南明离火
移动应用检测平台

ANDROID 静态分析报告

Mini Militia 65 · v4.0.36

分析日期: 2025-06-20 20:59:27

应用概览

文件名称:	6bb12509c1deeae7831ea9ed27baa1c711869fdb16cb6e168d73a308035d249e v4_0_36_apk
文件大小:	33.04MB
应用名称:	Mini Militia 6B
软件包名:	com.app.somnacs.da2
主活动:	com.appsomniacs.da2.DA2Activity
版本号:	4.0.36
最小SDK:	11
目标SDK:	23
加固信息:	未加壳
开发框架:	Cocos2d-x (C++)
应用程序安全分数:	40/100 (中风险)
跟踪器检测:	16/432
杀软检测:	AI评估：可能有安全隐患
MD5:	ff58ba88595dff9675cfb33f04228814
SHA1:	473e7db9f5ad5b0e2f7f965e604537f1a8414c4
SHA256:	6bb12509c1deeae7831ea9ed27baa1c711869fdb16cb6e168d73a308035d249e

分析结果严重性分布

高危	中危	信息	安全	关注
8	17	1	2	0

四大组件导出状态统计

Activity组件：25个，其中export的有： 1个
Service组件：3个，其中export的有： 1个
Receiver组件：4个，其中export的有： 4个

Provider组件：2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: False
v3 签名: False
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: 2008-02-29 01:33:46+00:00
有效期至: 2035-07-17 01:33:46+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: 0x936eacbe07f201df
哈希算法: sha1
证书MD5: e89b158e4bcf988ebd09eb83f5378e87
证书SHA1: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81
证书SHA256: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
证书SHA512:
5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640f05581053abfea303977272d1f959704d89b7711292a4569

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.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_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.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。
com.google.android.gms.permission.ACTIVITY_RECOGNITION	危险	允许应用程序识别身体活动	允许应用程序识别身体活动。
android.permission.BLUETOOTH	危险	创建蓝牙连接	允许应用程序查看或创建蓝牙连接。
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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。

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.BLUETOOTH_ADMIN	危险	管理蓝牙	允许程序发现和配对新的蓝牙设备。
com.android.vending.BILLING	普通	应用程序具有应用内购买	允许应用程序从 Google Play 进行应用内购买。
com.android.vending.CHECK_LICENSE	未知	未知权限	来自 android 引用的未知权限。
com.google.android.c2dm.permission.RECEIVE	普通	接收推送通知	允许应用程序接收来自云的推送通知。
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。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.appsomniacs.da2.DA2Activity	Schemes: https://, doodlearmy2://, Hosts: www.appsomniacs.com, login, Path Prefixes: /games/doodlearmy2/app/login,
com.amazon.identity.auth.device.authorization.AuthorizationActivity	Schemes: amzn://, Hosts: com.appsomnacs.da2,

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: **1** | 警告: **0** | 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
应用程序容易受到 Janus 漏洞的影响	高危	应用程序使用 v1 签名方案进行签名，如果仅使用 v1 签名方案进行签名，则在 Android 5.0-8.0 上容易受到 Janus 漏洞的影响。在使用 v1 和 v2/v3 方案签名的 Android 5.0-7.0 上运行的应用程序也容易受到攻击。

Manifest 配置安全分析

高危: **2** | 警告: **6** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息

本报告由南明离火移动安全分析平台生成

1	Broadcast Receiver (com.inmobi.commons.core.utilities.uid.ImIdShareBroadCastReceiver) 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。
2	Broadcast Receiver (com.amazon.device.iap.ResponseReceiver) 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。
3	Activity (com.amazon.identity.auth.device.authorization.AuthorizationActivity) 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。
4	Activity （com.amazon.identity.auth.device.authorization.AuthorizationActivity） 容易受到 Android Task Hijacking/StrandHogg 的攻击。	高危	活动不应将启动模式属性设置为“singleTask”。 然后，其他应用程序可以将恶意活动放置在活动栈顶部，从而导致任务劫持/StrandHogg 1.0 漏洞。 这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”或设置空 taskAffinity (taskAffinity="") 属性来修复此漏洞。 您还可以将应用的目标 SDK 版本 (23) 更新到 28 或更高版本以在平台级别修复此问题。
5	Activity (com.amazon.identity.auth.device.authorization.AuthorizationActivity) 未被保护。存在一个intent-filter。	警告	发现 Activity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Activity是显式导出的。
6	Broadcast Receiver (com.amazon.identity.auth.device.authorization.PackageIntentReceiver) 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。
7	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) 受权限保护，但是应该检查权限的保护级别。Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [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 (io.openvpn.vpn_api.bcast_recv) 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。

