南明离火
移动应用检测平台

ANDROID 静态分析报告

全民灭僵尸 • v1.3.2

分析日期: 2024-02-28 15:22:45

应用概览

文件名称:	quanminmiejiangshi_itmop.com.apk
文件大小:	14.93MB
应用名称:	全民灭僵尸
软件包名:	com.appabc.island
主活动:	com.appabc.island.JapanZombie
版本号:	1.3.2
最小SDK:	8
目标SDK:	8
加固信息:	未加壳
应用程序安全分数:	40/100 (中风险)
跟踪器检测:	2/432
杀软检测:	25 个杀毒软件报毒
MD5:	3e5a0825178a9706b17f30863f73a9f5
SHA1:	203e03207906f3ebfab7106b73b53e1121b8199a
SHA256:	195065c2bbc8bdd148000d8cd88d210a247fd6cb6c03b4dbb6fbaa72c136b7d8

分析结果严重性分布

高危	中危	信息	安全	关注
4	8	1	0	4

四大组件导出状态统计

Activity组件：4个，其中export的有： 2个
Service组件：3个，其中export的有： 2个
Receiver组件：2个，其中export的有： 2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: 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:
5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea3039772720179587704d89b7711292a4569

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.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.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.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序装载和卸载可移动存储器的文件系统。
android.permission.ACCESS_COARSE_LOCATION	未知	未知权限	来自 android 引用的未知权限。
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.GET_TASKS	危险	检索当前运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。恶意应用程序可借此发现有关其他应用程序的保密信息。
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。
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错略的经纬度信息，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.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.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。

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	应用程序已使用代码签名证书进行签名
应用程序存在Janus漏洞	高危	应用程序使用了v1签名方案进行签名，如果只使用v1签名方案，那么它就容易受到安卓5.0-8.0上的Janus漏洞的攻击。在安卓5.0-7.0上运行的使用了v1签名方案的应用程序，以及同时使用了v2/v3签名方案的应用程序也同样存在漏洞。

Manifest 配置安全分析

高危: **1** | 警告: **10** | 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 2.2-2.2.3, [minSdk=8]	警告	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 (VideoActivity) 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。
4	Activity (cn.play.dserv.EmpActivity) is Vulnerable to StrandHogg 2.0	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 (8) 更新到 29 或更高版本以在平台级别修复此问题。
5	Activity (cn.play.dserv.EmpActivity) 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，因此使其对设备上的任何其他应用程序都可访问。
6	Broadcast Receiver (cn.play.dserv.DsReceiver) 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	Broadcast Receiver (com.appabc.island.NetWorkChangeBroadcastReceiver) 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。
8	Service (com.appabc.island.JapanService) 未被保护。 存在一个intent-filter。	警告	发现 Service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Service是显式导出的。
9	Service (com.baidu.location.f) 未被保护。 存在一个intent-filter。	警告	发现 Service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Service是显式导出的。
10	高优先级的Intent (1000) [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。
11	高优先级的Intent (1000) [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: **2** | 警告: **6** | 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	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
3	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
4	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
5	该文件是World Readable。任何应用程序都可以读取文件	高危	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	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
8	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
9	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

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/libdserv.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	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	armeabi/libegamepay.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	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/liblocSDK4d.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	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/libsmsiap.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	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

5	armeabi/libypiap.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	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

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.SEND_SMS android.permission.ACCESS_FINE_LOCATION android.permission.GET_TASKS android.permission.ACCESS_COARSE_LOCATION android.permission.CALL_PHONE
其它常用权限	4/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.WRITE_EXTERNAL_STORAGE

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
www.gamebox6.com	安全	否	No Geolocation information available.
da.mmarket.com	安全	是	**IP地址:** 120.232.188.83 **国家:** China **地区:** Guangdong **城市:** Guangzhou **纬度:** 23.127361 **经度:** 113.264252 **查看:** 高德地图

www.talkingdata.net	安全	是	**IP地址:** 116.196.122.26 **国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看:** 高德地图
dserv.cc6c.net	安全	否	**IP地址:** 173.224.214.155 **国家:** United States of America **地区:** California **城市:** Walnut **纬度:** 34.015400 **经度:** -117.858223 **查看:** Google 地图
tj.box6.com	安全	否	No Geolocation information available.
gaandroid.talkingdata.net	安全	是	**IP地址:** 116.198.14.107 **国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看:** 高德地图
open.play.cn	安全	是	**IP地址:** 180.96.49.16 **国家:** China **地区:** Jiangsu **城市:** Nanjing **纬度:** 32.061668 **经度:** 118.777779 **查看:** 高德地图
u.talkingdata.net	安全	否	No Geolocation information available.

