南明离火
移动应用检测平台

ANDROID 静态分析报告

Statter • v1.1.9

分析日期: 2024-05-31 16:10:34

应用概览

文件名称:	Statter.apk
文件大小:	35.26MB
应用名称:	Statter
软件包名:	com.xxxx.statter
主活动:	com.xxxx.statter.WelcomeActivity
版本号:	1.1.0
最小SDK:	23
目标SDK:	33
加固信息:	顶像科技 加固
应用程序安全分数:	43/100 (中风险)
杀软检测:	AI评估：安全
MD5:	a0f9ffad41357f5e9287363334d18452
SHA1:	282eb5669450e463f230ed4c168caa0c8c22ccad
SHA256:	64859077fd328c76ffeead6357[illegible]197ed604139f19bf[illegible]675256a9436471b

分析结果严重性分布

高危	中危	信息	安全	关注
6	6	3	2	3

四大组件导出状态统计

Activity组件：72个，其中export的有：2个
Service组件：1个，其中export的有：0个
Receiver组件：0个，其中export的有：0个
Provider组件：1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

本报告由南明离火移动安全分析平台生成

v2 签名: True
v3 签名: False
v4 签名: False
主题: CN=statter
签名算法: rsassa_pkcs1v15
有效期自: 2022-06-09 06:48:35+00:00
有效期至: 2047-06-03 06:48:35+00:00
发行人: CN=statter
序列号: 0x3c627cc4
哈希算法: sha256
证书MD5: 6afa09a588821e25a90745e9a6e0a5e6
证书SHA1: 6f89d49c08d1df94176c0f19a98f2c7a4108dd53
证书SHA256: 1a126e192936861cfc0688e62845e2abd492cd008dfc4e9b9f75ebdb3a39488c
证书SHA512:
2fa65a32dcec7a8ad4eb684573ece2038266ca6753f15f5dc7a15852e8fe17d699f618455d464ff8c78357166a572d5fa435451aa7cbd5cf7fd94ac2042544f1

公钥算法: rsa
密钥长度: 2048
指纹: 7d214cc6d3d6d845da52c7996f146994b4391341c2b16b919e7488d88fda9a32
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.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.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.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.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_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.USE_BIOMETRIC	普通	使用生物识别	允许应用使用设备支持的生物识别方式。
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.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.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.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.PERMISSION_GRANTED	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.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.USE_FINGERPRINT	普通	允许使用指纹	此常量在 API 级别 28 中已弃用。应用程序应改为请求USE_BIOMETRIC

android.permission.MANAGE_EXTERNAL_STORAGE	危险	文件列表访问权限	Android11新增权限，读取本地文件，如简历，聊天图片。
com.xxxx.statter.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.xxxx.statter.login.activity.AuthorizationActivity	Schemes: stt://, Hosts: com.statter,
com.xxxx.statter.dapps.activity.AdvancedContractActivity	Schemes: xl://, Hosts: goods, Ports: 8888, Paths: /AdvancedContract,
com.xxxx.statter.MainActivity	Schemes: wc://,

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: **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: **6** | 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 6.0-6.0.1, [minSdk=23]	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。
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	Activity设置了TaskAffinity属性 (com.xxxx.statter.wc.activity.WCAuthorizedActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
5	Activity (com.xxxx.statter.login.activity.AuthorizationActivity) 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。
6	Activity (com.xxxx.statter.MainActivity) 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。
7	数据短信接收端设置在端口: 8888 上 [android:port]	警告	一个二进制短信接收器被配置为监听一个端口。发送到设备的二进制短信由应用程序以开发者选择的方式处理。这个短信中的数据应该被应用程序正确地验证。此外，应用程序应该假设接收到的短信来自一个不可信的来源。

代码安全漏洞检测

高危: **6** | 警告: **9** | 信息: **3** | 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	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	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
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	使用弱加密算法	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-4	升级会员：解锁高级权限

6	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
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	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
9	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
10	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
11	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
12	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，因为它为相同的明文块[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
13	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

