南明离火
移动应用检测平台

ANDROID 静态分析报告

Pron • v71.47.4386

分析日期: 2025-04-07 20:24:47

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

应用概览

文件名称:	app.apk1691235934.6228013.apk
文件大小:	6.23MB
应用名称:	Pron
软件包名:	farmers.isolation.incentive
主活动:	farmers.isolation.qswkudkncjcyecgrnzbtmojgjmthedxjqrcdjcinmimejpmmkg2.jtmpkupcxhhwjdfnmdkmtptmcvnyavwhmhvpgabtmcyaynwc31
版本号:	71.47.43.86
最小SDK:	16
目标SDK:	29
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	48/100 (中风险)
杀软检测:	25 个杀毒软件报毒
MD5:	0c74870ed029787ce4279c82b44bd0b7
SHA1:	1421e4e640352d1c5df49ff1cc60bc1d0f21289a
SHA256:	6d9ab28a5e5b33b7dbcc35a5e9b2e6bb996aec2d9e0c9a389362331c76c31f8c

分析结果严重性分布

高危	中危	信息	安全	关注
2	24	1	1	0

四大组件导出状态统计

Activity组件：20个，其中export的有： 4个
Service组件：9个，其中export的有： 5个
Receiver组件：6个，其中export的有： 6个
Provider组件：1个，其中export的有： 0个

应用签名证书信息

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

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=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
签名算法: rsassa_pkcs1v15
有效期自: 2008-04-15 23:40:57+00:00
有效期至: 2035-09-01 23:40:57+00:00
发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
序列号: 0xf2b98e6123572c4e
哈希算法: md5
证书MD5: 1900bbfba756edd3419022576f3814ff
证书SHA1: b79df4a82e90b57ea76525ab7037ab238a42f5d3
证书SHA256: 465983f7791f2abeb43ea2cbdc7f21a8260b72bc08a55c839fc1a43bc741a81e
证书SHA512:
eb31650fdcd66705a93d6d8071cb6fd59d5390069a4e82f10d8329a306847aaf2bdad654a99221f6cd538866453de477ee608e19c6c8124c56f974c03e3ac8fe

公钥算法: rsa
密钥长度: 2048
指纹: c7751f41c1146e24eb638ea5795ec0b51e79e1489ef2586430b0e236ec2eaf6e
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.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.SET_WALLPAPER	普通	设置壁纸	允许应用程序设置壁纸。
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.READ_CALL_LOG	危险	读取通话记录	允许应用程序读取用户的通话记录
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.GET_ACCOUNTS	普通	探索已知账号	允许应用程序访问帐户服务中的帐户列表。
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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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粗略的经纬度信息，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.ACCESS_FINE_LOCATION	危险	获取精确位置	通过GPS芯片接收卫星的定位信息，定位精度达10米以内。恶意程序可以用它来确定您所在的位置。
android.permission.CALL_PHONE	危险	直接拨打电话	允许应用程序直接拨打电话。恶意程序会在用户未知的情况下拨打电话造成损失。但不被允许拨打紧急电话。
android.permission.DISABLE_KEYGUARD	危险	禁用键盘锁	允许应用程序停用键锁和任何关联的密码安全设置。例如，在手机上接听电话时停用键锁，在通话结束后重新启用键锁。