URL 链接安全分析

URL信息	源码文件
• http://open.play.cn/api/v2/egame/log.json • http://open.play.cn/api/v2/egame/log/config.json?app_key=	cn/egame/terminal/sdk/log/s.java
• http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:feedback	com/chinaMobile/i.java
• http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:getappparameter&appkey= • 10.0.0.172 • http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:postactlog • http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:posterrlog • http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:posteventlog • http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:postsyslog	com/chinaMobile/MobileAgent.java
• http://tj.box6.com/Mobile/callback.aspx?Sign= • http://www.game.box6.com:8088/statistics/ststrackgameinstalllog.php?time= • http://www.game.box6.com:8088/getplatupdateinfo.php?time=	com/example/assetexam/LoginUser.java

• http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:getappparameter&appkey= • data:// • 211.151.121.43 • https://u.talkingdata.net/ota/b/android/dynamic/ver • http://open.play.cn/api/v2/egame/log.json • http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:feedback • https://u.talkingdata.net/ota/b/android/dynamic/sdk.zip • data://close • http://www.gamebox6.com:8088/getplatupdateinfo.php?time= • http://gaandroid.talkingdata.net/g/d?crc= • data://uri/ • http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:posteventlog • javascript:parseMessage(' • data://app • http://www.gamebox6.com:8088/statistics/stscrackgameinstalllog.php?time= • http://open.play.cn/api/v2/egame/log/config.json?app_key= • http://lba.baidu.com/ • http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:posterrlog • 10.0.0.200 • 10.0.0.172 • data://app/ • data://uri • www.talkingdata.net • http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:postsyslog • http://tj.box6.com/Mobile/callback.aspx?Sign= • http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:postactlog • http://10.10.32.105:9092/api/inappMsg/ • 3.0.0.53	自研引擎分析结果
• http://dserv.cc6c.net:8080/plserver/PS	lib/armeabi/libdserv.so

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。

第三方追踪器检测

名称	类别	网址
Baidu Location		https://reports.exodus-privacy.eu.org/trackers/97
TalkingData	Analytics, Advertisement	https://reports.exodus-privacy.eu.org/trackers/293

敏感凭证泄露检测

可能的密钥
2faaba4dc40738d0457235fe804e0f2c8
7243BD0B0[illegible]293BCAF3D9A83BF32D38D
134e3265829ff82daf16e7b740a600b5

308202eb30820254a00302010202044d36f7a4300d06092a864886f70d01010505003081b9310b3009060355040613023836311230100603550408130
94775616e67646f6e673111300f060355040713085368656e7a68656e31353033060355040a132c54656e63656e7420546563686e6f6c6f677928536865
6e7a68656e2920436f6d70616e79204c696d69746564313a3038060355040b133154656e63656e74204775616e677a686f752052657365617263682062
16e6420446576656c6f706d656e742043656e7465723110300e060355040313075465656e63656e74301e170d3131303131393134333933325a170d3431
303131313134333933325a3081b9310b3009060355040613023836311230100603550408130947756616e67646f6e673111300f060355040713085368686
56e7a68656e31353033060355040a132c54656e63656e7420546563686e6f6c6f6779285368656e7a68656e2920436f6d70616e79204c696d697465643
13a3038060355040b133154656e63656e74204775616e677a686f75205265736561726368206e6420446576656c6f706d656e742043656e746572311
0300e060355040313075465656e63656e7430819f300d06092a864886f70d010101050003818d0030818902818100c05f34b231b083fb1323670bfbe7bda
b40c0c0a6efc87ef2072a1ff0d60cc67c8edb0d0847f210bea6cbfaa241be70c86daf56be08b723c859e52428a064555d80db448cdcacc1aea2501eba06f8
bad12a4fa49d85cacd7abeb68945a5cb5e061629b52e3254c373550ee4e40cb7c8ae6f7a8151ccd8df582d446f39ae0c5e930203010001300d06092a864
886f70d01010505000381810009c8d9d7f2f908c42081b4c764c377109a8b2c70582422125ce545842d5f520aea69550b6bd8bfd94e987b75a3077eb04ad
341f481aac266e89d3864456e69fba13df018acdc168b9a19dfd7ad9d9cc6f6ace57c746515f71234df3a053e33ba93ece5cd0fc15f3e389a3f365588a9fcb
439e069d3629cd7732a13fff7b891499

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。

本报告由南明离火移动安全分析平台生成