14	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
15	不安全的Web视图实现。Web视图忽略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	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
17	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
18	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
19	此应用程序使用SQL Cipher。SQLCipher为sqlite数据库文件提供256位AES加密	信息	OWASP MASVS: MSTG-CRYPTO-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)	SYMBOLS STRIPPED(裁剪符号表)
1	arm64-v8a/libstub000.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检查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

2	arm64-v8a/libsys_misc.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	True info 二进制文件有以下加固函数: ['__FD_ISSET_chk', '__vsprintf_chk', '__memmove_chk', '__strchr_chk', '__strrchr_chk', '__memcpy_chk', '__FD_SET_chk', '__vsnprintf_chk', '__strcat_chk', '__read_chk', '__strlen_chk']	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	4/30	android.permission.READ_PHONE_STATE android.permission.VIBRATE android.permission.REQUEST_INSTALL_PACKAGES android.permission.CAMERA
其它常用权限	6/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.FOREGROUND_SERVICE

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
echo.walletconnect.com	安全	是	**IP地址:** 118.193.240.41 **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

www.winimage.com	安全	否	**IP地址:** 205.251.81.217 **国家:** 美利坚合众国 **地区:** 新泽西州 **城市:** 帕西帕尼 **纬度:** 40.862041 **经度:** -74.406120 **查看:** Google 地图
statter.io	安全	否	**IP地址:** 34.134.97.162 **国家:** 美利坚合众国 **地区:** 爱荷华州 **城市:** 康瑟尔布拉夫斯 **纬度:** 41.261940 **经度:** -95.86083 **查看:** Google 地图
info.chaindigg.com	安全	是	**IP地址:** 120.53.206.239 **国家:** 中国 **地区:** 山东 **城市:** 青岛 **纬度:** 36.098610 **经度:** 120.371941 **查看:** 高德地图
bsc-dataseed1.binance.org	安全	否	**IP地址:** 35.74.137.105 **国家:** 美利坚合众国 **地区:** 华盛顿 **城市:** 西雅图 **纬度:** 47.627499 **经度:** -122.346199 **查看:** Google 地图
apilist.tronscanapi.com	安全	否	**IP地址:** 18.196.44.239 **国家:** 德国 **地区:** 黑森 **城市:** 美因河畔法兰克福 **纬度:** 50.110882 **经度:** 8.681996 **查看:** Google 地图
docs.walletconnect.com	安全	否	**IP地址:** 76.76.21.22 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 核桃 **纬度:** 34.015400 **经度:** -117.858223 **查看:** Google 地图
wiki.torproject.org	安全	否	**IP地址:** 116.202.120.166 **国家:** 德国 **地区:** 拜仁 **城市:** 贡岑豪森 **纬度:** 48.323860 **经度:** 11.601019 **查看:** Google 地图

tronscan.org	安全	否	**IP地址:** 172.66.43.46 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
keys.walletconnect.com	安全	否	**IP地址:** 18.197.16.228 **国家:** 德国 **地区:** 黑森 **城市:** 美因河畔法兰克福 **纬度:** 50.110882 **经度:** 8.681996 **查看:** Google 地图
apilist.tronscan.org	安全	否	**IP地址:** 3.135.24.13 **国家:** 美利坚合众国 **地区:** 俄亥俄州 **城市:** 哥伦布 **纬度:** 39.961380 **经度:** -82.997749 **查看:** Google 地图
api-cn.etherscan.com	安全	否	**IP地址:** 217.79.243.34 **国家:** 美利坚合众国 **地区:** 佛罗里达州 **城市:** 坦帕 **纬度:** 27.947519 **经度:** -82.458427 **查看:** Google 地图
apifox.com	安全	是	**IP地址:** 120.27.226.76 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.293650 **经度:** 120.161583 **查看:** 高德地图
xxx.com	安全	否	**IP地址:** 141.0.173.173 **国家:** 荷兰（王国） **地区:** 北荷兰省 **城市:** 阿姆斯特丹 **纬度:** 52.378502 **经度:** 4.899980 **查看:** Google 地图
api.bscscan.com	安全	否	**IP地址:** 23.92.68.154 **国家:** 美利坚合众国 **地区:** 佛罗里达州 **城市:** 坦帕 **纬度:** 28.007360 **经度:** -82.515450 **查看:** Google 地图