代码安全漏洞检测

高危: **4** | 警告: **10** | 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	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	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
4	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
5	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
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	已启用远程WebView调试	高危	CWE: CWE-919: 移动应用程序中的弱点 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	升级会员：解锁高级权限

8	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
9	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
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	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
12	启用了调试配置。生产版本不能是可调试的	高危	CWE: CWE-919: 移动应用程序中的弱点 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	升级会员：解锁高级权限
13	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
14	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
15	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

16	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
17	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

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	armeabi-v7a/libjni_util.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。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程（ROP）攻击更难可靠地执行。	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	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	True info 符号被剥离
2	armeabi-v7a/libtcpvpn_svc_nopie.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。	No PIE high 共享库是在没有地址无关代码标志的情况下构建的。使用为了防止攻击者可靠地跳转到内存中被利用的特定函数，地址空间布局随机化（ASLR）随机排列进程关键数据区域的地址空间位置，包括可执行文件的基以及堆栈、堆和库的位置。使用编译器选项 -fPIC 启用位置无关代码。	False high 这个二进制文件没有在栈上添加栈哨兵值。栈哨兵是用于检测和防止攻击者覆盖返回地址的一种技术。使用选项-fstack-protector-all来启用栈哨兵。这对于Dart/Flutter库不适用，除非使用了 Dart FFI	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

3	armeabi-v7a/libtopvpn_svc_pie.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。	地址无关的可执行文件 (PIE) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 （ROP） 攻击更难可靠地执行。	False high 这个二进制文件没有在栈上添加栈哨兵值。栈哨兵是用于检测和防止攻击者覆盖返回地址的一种技术。使用选项-fstack-protector-all来启用栈哨兵。这对于Dart/Flutter库不适用，除非使用了 Dart FFI	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
4	armeabi-v7a/libcowind-crashlytics.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。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 （ROP） 攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它们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	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	True info 符号被剥离

应用行为分析

编号	行为	标签	文件
00064	监控来电状态	控制	升级会员：解锁高级权限
00034	查询当前数据网络类型	信息收集 网络	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
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
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
00016	获取设备的位置信息并将其放入 JSON 对象	位置 信息收集	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
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
00042	查询WiFi BSSID及扫描结果	信息收集 WiFi	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
00015	将缓冲流（数据）放入 JSON 对象	文件	升级会员：解锁高级权限
00014	将文件读入流并将其放入 JSON 对象中	文件	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
00009	将游标中的数据放入JSON对象	文件	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
00012	读取数据并放入缓冲流	文件	升级会员：解锁高级权限
00096	连接到 URL 并设置请求方法	命令 网络	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
00163	创建新的 Socket 并连接到它	socket	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
00078	获取网络运营商名称	信息收集 电话服务	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
00116	获取当前WiFi MAC地址并放入JSON中	WiFi 信息收集	升级会员：解锁高级权限
00076	获取当前WiFi信息并放入JSON中	信息收集 WiFi	升级会员：解锁高级权限
00082	获取当前WiFi MAC地址	信息收集 WiFi	升级会员：解锁高级权限
00137	获取设备的最后已知位置	位置 信息收集	升级会员：解锁高级权限
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
00052	删除内容 URI 指定的媒体（SMS、CALL_LOG、文件等）	短信	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
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
00153	通过 HTTP 发送二进制数据	http	升级会员：解锁高级权限
00065	获取SIM卡提供商的国家代码	信息收集	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
00108	从给定的 URL 读取输入流	网络 命令	升级会员：解锁高级权限
00072	将 HTTP 输入流写入文件	命令 网络 文件	升级会员：解锁高级权限
00123	连接到远程服务器后将响应保存为JSON	网络 命令	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
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
00134	获取当前WiFi IP地址	WiFi 信息收集	升级会员：解锁高级权限
00132	查询ISO国家代码	电话服务 信息收集	升级会员：解锁高级权限

