusted3	mm/purchasesdk/l/d.java
• 192.168.11.5 • 10.0.0.172	mm/purchasesdk/l/g.java
• https://msp.alipay.com/x.htm • https://mobilegw.alipay.com/mgw.htm • http://ospd.mmarket.com:80/taac • http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:postactlog • http://ospd.mmarket.com:80/trusted3 • http://m.alipay.com/?action=h5quit • https://api.weixin.qq.com/cgi-bin/token?grant_type=client_credential&appid=%s&secret=%s • https://gw.tenpay.com/gateway/normalorderquery.xml? • http://huangjun.dev.swiftpass.cn/pay/gateway • http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:getappparameter&appkey= • https://pay.swiftpass.cn/ • https://mclient.alipay.com/home/exterfaceAssign.htm? • https://wappaygw.alipay.com/home/exterfaceAssign.htm? • 192.168.11.5 • http://www.zhifuka.net/gateway/mbphonepay/mbphonepay.asp?customerid= • http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:posteventlog • http://example.com/ • http://211.154.151.196:8081/tenpay/payment/notifyCallBackUrl • https://paya.swiftpass.cn/pay/gateway • 10.0.0.172 • 127.0.0.255 • https://mclient.alipay.com/sdkErrorlog.do • http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:postsyslog • http://zhifu.dev.swiftpass.cn/spay/notify • http://mcgw.alipay.com/gateway.do • http://www.zhifuka.net/gateway/mbphonepay/mbphonepay.asp? • http://ospd.mmarket.com:80/trust • http://huangjun.dev.swiftpass.cn/ • http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:posterrlog • http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:feedback	自研引擎分析结果
• http://api.ipaynow.cn/ • http://posp.ipaynow.cn:10900/	lib/armeabi/libplugin_phone.so

第三方 SDK 组件分析

SDK名称	开发者	描述信息
支付宝 SDK	Alipay	支付宝开放平台基于支付宝海量用户，将强大的支付、营销、数据能力，通过接口等形式开放给第三方合作伙伴，帮助第三方合作伙伴创建更具竞争力的应用。

邮箱地址敏感信息提取

EMAIL	源码文件
wftid@swiftpass.cn	com/switfpass/pay/utils/Constants.java

wftid@swiftpass.cn	自研引擎分析结果

敏感凭证泄露检测

可能的密钥
"no_token_id" : "订单号为空或位数不对，请检查输入的订单号！"
54aa526e7a37d8ba2311a1d3d2ab79b3fbeaf3ebb9e7da9e7cdd9be1ae5a53595f47
8cc1d6ed5e1b2cc00489215aec3fc2eac008e767b0215981cb5e
11300f06035504081308536861 6e67686169311130
15060355040a130e4368696e6120556e696f6e506179311730150603550 40b130e4
3634385a3078310b3009060355040613023836 31
0a54b19a13b6712dc04d1b49215423d8
9d101c97133837e13dde2d32a5054abb
b1ff56cef0e21c87260c63ce3ca868bf5974c14
92a864886f70d010101050003818d0030818902818100c42e6236d5054ffccaa
64c2f89fdffa16729c9779f99562bc189d2ce4722ba0faedb11aa22d0d9db228fda
0dc1c1c001c4d6c48241ce1ac41fd5a0
efedc24fecde188aaa9161
XwYp8WL8bm6S4wu6yEYmLGy4RRRdJDIhxCBdk3[illegible]N7i[illegible]Qoj1bScVZEeVp9vBNsg[illegible]wD[illegible]tqZHP8QLoFM6o6MRYjW8QqyrZBI654mqoUk5SOLDyzordzOU5QhYguEJh54q3K1KqMEXpdEQJJjs1Urqjm2s[illegible]fCZ[illegible]hMuIjAMRrEQIuA7Fe[illegible]qWMJQwghcLcPVIeQ8PLzAcaKidybmwhvNAxIyKRpbZIcDjNCcUvsJYvyzEA9VUIaHkIAJ62lpA3EE3H
f6e5061793111300f06035504031308[illegible]6f6e50617930819[illegible]
08eb9b5c67474d027fa03ce35109b11604083ab6bb4df2c46240f879f
134e3265829ff82daf16e7b740a600b5
f6e50617931173015[illegible]60355040b130e43686[illegible]20556e696
d9255940ca7b6cd07483f4b4243fd1825b2705
3015060355040a130e436869[illegible]20556e696
861693111300f06035[illegible]1308[illegible]368616e67686169311730
0f0603550407130[illegible]6e676861693117
1001a3e74c601e3beb1b7ae4f9ab2872a0aaf1dbc2cba89c7528cd
891b9b2a1d867f95eefd537a56d4d805
e94ddc285669ec06b8a405dd4341eac4ea7030203010001300d06092a864886f70d010105050003818

hjwg16Y0G83C18H9wpMLWi25KDSLyNLA2I509GQ5wydMj2qRYVHjf9fV7Xl9cfcFstlYsOtRAxdUcMOa0nkO1qhsbeEqirQRJmnW0Yub6Yar1FzfWJTlHutV43HJmd8E
d6fc3a4a06adbde89223b
b1fdf62b0f540fca5458b063af9354925a6c3505a18ff164b6b195f6e517eaee1fb783
6e696f6e5061793111300f06035504031308556e696f6e5061
23456789abcdef12123456786789abcd

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。