greenrobot.org	安全	否	**IP地址:** 85.13.163.69 **国家:** 德国 **地区:** 图林根 **城市:** 弗里德斯多夫 **纬度:** 50.604919 **经度:** 11.035770 **查看:** Google 地图
stattertrx.xyz	安全	否	**IP地址:** 34.66.25.74 **国家:** 美利坚合众国 **地区:** 爱荷华州 **城市:** 康瑟尔布拉夫斯 **纬度:** 41.261940 **经度:** -95.86083 **查看:** Google 地图
www.zetetic.net	安全	否	**IP地址:** 13.225.114.113 **国家:** 大韩民国 **地区:** 京畿道 **城市:** 利川市 **纬度:** 37.279179 **经度:** 127.442421 **查看:** Google 地图
httpseed.bitcoin.schildbach.de	安全	否	No Geolocation information available.
eth-mainnet.improd.words	安全	否	No Geolocation information available.
verify.walletconnect.com	安全	否	**IP地址:** 52.57.114.123 **国家:** 德国 **地区:** 黑森 **城市:** 美因河畔法兰克福 **纬度:** 50.110882 **经度:** 8.681996 **查看:** Google 地图
relay.walletconnect.com	安全	否	**IP地址:** 18.143.19.154 **国家:** 新加坡 **地区:** 新加坡 **城市:** 新加坡 **纬度:** 1.289987 **经度:** 103.850281 **查看:** Google 地图
rpc.walletconnect.com	安全	否	**IP地址:** 52.58.89.212 **国家:** 德国 **地区:** 黑森 **城市:** 美因河畔法兰克福 **纬度:** 50.110882 **经度:** 8.681996 **查看:** Google 地图
solidity.readthedocs.io	安全	否	**IP地址:** 104.17.33.82 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图

statter.app	安全	否	**IP地址:** 35.232.159.135 **国家:** 美利坚合众国 **地区:** 爱荷华州 **城市:** 康瑟尔布拉夫斯 **纬度:** 41.261940 **经度:** -95.860832 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• https://tronscan.org/#/representative/	com/xxxx/statter/utils/tron/security/Constants.java
• https://statter.io/#/resource • https://statter.io • http://statter.app:8577/user-agreement.html	com/xxxx/statter/Global.java
• 35.232.159.135	com/xxxx/statter/GlobalWallet.java
• 107.148.238.67 • https://apifox.com • http://107.148.238.67:8080/insertinfo	com/xxxx/statter/MainActivity.java
• http://httpseed.bitcoin.schildbach.de/peers	org/bitcoinj/params/MainNetParams.java
• https://bsc-dataseed1.binance.org/	com/xxxx/statter/home/utils/WalletUtils.java
• https://api.bscscan.com • http://statter.app/ • 154.91.83.138 • 156.251.30.20 • https://api-cn.etherscan.com/ • 34.29.206.156 • https://info.chaindigg.com • http://34.66.25.74:8090 • http://35.232.159.135/ • https://eth-mainnet.improd.words • http://172.247.250.123:8077/datetok/ • https://apilist.tronscan.org • http://statter[redacted]:8090 • 34.134.98.47 • https://apilist.tronscanapi.com • 35.232.159.135 • 34.66.25.74	com/xxxx/statter/http/AppGetAPIManager.java