00131	获取当前GSM的位置并将其放入JSON中	信息收集 位置	升级会员：解锁高级权限
00085	获取ISO国家代码并将其放入JSON中	信息收集 电话服务	升级会员：解锁高级权限
00099	获取当前GSM的位置并将其放入JSON中	信息收集 位置	升级会员：解锁高级权限
00147	获取当前位置的时间	信息收集 位置	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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	6/30	android.permission.READ_PHONE_STATE android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.RECORD_AUDIO android.permission.RECEIVE_BOOT_COMPLETED android.permission.WAKE_LOCK
其它常用权限	8/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.WRITE_EXTERNAL_STORAGE com.google.android.gms.permission.ACTIVITY_RECOGNITION android.permission.BLUETOOTH android.permission.BLUETOOTH_ADMIN com.google.android.c2dm.permission.RECEIVE

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
i.l.inmobicdn.net	安全	否	**IP地址:** 34.36.52.227 **国家:** 美国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图

analytics.mopub.com	安全	否	**IP地址:** 192.48.236.10 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.773968 **经度:** -122.410446 **查看:** Google 地图
outcome.supersonicads.com	安全	否	**IP地址:** 13.226.210.66 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
a.applovin.com	安全	否	**IP地址:** 34.110.179.88 **国家:** 美国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图
amazon-adsystem.com	安全	否	**IP地址:** 34.107.157.36 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
live.chartboost.com	安全	否	**IP地址:** 34.107.157.36 **国家:** 美国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图
ua.supersonicads.com	安全	否	**IP地址:** 99.84.203.40 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
www.inmobi.com	安全	否	**IP地址:** 104.244.42.193 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 华盛顿 **纬度:** 38.713848 **经度:** -78.159439 **查看:** Google 地图

d.applovin.com	安全	否	**IP地址:** 34.107.157.36 **国家:** 美国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图
track.atom-data.io	安全	否	No Geolocation information available.
www.vungle.com	安全	否	**IP地址:** 141.193.213.11 **国家:** 美国 **地区:** 得克萨斯州 **城市:** 奥斯丁 **纬度:** 30.271158 **经度:** -97.741699 **查看:** Google 地图
sdktm.w.inmobi.com	安全	否	**IP地址:** 172.212.5.164 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 华盛顿 **纬度:** 38.713848 **经度:** -78.159439 **查看:** Google 地图
api.vungle.com	安全	否	**IP地址:** 54.239.16.249 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
ags-ext.amazon.com	安全	否	**IP地址:** 54.239.16.249 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
twitter.com	安全	否	**IP地址:** 104.244.42.193 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.773968 **经度:** -122.410446 **查看:** Google 地图
www.amazon.com	安全	否	**IP地址:** 13.249.119.161 **国家:** 美国 **地区:** 佐治亚州 **城市:** 亚特兰大 **纬度:** 33.748795 **经度:** -84.387543 **查看:** Google 地图
lol.vungle.com	安全	否	No Geolocation information available.