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

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.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.RECEIVE_BOOT_COMPLETED	普通	开机自启	允许应用程序在系统完成启动后即自行启动。这样会延长手机的启动时间，而且如果应用程序一直运行，会降低手机的整体速度。
android.permission.BIND_WALLPAPER	签名(系统)	绑定到壁纸	允许手机用户绑定到壁纸的顶级界面。应该从不需要将此权限授予普通应用程序。
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.BACKGROUND_ACTIVITY_STARTER	未知	未知权限	来自 android 引用的未知权限。
oppo.permission.OPPO_COMPONENT_SAFE	签名	特定于 OPPO 设备的权限	它用于授予应用访问某些系统级功能或组件的能力，否则这些功能或组件会因安全原因而受到限制。此权限可确保只有受信任的应用程序才能与 OPPO 系统的敏感部分进行交互。
com.huawei.permission.external_app_settings.USE_COMPONENT	签名	特定于华为设备的权限	它用于授予应用访问某些系统级功能或组件的能力，否则这些功能或组件会因安全原因而受到限制。该权限确保只有受信任的应用才能与华为系统的敏感部分进行交互。
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.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.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.WAKE_LOCK	危险	防止手机休眠	允许应用程序防止手机休眠，在手机屏幕关闭后后台进程仍然运行。
com.android.alarm.permission.SET_ALARM	未知	未知权限	来自 android 引用的未知权限。
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.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.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	普通	使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS 的权限	应用程序必须拥有权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
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。
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.REQUEST_DELETE_PACKAGES	普通	请求删除应用	允许应用程序请求删除包。
android.permission.USE_FULL_SCREEN_INTENT	普通	全屏通知	Android 10以后的全屏 Intent 的通知。

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

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	应用程序使用代码签名证书进行签名

Manifest 配置安全分析

高危: **1** | 警告: **18** | 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。
3	Activity (farmers.isolation.qswkudkncjcyecgrnzbtmojgjmthedxjqrcdjcinmimejpmmkg2.nydyjsemqcrmgqtooflwtifimvmxmvvjtcyhbpwyspczkniagn20) 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 (farmers.isolation.qswkudkncjcyecgrnzbtmojgjmthedxjqrcdjcinmimejpmmkg2.cnrryqahsetrnkpwagjmlxlmajjncsxfzyvbidzeebkjybe1...) 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 (farmers.isolation.qswkudkncjcyecgrnzbtmojgjmthedxjqrcdjcinmimejpmmkg2.nydyjsemqcrmgqtooflwtifimvmxmvvjtcyhbpwyspczkniagn20.install) 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 (farmers.isolation.qswkudkncjcyecgrnzbtmojgjmthedxjqrcdjcinmimejpmmkg2.installupdate) 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。

本报告由南明离火移动安全分析平台生成

7	Service (farmers.isolation.qswkudkncjcyecgrnzbtmojgjmthedxjqrcdjcinmimejpmmkg2.fpjlfhxoxlpldeyjrpskiolhetssvtokzkqmezxezfrmgpnbis5.ctmvneoouosfcqgxtpfnxqanecyizoohgymlcnnssrydgbzbcp7_WKJ) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
8	Broadcast Receiver (farmers.isolation.qswkudkncjcyecgrnzbtmojgjmthedxjqrcdjcinmimejpmmkg2.fpjlfhxoxlpldeyjrpskiolhetssvtokzkqmezxezfrmgpnbis5.SRctmvneoouosfcqgxtpfnxqanecyizoohgymlcnnssrydgbzbcp74B) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver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。
9	Service (farmers.isolation.qswkudkncjcyecgrnzbtmojgjmthedxjqrcdjcinmimejpmmkg2.ischgajqzikciykrinzcgkqngdcfvtygwxtdgikassczdkansr3.ctmvneoouosfcqgxtpfnxqanecyizoohgymlcnnssrydgbzbcp72) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_ACCESSIBILITY_SERVICE [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
10	Service (farmers.isolation.qswkudkncjcyecgrnzbtmojgjmthedxjqrcdjcinmimejpmmkg2.ischgajqzikciykrinzcgkqngdcfvtygwxtdgikassczdkansr3.Bworker) 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。
11	Broadcast Receiver (farmers.isolation.qswkudkncjcyecgrnzbtmojgjmthedxjqrcdjcinmimejpmmkg2.fpjlfhxoxlpldeyjrpskiolhetssvtokzkqmezxezfrmgpnbis5.ctmvneoouosfcqgxtpfnxqanecyizoohgymlcnnssrydgbzbcp7) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.RECEIVE_BOOT_COMPLETED [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。