• https://wiki.torproject.org/theonionrouter/torfaq#socksanddns	com/subgraph/orchid/socks/SocksRequest.java
• 127.0.0.1	com/subgraph/orchid/dashboard/DashboardFragment.java
• https://verify.walletconnect.com/	com/walletconnect/android/internal/common/di/VerifyModuleKt.java
• http://solidity.readthedocs.io/en/develop/types.html#members	org/web3j/abi/TypeDecoder.java
• 192.168.1.30	com/xxxx/common/config/SpUtilTest.java
• file:////android_asset/how_collect.html	com/xxxx/statter/fragments/DAppsFragment.java
• 119.23.238.152 • 192.168.1.30	com/xxxx/common/http/GetAPIManager.java
• https://echo.walletconnect.com/	com/walletconnect/android/CoreClient.java
• https://docs.walletconnect.com/2.0/specs/clients/sync	com/walletconnect/android/sync/engine/use_case/calls/GetMessageUseCase.java
• https://rpc.walletconnect.com/v1/?chainid=eip155:1&projectid=	com/walletconnect/android/internal/common/signing/eip1271/EIP1271Verifier.java
• https://greenrobot.org/greendao/documentation/database-encryption/	org/greenrobot/greendao/database/DatabaseOpenHelper.java
• https://keys.walletconnect.com	com/walletconnect/android/internal/common/di/KeyServerModuleKt.java
• https://github.com/tootallnate/java-websocket/wiki/lost-connection-detection	org/java_websocket/AbstractWebSocket.java
• 193.23.244.244 • 171.25.193.9 • 82.94.251.203 • 128.31.0.39 • 194.109.206.212 • 86.59.21.38 • 154.35.32.5 • 202.85.227.201 • 212.112.245.170 • 208.83.223.34	com/subgraph/orchid/directory/TrustedAuthorities.java
• wss://relay.walletconnect.com?projectid=d60c2b5bd57e262760f8508ef4c1a250	com/xxxx/statter/WalletConnectkt.java
• 127.0.0.1	org/bitcoinj/core/PeerAddress.java
• 127.0.0.1	org/bitcoinj/core/PeerGroup.java

• https://www.zetetic.net/sqlcipher/license/ • https://www.zetetic.net/sqlcipher/ • https://xxx.com • https://github.com/sqlcipher/android-database-sqlcipher	自研引擎-S
• http://www.winimage.com/zlibdll	lib/arm64-v8a/libsys_misc.so

第三方 SDK 组件分析

SDK名称	开发者	描述信息
SQLCipher	Zetetic	SQLCipher 是一个 SQLite 扩展，它提供数据库文件的 256 位 AES 加密能力。
libYUV	Google	libYUV 是 Google 开源的 yuv 图像处理库，实现对各种 yuv 数据之间的转换，包括数据转换，裁剪，缩放，旋转。
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 APIs 可以大大提高开发效率。
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，高效和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。
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 AppCompat	Google	Allows access to new APIs on older API versions of the platform (many using Material Design).

敏感凭证泄露检测

可能的密钥
"password" : "Password"
"library_android_database_sqlcipher_authorWebsite" : "https://www.zetetic.net/sqlcipher/"
"authorization" : "Authorization"
TCFLL5dx5ZJdKnWuesXxi1VPwjLVmWZZy9
14C131DFC5C6F93646BE72FA1401C02A0DF2E8B4
0000000000095413afC295d19EdeB1Ad7B71c952
8ac76a51cc950d9822d68b83fe1ad97b32cd580d
55d398326f99059fF775485246999027b3197955
E534619d5EDcF0cAf673b8AbF7158714F5BD4bd9
23D15D965BC35114467363C165C4F724B64B4F66

00FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE65381FFFFFFFFFFFFFFFF
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
0566B9a8fFb8908682796751EEd00722da967Be0
000000000933ea01ad0ee984209779baaec3ced90fa3f408719526f8d77f4943
EFCBE720AB3A82B99F9E953CD5BF50F7EEFC7B97
1fa4426a1647e5df292757efa5c12981
90758863f6bf42e6585781b04a076930
d60c2b5bd57e262760f8508ef4c1a250
TUpMhErZL2fhh4sVNULAbNKLokS4GjC1F4
D586D18309DED4CD6D57C18FDB97EFA96D330566
49015F787433103580E3B66A1707A00E60F2D15B
42a71397afbaf92492ced302dcc08e51
53590fb8244d600075c539b02a7b97bd
04678afdb0fe5548271967f1a67130b7105cd6a828e03909a67962e0ea1f61deb649f6bc3f4cef38c4f35504e51ec112de5c384df7ba0b8d578a4c702b6bf11d5f
dAC17F958D2ee523a2206206994597C13D831ec7
156ab3346823B651294766e23e6Cf87254d68962
5e5398f0546d1d7afd62641edb14d82894f11dc041bcc363a0c8d0dac82c95a
a7f155fbc59c18b6ad4fb5650067dd41

