



ANDROID 静态分析报告



📱 [晚晚]蚂蚁数藏抢购 v1.0.0

分析日期: 2025-04-04 04:22:03

i应用概览

文件名称:	[晚晚]蚂蚁数藏抢购 v1.0.0.apk
文件大小:	6.93MB
应用名称:	[晚晚]蚂蚁数藏抢购
软件包名:	ww.myscqg
主活动:	ww.myscqg.SplashActivity
版本号:	1.0.0
最小SDK:	21
目标SDK:	28
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:	14 个杀毒软件报毒
MD5:	60ec765361433a62497318ec5a88655e
SHA1:	d5a8b05b8c6ab020f14e34f1a06b0b3bbff0a6b
SHA256:	b70e86e41cee62ece6dd8c8b4a1fe6647891677c963028e90d5b308cd543dc9d

📊分析结果严重性分布

🔴 高危	🟡 中危	🟢 信息	✅ 安全	🔍 关注
2	16	3	1	0

📦四大组件导出状态统计

Activity组件: 9个, 其中export的有: 1个
Service组件: 2个, 其中export的有: 0个
Receiver组件: 2个, 其中export的有: 1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: True
v3 签名: True
v4 签名: False
主题: O=Auto.js Pro, CN=Default
签名算法: rsassa_pkcs1v15
有效期自: 2022-06-07 10:10:51+00:00
有效期至: 2049-07-27 10:10:51+00:00
发行人: O=Auto.js Pro, CN=Default
序列号: 0x6f231e86
哈希算法: sha1
证书MD5: 3a3269e3e05e2ac1655a216eb1405658
证书SHA1: 524c370ff61755e889f4e5d8712e1db9e621a1ab
证书SHA256: c138fd2f4c22ca4d7540db10ef51efb7193fc81680376a63478e2e3c80c1c362
证书SHA512:
4d95be47e966f8312b7cb69f3ac08b58e9b334e1f375a23372d9173cf0aebd3e376f7dcc4dfbcde0f70454c73a89325a32eb3d1c9e010409b9d4f786b369e40

公钥算法: rsa
密钥长度: 2048
指纹: ef3ad7b572b8e3df1e2d99fb41a092a2bb6c34b91140286489fce5f35bfec72d
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.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.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_EXTERNAL_STORAGE	危险	读取SD卡内容	允许应用程序从SD卡读取信息。
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.UNINSTALL_SHORTCUT	签名	删除快捷方式	这个权限是允许应用程序删除桌面快捷方式。
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.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.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。
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.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.WRITE_SECURE_SETTINGS	签名(系统)	修改安全系统设置	允许应用程序修改系统的安全设置数据。普通应用程序不能使用此权限。

android.permission.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设置方面的数据。恶意应用程序可借此破坏您的系统配置。
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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
com.android.alarm.permission.SET_ALARM	未知	未知权限	来自 android 引用的未知权限。
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.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.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。
android.permission.REQUEST_INSTALL_PACKAGES	危险	允许安装应用程序	Android 8.0 以上系统允许安装未知来源应用程序权限。
android.permission.QUERY_ALL_PACKAGES	普通	获取已安装应用程序列表	Android 11引入与包可见性相关的权限，允许查询设备上的任何普通应用程序，而不考虑清单声明。
android.permission.REQUEST_DELETE_PACKAGES	普通	请求删除应用	允许应用程序请求删除包。
moe.shizuku.manager.permission.API_V23	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: 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: 6 | 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	Activity设置了TaskAffinity属性 (www.myscgg.PgtyxthActivity)	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

3	Activity设置了TaskAffinity属性 (ww.myscqg.AefcliwActivity)	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
4	Broadcast Receiver (ww.myscqg.PlqbrkrjsReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。
5	Activity设置了TaskAffinity属性 (ww.myscqg.NsntgxeActivit y)	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
6	Activity (ww.myscqg.NsntgxeActivity) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity=”) 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本，在平台级别修复此问题。
7	Activity (ww.myscqg.NsntgxeActivity) 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。

代码安全漏洞检测

高危: 1 | 警告: 9 | 信息: 3 | 安全: 0 | 屏蔽: 0

序号	问题	等级	参考标准	文件位置
1	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
2	可能存在跨域漏洞。在Web view 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
3	应用程序记录日志信息,不禁止敏感信息	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
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	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
7	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
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	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
10	此应用侦听剪贴板更改。一些恶意软件也会监听剪贴板更改	信息	OWASP MASVS: MSTG-PLATFORM-4	升级会员：解锁高级权限
11	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
12	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

13	应用程序创建临时文件。敏感信息永远不应该被写入临时文件	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
----	-----------------------------	----	---	-----------------------------