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

12	Broadcast Receiver (farmers.isolation.qswkudkncjcyecgrnzbtmojgjmthedxjqrcdjcinmimejpmmkg2.fpjlfhxoxlpldeyjrpskiolhetssvtokzkqmezxezfrmgpnbis5.cnrryqjahsetrfokpwagjmlxlmajilqcsxfzjvbidzeebkjybe14_RC) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver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。
13	Activity (farmers.isolation.qswkudkncjcyecgrnzbtmojgjmthedxjqrcdjcinmimejpmmkg2.flyactiv) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance" ，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
14	Broadcast Receiver (farmers.isolation.qswkudkncjcyecgrnzbtmojgjmthedxjqrcdjcinmimejpmmkg2.fpjlfhxoxlpldeyjrpskiolhetssvtokzkqmezxezfrmgpnbis5.ctmvneoouosfcqgxtpfnxqanecyizoohgymlcnnssrydgbzbcp74) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver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。
15	Service (farmers.isolation.qswkudkncjcyecgrnzbtmojgjmthedxjqrcdjcinmimejpmmkg2.ithecbkyvgmyqdyouiuhikjhuulsyszidecxjdustacxwqhsnj27) 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。
16	Broadcast Receiver (farmers.isolation.qswkudkncjcyecgrnzbtmojgjmthedxjqrcdjcinmimejpmmkg2.fpjlfhxoxlpldeyjrpskiolhetssvtokzkqmezxezfrmgpnbis5.daterec) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver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。
17	Broadcast Receiver (farmers.isolation.qswkudkncjcyecgrnzbtmojgjmthedxjqrcdjcinmimejpmmkg2.fpjlfhxoxlpldeyjrpskiolhetssvtokzkqmezxezfrmgpnbis5.ctmvneoouosfcqgxtpfnxqanecyizoohgymlcnnssrydgbzbcp74_AR) 受权限保护，但应该检查权限的保护级别。 Permission: android.permission.BIND_DEVICE_ADMIN [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。

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

18	Service (farmers.isolation.qswkudkncjcyecgrnzbtmojgjmthedxjqrcdjcinmimejpmmkg2.ischgajqzikciykrinzcgkqngdcfvtygwxtdgikassczdkansr3.Swhdfrqdcgmoercvfmtomersojcwyaoeqjcxhgurahbskounora6IME) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_INPUT_METHOD [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
19	高优先级的Intent （999） -{2} 个命中 [android:priority]	警告	通过设置一个比另一个Intent更高的优先级，应用程序有效地覆盖了其他请求。

代码安全漏洞检测

高危: **1** | 警告: **5** | 信息: **1** | 安全: **0** | 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
3	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用已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
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	可能存在跨域漏洞。在 WebView 中启用从 URL 访问文件可能会泄漏文件系统中的敏感信息	警告	CWE: CWE-200: 信息泄露 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	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
本报告由南明离火移动安全分析平台生成

6	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
7	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

应用行为分析

编号	行为	标签	文件
00183	获取当前相机参数并更改设置	相机	升级会员：解锁高级权限
00162	创建 InetSocketAddress 对象并连接到它	socket	升级会员：解锁高级权限
00163	创建新的 Socket 并连接到它	socket	升级会员：解锁高级权限
00208	捕获设备屏幕的内容	信息收集 屏幕	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
00195	设置录制文件的输出路径	录制音视频 文件	升级会员：解锁高级权限
00199	停止录音并释放录音资源	录制音视频	升级会员：解锁高级权限
00198	初始化录音机并开始录音	录制音视频	升级会员：解锁高级权限
00194	设置音源（MIC）和录制文件格式	录制音视频	升级会员：解锁高级权限
00197	设置音频编码器并初始化录音机	录制音视频	升级会员：解锁高级权限
00007	Use absolute path of directory for the output media file path	文件	升级会员：解锁高级权限
00196	设置录制文件格式和输出路径	录制音视频 文件	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
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
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限
00075	获取设备的位置	信息收集 位置	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
本报告由南明离火移动安全分析平台生成