6080604052348015610010576000080fd5b506000808052602052 7fad3228b676f7d3cd4284a5443f17f1962b36e491b30a40b2405849e597ba5fb580 54600160a060020a031916331790556105008061005960003960 00f3006080604052600436106100825763ffffffff7c010000000000000000000000 0000000000000000000000000000000000000000600035041663 0178b8bf8114610087578063025 71be3146100bb57806306ab5923146100d357806314ab90 38146100fc57806316a25cbd1461012157806318 96f70a146101565780635b0fc9c31461017a575b600080fd5b34801561009357600080fd5b506100 9f60043561019e565b60408051600160a060020a 0390921682525190819003602001 90f35b3480156100c757600080fd5b5061009f6004356101bc56 5b3480156100df57600080fd5b506100fa60043560 2435600160a060020a03604435166101d7565b005b34801561010857600080fd5b506100fa6004 3567ffffffffffffffff6024356 10291565b34801561012d57600080fd5b506101396004356 1035a565b6040805167ffffffffffffffff9092168252519081900360 0200190f35b34801561016257600080fd5b506100fa600435600160a060020a 0360243516610391565b34801561018657600080fd5b506100fa60043 5600160a060020a0360243516610434565b60009081526020819052604090206001015460 0160a060020a031690565b60009081526020819052604 0902054600160a060020a031690565b60008381526020819052604081205484 8490600160a060020a031633146101fc57600080fd5b60408051868152 6020808201879052825191829003830182206001 60a060020a038716835292519294508692889 27fce0457fe73731f824cc27237615a235128c118b4 9d344817417c6d108d155e8292908290030190a350600090815260208190526040902080547 3fffffffffffffffffffffffffffffffffffffff1916600160a060020a03 92909216919091179055505056 5b60008281526020819052604090205482906001 60a060020a031633146102b657600080fd5b60408051675167ffffffffffff ffff84168152905184917f1d4f9bbfc9cab89d66e1a1562f2233ccbf1308cb4f63de2ead5787adddb8fa689190819003602001905a250600091825260208 2905260409091206001018054 67fffffffffffffff9092167401000000000000000000000000000000000000000027fffffffff000000000000000ffffffffffffffff ffffffffffffffffffffffff9092169190911790555 65b60009081526020819052604090206001015474010000000000000000000000000000000000900 467fffffffffffffff1690565b60008281526020819052604090205482906001 60a060020a031633146103b657600080fd5b60408051600160a060020a038 41681529051849 17f1d4f335721b01866dc23fbee8b6b2c7b1e14d6f05c28cd35a2c934239f94095602a0919081900360200190a2506000918252602082 9052604090912060010180547 3fffffffffffffffffffffffffffffffffffffffffffffff1916600160a060020a03909216919091179055565b600082815260208190526040902 0548290600160a060020a031633146104595760 0080fd5b60408051600160a060020a038416815290518491 7fd4735d920b0f87494 13f556dd9b54c8f 309026070caea5c737245152564d266919081900360200190a2506000918252602082905260409091206005473ffffffffffffffffffffffffffffffffffffffff19166001 60a060020a039092169190911790555600a165627a7a72305820f201bf7d54db31743dfa9e72c9529b4b797c8e550d2355afb39d50e2ab48b4fb0029
46852978259cc4b5e92695cead1b7a81
04ffff001d0104455468652054696d65732030332f4a616e2f32303039204368616e63656c6c6f72206f6e206272696e6e206f66207365636f6e6420626 1696c6f757420666f722062616e6b73
TMwFHYXLJaRUPeW6421aqXL4ZEzPRFGkGT
04302390343f91cc401d56d68b123028bf52e5fca1939df127f63c6467cdf9c8e2c14b61104cf817d05780da337893ecc4aaff1309e536162dabbdb4520 0ca2b0a
00000007199508e34a9ff81e6ec0c477a4cccff2a4767a8eee3 c11ab367b008
ED03BB616EB2F60BEC80151114BB25CEF515B226
A0b86991c6218b36c1d19D4a2e9Eb0cE3606eB48
aA8F550ED21aE4ecE978f4141c4551D1DeB7390A
TEkxiTehnzSmSe2XqrBj4w32RUN96Grd28
E8A9C45EDE6D711294A5F8E7951F4DE6CA56B58
0e09fabb73bd3ade0a17ecc321fd13a19e81ce32
00000000000743f190a18c5577a3c2d0a1fc10ae9601ac046a38084ccb7cd721
514910771AF9Ca656af840dff83E8264EcF986CA
1f9840a85d5aF5bf1D1762F925BDADdC4201F984
000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
585769C78764D58426B8B52B6651A5A71137189A
00000000000af0aed4792b1acee3d966af36cf5def14935db8de83d6f9306f2f
a91c23e317b2650d0600d1f10a42a969

