南明离火
移动应用检测平台

ANDROID 静态分析报告

微觅圈 • v1.0.0

分析日期: 2025-04-11 05:39:06

i应用概览

文件名称:	微觅圈 v1.0.0.apk
文件大小:	6.89MB
应用名称:	微觅圈
软件包名:	v01dk.v9bt1.kqkk8
主活动:	o5ijst.ruvmuv.tf2cuc.mowh71
版本号:	1.0.0
最小SDK:	23
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:	61/100 (低风险)
杀软检测:	25 个杀毒软件报毒
MD5:	ec159a27b02ad63a4699e9216a0353e5
SHA1:	94e24b52d838a330d273239d9a3ea306fa908239
SHA256:	291b624532b6498a50cbbad5eff1a5e34ce2cf9625158fa2301c629dee7c51f6

⚠恶意软件家族信息

恶意家族	QinyueRansom
描述信息	QinyueRansom（勤月勒索）是一款勒索软件，由南明离火平台根据其关键包名"com.qinyue.vmain.activity"进行命名，其活动最早可追溯至2023年9月，该软件疑似由一个缅甸诈骗团伙运营，主要通过窃取受害者的聊天记录和观看色情视频来对受害者进行恐吓，进而勒索财物。这个恶意软件家族在国内非常活跃，受害者众多，常见的相关恶意软件名称包括：奴欲、趣约、猫咪、兔兔、陌聊、91传媒、同城约、欲乐园、番茄社区、动态网、私密空间、同城韦丽、激情互动、纯欲派对、闭月羞花以及私密相冊管家等。
C2服务器	http://115.159.23.175:16904/api/uploadimgs http://115.159.23.175:16904/api/sublist http://115.159.23.175:16904/api/register http://115.159.23.175:16904/api/subsmslist
凭证数据	升级会员：解锁高级权限
关联情报	升级会员：解锁高级权限

分析结果严重性

高危	中危	信息	安全	关注
1	10	1	3	1

四大组件信息

Activity组件：6个，其中export的有： 3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：2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: True
v4 签名: False
主题: C=adminl7ef4e, ST=adminl7ef4e, L=adminl7ef4e, O=adminl7ef4e, OU=adminl7ef4e, CN=adminl7ef4e
签名算法: rsassa_pkcs1v15
有效期自: 2025-03-13 07:12:30+00:00
有效期至: 2125-02-17 07:12:30+00:00
发行人: C=adminl7ef4e, ST=adminl7ef4e, L=adminl7ef4e, O=adminl7ef4e, OU=adminl7ef4e, CN=adminl7ef4e
序列号: 0xa6c037c
哈希算法: sha256
证书MD5: c37be7b14b801b103849cf2d5689c131
证书SHA1: 63541bccf76005447e093850ac83699dc58ad10b
证书SHA256: e9e92e0d73629b35ac5221e3641[illegible]8b892845370ef3b6f0a6[illegible]da34ff8a
证书SHA512:
d664bfc896a40a064e5dc862dfbe9b4a02d245[illegible]f0d69709608662dd[illegible]4b5[illegible]6b4d69b99cf3e57c7f2ec03aedee234858f90c019a76fe55fe6bf5c689e3344d

公钥算法: rsa
密钥长度: 1024
指纹: c9a0e7848045cc1e2d1e6[illegible]b95eefb4ae7e664a4425bb[illegible]7088a071c1b281d
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.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.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.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.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_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.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。

网络通信安全

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	应用程序已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用程序打算使用明文网络流量，例如明文HTTP，FTP协议，DownloadManager和MediaPlayer。针对API级别27或更低的应用程序，默认值为“true”。针对API级别28或更高的应用程序，默认值为“false”。避免使用明文流量的主要原因是缺乏机密性，真实性和防篡改保护；网络攻击者可以窃听传输的数据，并且可以在不被检测到的情况下修改它。
2	应用程序具有网络安全配置 [android:networkSecurityConfig=@xml/c]	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	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: **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	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
3	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
4	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
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	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	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
8	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

9	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

行为分析

编号	行为	标签	文件
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
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
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00035	查询已安装的包列表	反射	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
00031	检查当前正在运行的应用程序列表	反射 信息收集	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
00036	从 res/raw 目录获取资源文件	反射	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
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
00054	从文件安装其他APK	反射	升级会员：解锁高级权限
00202	打电话	控制	升级会员：解锁高级权限
00203	将电话号码放入意图中	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
00033	查询IMEI号	信息收集	升级会员：解锁高级权限
00119	将IMEI号写入文件	信息收集 文件 电话服务 命令	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
00192	获取短信收件箱中的消息	短信	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
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

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
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
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
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
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
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
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

敏感权限分析

类型	匹配	权限
恶意软件常用权限	2/30	android.permission.READ_CONTACTS android.permission.READ_SMS
其它常用权限	5/46	android.permission.ACCESS_NETWORK_STATE android.permission.INTERNET android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.RECORD_TASKS

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
www.wanandroid.com	安全	是	**IP地址:** 39.101.178.149 **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链接分析

URL信息	源码文件

• https://www.wanandroid.com/	o5ijst/ruvmuv/r750zo/t84w_v/jqwuno.java
• http://115.159.23.175:16904/api/register • http://115.159.23.175:16904/api/sublist • http://115.159.23.175:16904/api/subsmslist • http://115.159.23.175:16904/api/uploadimgs	o5ijst/ruvmuv/hye45k/opwyw1/fv2voq.java

第三方SDK

SDK名称	开发者	描述信息
Jetpack Test	Google	在 Android 中进行测试。
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。
AndroidAutoSize	JessYanCoding	今日头条屏幕适配方案终极版，一个极低成本的 Android 屏幕适配方案。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。

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。