00115	获取设备的最后已知位置	信息收集 位置	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
00193	发送短信	短信	升级会员：解锁高级权限
00160	使用辅助服务执行通过视图 ID 获取节点信息的操作	无障碍服务	升级会员：解锁高级权限
00121	创建目录	文件 命令	升级会员：解锁高级权限
00004	获取文件名并将其放入 JSON 对象	文件 信息收集	升级会员：解锁高级权限
00159	使用辅助服务执行通过文本获取节点信息的操作	无障碍服务	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
00173	获取 AccessibilityNodeInfo 屏幕中的边界并执行操作	无障碍服务	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
00209	从最新渲染图像中获取像素	信息收集	升级会员：解锁高级权限
00210	将最新渲染图像中的像素复制到位图中	信息收集	升级会员：解锁高级权限
00023	从当前应用程序启动另一个应用程序	反射 控制	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
00079	隐藏当前应用程序的图标	规避	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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	16/30	android.permission.SEND_SMS android.permission.SET_WALLPAPER android.permission.READ_SMS android.permission.READ_CALL_LOG android.permission.READ_CONTACTS android.permission.GET_ACCOUNTS android.permission.CAMERA android.permission.RECORD_AUDIO android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.CALL_PHONE android.permission.RECEIVE_BOOT_COMPLETED android.permission.SYSTEM_ALERT_WINDOW android.permission.READ_PHONE_STATE android.permission.WAKE_LOCK android.permission.REQUEST_INSTALL_PACKAGES

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

其它常用权限	10/46	android.permission.FOREGROUND_SERVICE android.permission.READ_EXTERNAL_STORAGE android.permission.BIND_WALLPAPER android.permission.WRITE_EXTERNAL_STORAGE android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_WIFI_STATE android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS com.android.launcher.permission.INSTALL_SHORTCUT

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
porndude.p67z.com	安全	否	**IP地址:** 104.21.80.1 **国家:** 美国 **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

URL 链接安全分析

URL信息	源码文件
• http://porndude.p67z.com/	farmers/isolation/qswkudkncjcyecgrnzbtmojgjmthedxjqrcdjcinmimejpmmkg2/jtmpkupcxhhwjdfnmdllmtotdmcvnyavwhmhvpgabtmcyaynwc31.java

第三方 SDK 组件分析

SDK名称	开发者	描述信息
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。

敏感凭证泄露检测

可能的密钥
谷歌地图的=> "com.google.android.maps.v2.API_KEY" : "cnrryqjahsetrfokpwagjmlxlmajilqcsxfzjvbidzeebkjybe14"
"google_api_key" : "xOJSPronID"
"google_app_id" : "2:91Pron12"

本报告由南明离火移动安全分析平台生成

"google_crash_reporting_api_key" : "4JRPronA"
"appreciatedauthorizationa335" : "forumsktrbrxmdspxkwpzpyzpjahqoe336"
"llpprivatenthermalv471" : "conflictsfbrnnjrcfgwlimsubvkgnqpeh472"
"singpossessionf515" : "downloadsrlpqbqkqxfbmccopvamokwvfr516"
Swhdfrqdcgmoercvfmtomersojcwyaoeqjcxhgurahbskounora6IME
cnrryqjahsetrfokpwagjmlxlmajilqcsxfzjvbidzeebkjybe14
jiflfdsibmxbowycwttqqhplnrvjsnlgkbfmcxcapxwahtypml38con
nydyjsemqcrmgqtooflwtifimvmxmvvjtcyhbpwyspczkniagn20instll
jiflfdsibmxbowycwttqqhplnrvjsnlgkbfmcxcapxwahtypml38

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，深入剖析软件中中潜在的漏洞和安全隐隐患。

© 2025 南明离火 - 移动安全分析平台自动生成

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