7130d2a12b9bcbfae4f2634d864a1ee1ce3ead9c
00000000000C2E074eC69A0dFb2997BA6C7d2e1e
2260FAC5E5542a773Aa44fBCfeDf7C193bc2C599
0238746c59d46d5408bf8b1d0af5740fe1a6e1703fcb56b2953f0b965c740d256f
80550987E1D626E3EBA5E5E75A458DE0626D088C
04fc9702847840aaf195de8442ebecedf5b095cdbb9bc716bda9110971b28a49e0ead8564ff0db22209e0374782c093bb899692d524e9d6a6956e7c5ecbcd68284
0bc529c00C6401aEF6D220BE8C6Ea1667F6Ad93e
00000000000271a2dc26e7667f8419f2e15416dc6955e5a6c6cdf3f2574dd08e
ad90bf3beb7b0eb7e5acd74727dc0da96e0a280a258354e7293fb7e211ac03db
TR7NHqjeKQxGTCi8q8ZY4pL8otSzgjLj6t
608060405234801561001057600080fd5b5060405160208061111dd833981016040525160008054600160a060020a0390921660016 0a060020a03199092169190911790556 1118b806100526000396000f3006080604052600436106100c45763ffffffff7c0100000000000000000000000000000000000000000000000000000000600035041663 01ffc9a781146100c957806310f13a8c146100ff5780632203ab561461019d57806329cd62ea146102375780632dff6941146102555780633b3b57de1461027f57806359d1d43c146102b3578063623195b014610386578063691f3431146103e657806377372213146103fe578063c3d014d61461045c578063c869023314610477578063d5fa2b00146104a8575b600080fd5b3480156100d557600080fd5b506100eb600160e060020a0319600435166104cc565b604080519115158252519081900360200190f35b34801561010b57600080fd5b5060408051602060046024803582810135601f81018590048502860185019096528585526101 9b95833595369560449491939091019190819084018382808284375050604080516020601f89358b01803591820183900483028401830190945280835295979699988101979196509182019450925082915084018382808284375094975061063996505050505050505050565b005b3480156101a957600080fd5b506101b86004356024356103 4d565b60405180838152602001806020018281038252838181518152602001915080519060200190808383600 05b838110156101fb578181015183820152602001610 1e3565b50505050905090810190601f1680156102285780820380516001836020036101000a031916815260200191505b50935050505050604051809103 90f35b34801561024357600080fd5b5061019b600435602435604435610959565b34801561026157600080fd5b5061026d600435610a5d565b60408051918252519081900360200190f35b34801561028b57600080fd5b50610297600435610a73565b60408051600160a060020a0390921682525190819003602001 90f35b3480156102bf57600080fd5b5060408051602060046024803582810135601f81018590048502860185019096528585526103119583359536956044949193909101919081908401838280828437509497506[illegible]a5e96505050505050505050565b6040805160208082528351818301528351919283929083019180519080838360005b8381101561034b5781810151838201526020016103 33565b50505050905090810190601f16801561037857808203805160018360200361 01000a031916815260200191505b509250505050604051809103 90f35b34801561039257600080fd5b506040805160206004604435818101 35601f810184900484028501840190955284845261019b9482359460248035953695946064949201919081908401838280828437509497506 