appsomniacs.com	安全	否	**IP地址:** 54.239.16.249 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 帕萨迪纳 **纬度:** 34.152027 **经度:** -118.087570 **查看:** Google 地图
applab-sdk.amazon.com	安全	否	**IP地址:** 54.239.16.249 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
dock.inmobi.com	安全	否	No Geolocation information available.
androidads23.adcolony.com	安全	否	**IP地址:** 35.186.210.75 **国家:** 美国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图
z.moatads.com	安全	否	No Geolocation information available.
hola.org	安全	否	**IP地址:** 54.225.121.9 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
amazon-adsystem.amazon.com	安全	否	No Geolocation information available.
cortana-gateway.amazon.com	安全	否	**IP地址:** 52.46.132.93 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
vid.applovin.com	安全	否	**IP地址:** 34.160.64.118 **国家:** 美国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图

rt.applovin.com	安全	否	**IP地址:** 34.117.147.68 **国家:** 美国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图
ingest.vungle.com	安全	否	**IP地址:** 52.55.68.114 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
init.supersonicads.com	安全	否	**IP地址:** 18.65.25.3 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
mobilelogs.supersonic.com	安全	否	No Geolocation information available.
i.w.inmobi.com	安全	否	**IP地址:** 142.250.72.174 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 华盛顿 **纬度:** 38.713848 **经度:** -78.159439 **查看:** Google 地图
sdkm.w.inmobi.com	安全	否	**IP地址:** 142.250.72.174 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 华盛顿 **纬度:** 38.713848 **经度:** -78.159439 **查看:** Google 地图
clientsdk.luminati.io	安全	否	**IP地址:** 3.228.177.90 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
market.android.com	安全	否	**IP地址:** 142.250.72.174 **国家:** 美国 **地区:** 科罗拉多州 **城市:** 丹佛 **纬度:** 39.739361 **经度:** -104.983597 **查看:** Google 地图
www.supersonicads.com	安全	否	No Geolocation information available.

schemas.applovin.com	安全	否	No Geolocation information available.
config.inmobi.com	安全	否	**IP地址:** 52.46.132.93 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 华盛顿 **纬度:** 38.713848 **经度:** -78.159439 **查看:** Google 地图
support.newrelic.com	安全	否	**IP地址:** 173.222.162.161 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052370 **经度:** -118.243004 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• http://config.inmobi.com/config-server/v1/config/secure.cfg	com/inmobi/commons/core/configs/e.java
• https://www.supersonicads.com/mobile/sdk5/log?method=	com/supersonicads/sdk/controller/OpenUrlActivity.java
• https://vid.applovin.com/,https://pdn.applovin.com/,https://img.applovin.com/,https://d.applovin.com/,https://assets.applovin.com/,https://cdnjs.cloudflare.com/,http://vid.applovin.com/,http://pdn.applovin.com/,http://img.applovin.com/,http://d.applovin.com/,http://assets.applovin.com/,http://cdnjs.cloudflare.com/ • http://d.applovin.com/ • http://a.applovin.com/ • http://rt.applovin.com/pix	com/applovin/impl/sdk/cd.java
• javascript:handleoverlaydata	com/amazon/ags/html5/overlay/GameCircleUserInterface.java
• https://www.supersonicads.com/mobile/sdk5/log?method=injectjavascript	com/supersonicads/sdk/controller/SupersonicWebView$5.java
• javascript:handleoverlaydata	com/amazon/ags/html5/overlay/GameCircleAlertUserInterface.java
• https://www.supersonicads.com/mobile/sdk5/log?method=	com/supersonicads/sdk/utils/SupersonicSharedPrefHelper.java
• javascript:handlemessage	com/amazon/ags/html5/service/WebViewServiceHelper.java
• http://www.inmobi.com/products/sdk/#downloads	com/inmobi/commons/a/b.java
• https://www.supersonicads.com/mobile/sdk5/log?method=	com/supersonicads/sdk/utils/SupersonicStorageUtils.java