应用行为分析

编号	行为	标签	文件
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
00013	读取文件并将其放入流中	文件	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
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
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
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限
00089	连接到 URL 并接收来自服务器的输入流	命令 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
00026	方法反射	反射	升级会员：解锁高级权限
00062	查询WiFi信息和WiFi Mac地址	WiFi 信息收集	升级会员：解锁高级权限
00130	获取当前WiFi信息	WiFi 信息收集	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
00083	查询IMEI号	信息收集 电话服务	升级会员：解锁高级权限
00056	修改语音音量	控制	升级会员：解锁高级权限
00082	获取当前WiFiMac地址	信息收集 WiFi	升级会员：解锁高级权限
00045	查询当前运行的应用程序名称	信息收集 反射	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
00161	对可访问性节点信息执行可访问性服务操作	无障碍服务	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

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
00025	监视要执行的一般操作	反射	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
00054	从文件安装其他APK	反射	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
00068	执行指定字符串的Linux命令	控制	升级会员：解锁高级权限
00024	Base64解码后写入文件	反射 文件	升级会员：解锁高级权限
00091	从广播中检索数据	信息收集	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
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
00028	从assets目录中读取文件	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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	9/30	android.permission.SYSTEM_ALERT_WINDOW android.permission.RECEIVE_BOOT_COMPLETED android.permission.WRITE_SETTINGS android.permission.ACCESS_FINE_LOCATION android.permission.RECORD_AUDIO android.permission.READ_PHONE_STATE android.permission.VIBRATE android.permission.WAKE_LOCK android.permission.REQUEST_INSTALL_PACKAGES
其它常用权限	8/46	android.permission.ACCESS_WIFI_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE com.android.launcher.permission.INSTALL_SHORTCUT android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS 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
javascript.crockford.com	安全	否	IP地址: 217.160.0.111 国家: 德国 地区: 北莱茵-威斯特法伦 城市: 斯特朗 纬度: 51.968700 经度: 8.753360 查看: Google 地图

🌐 URL 链接安全分析

URL信息	源码文件
https://www.jsdelivr.com/using-sri-with-dynamic-files	自研引擎-S
- https://github.com/grandcentrix/tray/issues - https://github.com/grandcentrix/tray/wiki/custom-authority	newgrandcentrix/tray/provider/TrayContract.java
- http://javascript.crockford.com/jsmin.html - https://github.com/then/promise - https://github.com/promises-aplus/promises-spec#the-promise-resolution-procedure	f/l.java
- https://github.com/vinc3m1 - https://github.com/vinc3m1/roundedimageview - https://github.com/vinc3m1/roundedimageview.git	自研引擎-S

📦 第三方 SDK 组件分析

SDK名称	开发者	描述信息
C++ 共享库	Android	在 Android 应用中运行原生代码。
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，高效的方法在应用程序启动时初始化组件。库开发人员 and 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。
Shizuku	RikkaW	Shizuku 可以帮助普通应用借助一个由 app_process 启动的 Java 进程直接以 adb 或 root 特权使用系统 API。

✉ 邮箱地址敏感信息提取

EMAIL	源码文件
events.min@360.js	com/stardust/widget/EventWebView.java

🔑 敏感凭证泄露检测

可能的密钥
"key_dont_show_main_activity" : "key_dont_show_main_activity"
"key_enable_accessibility_service_by_root" : "key_enable_accessibility_service_by_root"
"key_foreground_service" : "key_foreground_service"
"key_print_java_stack_trace" : "key_print_java_stack_trace"
"key_stable_mode" : "key_stable_mode"
"key_use_volume_control_running" : "key_use_volume_control_running"
"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"
"tray_authority" : "legacyTrayAuthority"
ec6702b12797ddcb8c715fb85028eef2
0a4fd5d5accf385b8d5f382d7abcfea7
904457d0ec9762027ffcb42f669a1d53
1e015d177062c6f5ccbc81db6a04c9b7
c5385f1454322b2bf60ff9ea87a863fa
4e58948ac5fd82f9e3c330825c609cec
15a24de203d02ad8e30da74b59d7d422
5ae9573c2ca4033f1e56f860a322a21e
a67f4aa372b5e45170790ed96481d439
6704a5f0e824369e2952c6417db87d66
2893767dcba7980a31f87ad7f785fb5
2a85805aeafee834a713627751dc324d
bf8d0efd614a29a7d621aa702ed487fd
bd576375c6d3e043ad851b4f97628185
eeaebc3522097e31e089b509da98e878
ac5fd82f9e3c330825c609cec
26d3cd86cf1a863343bb5b16920a59a2
3015bad3e9c15183579316d78ec15abf
0de7da6cd35bb1b99ca3ddc470ccb55e
15758fde5783ff46cbd780582f057dc5
61680806d85ffce775d32159ef368edf

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。

© 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