10b9796505050505050505050565b3480156103[illegible]57600080fd5b50610311[illegible]0435610c9c565b34801561040a57600080fd5b50604080516020600460248035828101 35601f8101859004850286018501909652858552610 19b958335953695604494919390910191908190840183828082843750949750610d4096505050505050505050565b34801561046857600080fd5b5061019b600435602435610e9a565b34801561048357600080fd5b5061048f600435610f7f565b6040805192835260208301919091528051918290030190f35b3480156104b457600080fd5b5061019b600435600160a060020a0360243516610f9c565b6000600160e060020a031982167f3b3b57de00000000000000000000000000000000000000000000000000000000148061052f5750600160e060020a031982167fd8389dc500000000000000000000000000000000000000000000000000000000145b806105635750600160e060020a031982167f691f343100000000000000000000000000000000000000000000000000000000145b806105975750600160e060020a031982167f2203ab5600000000000000000000000000000000000000000000000000000000145b806105cb5750600160e060020a031982167fc869023300000000000000000000000000000000000000000000000000000000145b806105ff5750600160e060020a031982167f59d1d43c00000000000000000000000000000000000000000000000000000000145b806106335750600160e060020a031982167f01ffc9a700000000000000000000000000000000000000000000000000000000145b92915050565b60008054604080516000805160206111408339815191528152600481018790529051869333936001 60a060020a0316926302571be39260248083019360209283900390910190829087803b15801561069057600080fd5b505af11580156106a4573d6000803e3d6000fd5b505050506040513d60208110156106ba57600080fd5b5051600160a060020a0316146106cf57600080fd5b6000848152600160209081526040918290209151855185936005019287929182918401908083835b602083106107165780518252601f199092019160209182019101610 6f7565b51815160209384036101000a6000190180199092169116179052920194855250604051938490038101909320845161075795919491909101925090506110a4565b50826040518082805190602001908083835b602083106107885780518252601f19909201916020918201910161 0769565b51815160209384036101000a60001901801990921691161790526040805192909401829003822081835289518383015289519096508a95507fd8c9334b1a9c2f9da342a0a2b32629c1a229b6445dad78947f674b44444a7550948a94508392908301919085019080838360005b8381101561080d5781810151838201526020016107f5565b50505050905090810190601f16801561083a57808203805160018360200361 01000a031916815260200191505b509250505060405180910390a3505050505 0565b60008281526001602052604090912060060905b83831161094c57828416158015906108 9b575060008381526006820160205260408120546002600019610100600184161502019091160411 5b1561094157600083815260068201602090815260409182902080548351601f600260001961010060018616150201909316929092049182018490048402810184019094528084529091830182828015610935578060 1f1061090a576101008083540402835291602001916109 35565b820191906000526020600020905b8154815290600101906020018083116109185782900 3601f1682