• http://amazon-adsystem.com	com/amazon/device/ads/WebViewFactory.java
• https://outcome.supersonicads.com/mediation/	com/supersonic/mediationsdk/events/OutcomeEventsFormatter.java
• https://www.supersonicads.com/mobile/sdk5/log?method=	com/supersonicads/sdk/agent/SupersonicAdsPublisherAgent.java
• https://mobilelogs.supersonic.com	com/supersonic/mediationsdk/logger/LogsSender.java
• https://track.atom-data.io	com/supersonic/mediationsdk/events/IronbeastEventsFormatter.java
• http://schemas.applovin.com/android/1.0	com/applovin/impl/adview/m.java
• https://ua.supersonicads.com/api/rest/v1.1/uniqueusers?	com/supersonic/mediationsdk/server/Server.java
• http://appsomniacs.com/home/terms	com/appsomniacs/da2/DA2Activity.java
• http://dock.inmobi.com/carb/v1/o • https://sdkm.w.inmobi.com/user/e.asm • http://dock.inmobi.com/carb/v1/i	com/inmobi/signals/p.java
• http://amazon-adsystem.amazon.com/	com/amazon/device/ads/AdController.java
• https://init.supersonicads.com/sdk/v	com/supersonic/mediationsdk/server/ServerURL.java
• javascript:chartboost.eventhandler.handleNativeEvent	com/chartboost/sdk/impl/bs.java
• https://androidads23.adcolony.com/configure	com/jirbo/adcolony/c.java
• https://applab-sdk.amazon.com/1.0	com/amazon/insights/delivery/ERSRequestBuilder.java
• https://applab-sdk.amazon.com/1.0	com/amazon/insights/abtest/DefaultABTestClient.java
• https://sdkm.w.inmobi.com/metrics/e.asm?v=1&	com/inmobi/commons/core/d/c.java
• http://www.amazon.com/gp/mas/get-appstore/android/ref=mas_mx_mba_iap_dl	com/amazon/device/iap/internal/b/b.java
• https://www.vungle.com/privacy/	com/vungle/publisher/ak.java
• https://analytics.mopub.com/i/jot/exchange_client_event	com/mopub/common/event/ScribeEventRecorder.java
• https://twitter.com/%s/status/%s	com/mopub/common/util/Intents.java
• https://z.moatads.com/	com/moat/analytics/mobile/inm/av.java

• https://z.moatads.com/	com/moat/analytics/mobile/inm/af.java
• javascript:%s.dispatchmany • https://z.moatads.com/'	com/moat/analytics/mobile/inm/ad.java
• file:///android_res/	com/chartboost/sdk/impl/as.java
• https://applab-sdk.amazon.com/1.0	com/amazon/insights/core/configuration/HttpCachingConfiguration.java
• http://support.newrelic.com	com/newrelic/agent/android/NewRelic.java
• https://ags-ext.amazon.com/service/gamedata/whisperdata	com/amazon/ags/client/whispersync/network/WhispersyncHttpClientImpl.java
• http://market.android.com/	com/chartboost/sdk/impl/ba.java
• https://www.supersonicads.com/mobile/sdk5/log?method=setwebviewsettings • https://www.supersonicads.com/mobile/sdk5/log?method=extraparameterstojson • https://www.supersonicads.com/mobile/sdk5/log?method=encodeappkey • https://www.supersonicads.com/mobile/sdk5/log?method= • https://www.supersonicads.com/mobile/sdk5/log?method=webviewresume • https://www.supersonicads.com/mobile/sdk5/log?method=webviewpause • https://www.supersonicads.com/mobile/sdk5/log?method=webviewloadblank • https://www.supersonicads.com/mobile/sdk5/log?method=noproductype • https://www.supersonicads.com/mobile/sdk5/log?method=webviewloadwithpath • https://www.supersonicads.com/mobile/sdk5/log?method=htmlcontrollerdoesnotexistonfilesystem • https://www.supersonicads.com/mobile/sdk5/log?method=encodeappuserid	com/supersonicads/sdk/controller/SupersonicWebView.java
• https://i.l.inmobicdn.net/sdk/sdk/500/android/mraid.js • http://i.w.inmobi.com/showad.asm • https://sdktm.w.inmobi.com/sdkpubreq	com/inmobi/ads/c.java
• https://cortana.gateway.amazon.com/cortana/gateway/getsigneddownloadurl	com/amazon/ags/client/whispersync/migration/MigrationHttpClient.java
• https://live.chartboost.com	com/chartboost/sdk/impl/az.java
• http://lol.vungle.com/	com/vungle/publisher/mv.java
• https://api.vungle.com/api/v4/ • https://ingest.vungle.com/	com/vungle/publisher/inject/EndpointModule.java
• 127.0.0.1	io/topvpn/vpn_api/be$worker.java
• http://hola.org/faq#intro-more	io/topvpn/vpn_api/peer_dialog$4.java
• http://hola.org/legal/sla	io/topvpn/vpn_api/peer_dialog.java

