



ANDROID 静态分析报告



◆ 遇见心动 · v1.0.0

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

分析日期: 2025-04-08 12:25:45

i应用概览

| | |
|----------|--|
| 文件名称 | 遇见心动 v1.0.0.apk |
| 文件大小 | 7.02MB |
| 应用名称 | 遇见心动 |
| 软件包名 | tjsro.kd7py.g0cgu |
| 主活动 | tjsro.kd7py.g0cgu.SplashActivity |
| 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: | c5b74124ac71cf959fe484ab6af5a339 |
| SHA1: | a5e4ff693ecfa9749e75c1528c9e77bb8a7623e0 |
| SHA256: | f1d8e8638477bf92dc817e3c9162bb38fd958b469558d92c54831f5d4339b52d |

▲ 恶意软件家族信息

| | |
|-------|--|
| 恶意家族 | QinyueRansom |
| 描述信息 | QinyueRansom (某月勒索) 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, 其活动最早可追溯到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、动态网盘、私密空间、同城佳丽、激情互动、纯欲派对、闭月羞花以及私密相册管家等。 |
| C2服务器 | http://120.24.175.2:16897/api/uploadimgs http://120.24.175.2:16897/api/subsmslist http://120.24.175.2:16897/api/register http://120.24.175.2:16897/api/sublist |
| 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 | i 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=qglcw6, ST=qglcw6, L=qglcw6, O=qglcw6, OU=qglcw6, CN=qglcw6

签名算法: rsassa_pkcs1v15

有效期自: 2024-09-08 12:18:32+00:00

有效期至: 2124-08-15 12:18:32+00:00

发行人: C=qglcw6, ST=qglcw6, L=qglcw6, O=qglcw6, OU=qglcw6, CN=qglcw6

序列号: 0x7133fd8

哈希算法: sha256

证书MD5: 24f9ab00560ad42aab50fd433b9b2677

证书SHA1: 83f7d9f40cc386b3cb843a20671d806c71919d32

证书SHA256: a2ce1ba61676b87f256284e35c00d70cb9484f419581669d8f2f8a03e8d4be49

证书SHA512:

3f18303910cd2bac42602dd4a8b98f0679be41eac7da560f3a45a7a0b7a1b0127ab712b7756d827953172f99e3290bd7e5416a9f1a00ef72817e22b079c166a

公钥算法: rsa

密钥长度: 1024

指纹: cecf7dd23bb80e87ac6fae1dc05e10abd9d9dc3e7b96823c42f0157537c7b3b4

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时进行修改。 |
| 2 | 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。 |
| 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 | 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 |
| 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 | 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 |
| 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 |
| 7 | 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 |
| 8 | SHA1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: MST G-NETWORK-4 | 升级会员: 解锁高级权限 |
|---|---|----|------------------------------|------------------------------|

行为分析

| 编号 | 行为 | 标签 | 文件 |
|-------|------------------------------|--------------------------|------------------------------|
| 00189 | 获取短信内容 | 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 |
| 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 |
| 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 |
| 00191 | 获取短信收件箱中的消息 | 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 |
| 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 |
| 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 |
| 00012 | 读取数据并放入缓冲流 | 文件 | 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 |
| 00003 | 将压缩后的位图数据放入JSON对象中 | 相机 | 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 |
| 00001 | 初始化位图对象并将数据 (例如 PNG) 压缩为位图对象 | 相机 | 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 00192 | 获取短信收件箱中的消息 | 短信 | 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.REORDER_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 |
|--|--------------------------------------|
| <ul style="list-style-type: none"> http://120.24.175.2:16897/api/uploadimgs http://120.24.175.2:16897/api/subsmsglist http://120.24.175.2:16897/api/register http://120.24.175.2:16897/api/sublist | com/qinyue/vmain/activity/Urls.java |
| <ul style="list-style-type: none"> https://www.wanandroid.com/ | com/qinyue/vcommon/http/HttpUrl.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 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，深入扫描软件中潜在的漏洞和安全隐患。

© 2025 南明离火 - 移动安全分析平台自动生成