01915b50505050509150610951565b600290920291610862565b600092505b509250929050565b60008054604080516000805160206111408339815191528152600481018790529051869333936001 60a060020a0316926302571be39260248083019360209383900390910190829087803b1580156109b057600080fd5b505af11580156109c4573d6000803e3d6000fd5b505050506040513d60208110156109da57600080fd5b5051600160a060020a0316146109ef57600080fd5b604080518082018252848152602080820185815260008881526001835284902092516003840155516004909201919091558151858152908101849052815186927f1d6f5e03d3f63eb58751986629a5439baee5079ff04f345becb66e23eb154e46928290030190a250505050565b6000908152600160208190526040909120015490565b600090815260016020526040902054600160a060020a031690565b600082815260016020908152604091829020915183516060936005019285929182918401908083835b60208310610ad65780518252601f199092019160209182019101610ab7565b5181516000196020948503610100090810a820192831692199390931691909117909252949092019687526040805197889003820188208054601f6002600183161590980290950116959095049283018290048202880182019052818752929450925050830182828015610b8a5780601f10610b5f57610100808354040283529160200191610b8a565b820191906000526020600020905b815481529060010190602001808311610b6d57829003601f168201915b5050505050905092915050565b6000805460408051600080516020611140833981519152815260048101879052905186933393600160a060020a0316926302571be39260248083019360209383900390910190829087803b158015610bee57600080fd5b505af1158015610c02573d6000803e3d6000fd5b505050506040513d6020811015610c1857600080fd5b5051600160a060020a031614610c2d57600080fd5b6000918301831615610c3e57600080fd5b60008481526001602090815260408083208684526006018252909120835161 0c68928501906110a4565b50604051839085907faa121bbeef5f32f5961a2a28966e769023910fc9479059ee3495d4c1a696efe390600090a350505050565b6000818152600160208181526040928390206002908101805485516000199582161561010002959095011691909104601f8101839004830284018301909452838352606093909183018282801561 0d345780601f10610d0957610100808354040283529160200191610d34565b820191906000526020600020905b815481529060010190602001808311610d1757829003601f168201915b5050505050905091905056 5b6000805460408051600080516020611140833981519152815260048101869052905185933393600160a060020a0316926302571be39260248083019360209383900390910190829087803b158015610d9757600080fd5b505af1158015610dab573d6000803e3d6000fd5b505050506040513d6020811015610dc157600080fd5b5051600160a060020a031614610dd657600080fd5b600083815260016020908152604090912083516 10dfb92600290920191850190611 0a4565b5060408051602080825284518183015284518693 7fb7d29e911041e8d9b843369e890bcb72c9388692ba48b65ac54e7214c4c348f793879390928392830191850190808383600 05b83811015610e5b578181015183820152602001610e43565b50505050905090810190601f168015610e885780820380516001836020036101000a031916815260200191505b509250505060405180910390a2505050565b6000805460408051600080516020611140833981519152815260048101879052905185933393600160a060020a0316926302571be39260248083019360209383900390910190829087803b158015610ef157600080fd5b505af1158015610f05573d6000803e3d6000fd5b505050506040513d6020811015610f1b57600080fd5b5051600160a060020a031614610f3057600080fd5b60008381526001602081815260409283902090910184905581518481529151859 27f0424b6fe0d9c3bdbece0e7879dc241bb0c22e900be8b6c158b4ee08bd9bf83bc92908290030190a2505050565b6000908152600160205260409020600381015460049091015490915 65b60008054604080516000805160206111408339815191528152600481018690529051859333936001 60a060020a0316926302571be39260248083019360209383900390910190829087803b158015610ff357600080fd5b505af11580156110075 73d6000803e3d6000fd5b505050506040513d602081101561101d57600080fd5b5051600160a060020a03161461103257600080fd5b600083815260016020908152604091829020805473ffffffffffffffffffffffffffffffffffffffff191660016 0a060020a03861690811790915 58251908152915185927f52d7d861f09ab3d26239d492e8968629195e9e3f8cf0b73bfddc441522a15fd292908290030190a2505050565b828054600181600116156101000203166002900490600052602060002090601f016020900481019282601f106110e557805160ff1916838001178555611112565b82800160010185558215611112579182015b82811115611112578251825591602001919060010190 6110f7565b5061111e929150611122565b5090565b61113c91905b8082111561111e576000815560010161 1128565b90560002571be3000000000000000000000000000000000000000000000000000000000a165627a7a72305820c27de7e59fab60071f39ba74a6a8d7e8a5eac02905b0a26fee254f94ff3ae4b60029
00000000000a4d0a398161ffc163c503763b1f4360639393e0e4c8e300e0caec
000000000000034a7dedef4a161fa058a2d67a173a90155f3a2fe6fc132e0ebf
0f9188f13cb7b2c71f2a335e3a4fc328bf5eeb436012afca590b1a71466e2206

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。