• https://clientsdk.luminati.io/setup_android.json?	io/topvpn/vpn_api/svc.java
• http://127.0.0.1:6880/	io/topvpn/vpn_api/util.java
• 54.197.246.90 • 198.211.96.91 • 54.243.159.121 • 162.243.24.21 • 66.85.186.228 • 192.81.209.23 • 104.236.38.205	io/topvpn/vpn_api/zajax.java

第三方 SDK 组件分析

SDK名称	开发者	描述信息
cocos2d-cpp	cocos2d-cpp	cocos2d-cpp 是用 C++ 14 编写的 2D 便携式游戏引擎，适用于 Android，iOS，Linux，MacOS 和 Windows。
Crashlytics	Google	Crashlytics 是 Firebase 的主要崩溃报告工具，将众多崩溃整理成一个方便管理的问题列表，从而缩短问题排查时间。在 Crashlytics 信息中心内查看问题对用户造成的影响，从而清楚合理地确定应当首先解决哪些问题。
Google Sign-In	Google	提供使用 Google 登录的 API。
Google Play Service	Google	借助 Google Play 服务，您的应用可以利用由 Google 提供的最新功能，例如地图，Google+ 等，并通过 Google Play 商店以 APK 的形式分发自动平台更新。 这样一来，您的用户可以更快地接收更新，并且可以更轻松地集成 Google 必须提供的最新信息。
Firebase	Google	Firebase 提供了分析、数据库、消息传递和崩溃报告等功能，可助您快速采取行动并专注于您的用户。
Google Analytics	Google	提供各种 API，可帮助您收集、配置和报告用户与您的在线内容进行互动的数据。

邮箱地址敏感信息提取

EMAIL	源码文件
publishers@cuebiq.com	com/cuebiq/cuebiqsdk/CuebiqSDKImpl.java
support@appsomniacs.com	com/amazon/iap/util/DA2IapManager.java
support@appsomniacs.com	com/appsomniacs/da2/DA2Activity.java
creative-review@mopub.com	com/mopub/mobileads/AdAlertReporter.java

第三方追踪器检测

名称	类别	网址

AdColony	Advertisement	https://reports.exodus-privacy.eu.org/trackers/90
Amazon Advertisement		https://reports.exodus-privacy.eu.org/trackers/92
Amazon Analytics (Amazon insights)	Analytics	https://reports.exodus-privacy.eu.org/trackers/95
AppLovin (MAX and SparkLabs)	Advertisement, Identification, Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/72
ChartBoost		https://reports.exodus-privacy.eu.org/trackers/53
Cuebiq	Location, Analytics	https://reports.exodus-privacy.eu.org/trackers/57
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105
Inmobi		https://reports.exodus-privacy.eu.org/trackers/106
Moat	Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/61
New Relic	Analytics	https://reports.exodus-privacy.eu.org/trackers/130
Supersonic Ads		https://reports.exodus-privacy.eu.org/trackers/110
Twitter MoPub	Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/35
Vungle	Advertisement	https://reports.exodus-privacy.eu.org/trackers/169

敏感凭证泄露检测

可能的密钥
凭证信息=> "com.google.android.gms.appstate.APP_ID" : "@string/app_id"
凭证信息=> "com.google.android.gms.games.APP_ID" : "@string/app_id"

凭证信息=> "io.fabric.ApiKey" : "8d7b56be8ad769d011fe03a6e51aa5d0382c53f0"
AppLovin广告SDK的=> "applovin.sdk.key" : "8W7iT2gSMRRUZsw0GfivTEgnz0TmGx9ORG6_JoRgDt9ok3p_kVuBkZzgZQRqLbDosJnA6DrK5_6p2vpmPgy7Ev"
"cuebiq_appkey" : "aAPSaps"
"app_id" : "351666831778"
22425945969293236512819607281747202268852113345956851069545419503178249900977203670147638322801582881051882957205768557918356441519366172126884608406316888515239296504501830280664879549133570276792155151832332847188532369002492210234010155186842709493620665119919750832332220777141369255943445578381285984064028865613478676828533273460580467686485184132743895959974709745438545286840895760124666752388237221644605602983168913347871459783870086411927320995518254863318224870023308580257590482785997100119659900506004545077959576775994398499163041304680055434779114516791088335562709611814859384126105309877333759273409 7
WszOzU7MTsgQW5kcm9pZC0xLmNvbSA7
04cd85b5d6f4422b83fbd5894e1b4ccf
389C9738-A761-44DE-8A66-1668CFD67DA1
55992150067220841518419707028278601511394651979781185292425911978043807792497354049312786480922685937183515922655386900862209824345619534785255424191774488876299813392684207215037954228104140316386276563822668688749798059093000955276040670726928689815089099832532589025210382801111166417447548711495769652615779093786937954600085450453371238028311033168218737171144699577236108423054506552958366535341910569552237227686862748056351625445328103571242304350679310783572604715134660857658308180796945836885301010496984356362957975093655177175638953857406222191591998031699221603211918289692804308799622409361028579777
470fa2b4ae81cd56ecbcda9735803434cec591fa
b1607fd0620f4213911cd6ba2bc44f16
599f2bef1acd76c77ae101213551529424c87e00
f69388d72eba447d89b2af7f98fd2d47
AA3f2ddc0c0c2fcb54d2484561ab0776a4ad7c718c
e920dac0641b4758a0b2d3e38c2a3448
161f45bad9264cc99d03eb2fad1acb21
iVBORw0KGgoAAAANSUhEUgAAAGAAAABgBAMAAAA2tmoLAAAAGFBMVEUAAAAzMzMzMzMzMzMzMzMzMzMzMzMzMzOW6p+xAAAACHRSTlMAmTkdj2BzYg1E16EAAAABtSURBVHhe7dExCgAwDAVRow0+RHatDbJDFsj+02SAQMIVqvyvFw9jDPL4yzkXNwQqISAxoqSEACNKkhYEdEHgODcDDBgw8N18AAAgSUqqHwg1HJoRE18cfz1ZESZMmFh8DWVE8lUaVdnwHXDOPfezMoezhMEMAAAAAElFTkSuQmCC
7a47d22d0552a4c94a49cbb29845cde4f
08f2b9c82c2643d38af52694bc6a166d
2ed112180a4e4d8f9b02a995d019740
7aab546884a7453cb756f8a55f4a1d49
9810efc33b5a4855b366a5976be60f40
3f2c1a504f6c4ab9b1fe24a119b05a55

4ce92cf6-7fae-49f9-8a16-bbf18991143e
d2728786e8244c2bacc592337ce0fe63
2e0b46f8d04a06ac187a2eb0429558fe
815fbd0e71604d529b39bac95a90433a
c4fb5977777f4fbcb10d22763c4257a7
AAfbeca5a9981874b750bc146f815eea5061fe838c
jqyngW96w5vk9a3gLSPP0srNdRpFkRi2+Fjl6qMoPrg=
C10F7968CFE2C76AC6F0650C877806D4514DE58FC239592D2385BCE5609A84B2A0FBDAF29B05505EAD1FDFEF3D7209ACBF34B5D0A806DF18147EA9C0337D6B5B
2fbee7e9bcc5474496fb292497a6e0a6
97e83c003bded24445aefd4c72dc4b85
Y29tLmFuZHJvaWQudmVuZGluZy5saWNlbnNpbmcuSUxpY2Vuc2luZ1NlcnZpY2U=
b69689323e219b1f98ce443d4ec4917a65c014b7
E72409364B865B757E1D6B8DB73011BBB1D20C1A9F931ADD3C4C09E2794CE101FAA7F2D50EB88F9880A576E6C7B0E95712CAE9416F7BACB798564627846E93B

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检测框架。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。