南明离火
移动应用检测平台

ANDROID 静态分析报告

Word Cookies • v1.2.5

分析日期: 2025-04-15 14:39:08

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:	Word Cookies v1.2.5.apk
文件大小:	26.18MB
应用名称:	Word Cookies
软件包名:	com.bitmango.go.wordcookies
主活动:	com.bitmango.go.wordcookies.UnityPlayerActivity
版本号:	1.2.5
最小SDK:	15
目标SDK:	23
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	33/100 (高风险)
跟踪器检测:	14/432
杀软检测:	3 个杀毒软件报毒
MD5:	b8559fd83632cc98ee4605c90ded6210
SHA1:	b7533ddc9edb24eb9c24501403fad75f0820d5eb
SHA256:	37b50ccfc3d888b0c5b8c9a4fc0e706d62981476a4110e46275398c0197f7a56

分析结果严重性

高危	中危	信息	安全	关注
12	20	2	1	0

四大组件信息

Activity组件：29个，其中export的有： 3个
Service组件：4个，其中export的有： 2个
Receiver组件：7个，其中export的有： 4个
Provider组件：2个，其中export的有： 1个

证书信息

未报告由南明离火移动安全分析平台生成
未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: 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:
5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea303977272d17958704d89b7711292a4569

找到 1 个唯一证书

应用权限

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。
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。
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。
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。
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。
com.bitmango.go.wordcookies.permission.C2D_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
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。

网络通信安全

序号	范围	严重级别	描述

证书安全分析

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

本报告由南明离火移动安全分析平台生成

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分析

高危: **5** | 警告: **11** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	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。默认情况下已被设置为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。
2	Activity (com.bitmango.go.wordcookies.UnityPlayerActivity) 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。
3	Activity (com.bitmango.go.wordcookies.UnityPlayerActivity) 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。
4	Activity (com.facebook.unity.FBUnityAppLinkActivity) 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 (23) 更新到 29 或更高版本以在平台级别修复此问题。
5	Activity (com.facebook.unity.FBUnityAppLinkActivity) 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.facebook.unity.FBUnityDeepLinkingActivity) 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 (23) 更新到 29 或更高版本以在平台级别修复此问题。
7	Activity (com.facebook.unity.FBUnityDeepLinkingActivity) 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。
8	Content Provider (com.facebook.FacebookContentProvider) 未被保护。 [android:exported=true]	警告	发现 Content Provider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	Broadcast Receiver (com.kochava.android.tracker.lite.ReferralCapture) 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。

本报告由南明离火移动安全分析平台生成

10	Broadcast Receiver (com.bitmango.gcm.GCMBroadcastReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.google.android.c2dm.permission.SEND [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。
11	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.google.android.c2dm.permission.SEND [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。
12	Service (com.google.firebase.iid.FirebaseInstanceIdService) 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。
13	Broadcast Receiver (com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.INSTALL_PACKAGES [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。
14	Service (com.google.firebase.messaging.FirebaseMessagingService) 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。
15	Activity (com.facebook.CustomTabActivity) 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 (23) 更新到 29 或更高版本以在平台级别修复此问题。
16	Activity (com.facebook.CustomTabActivity) 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。

</> 安全漏洞检测

高危: **5** | 警告: **7** | 信息: **1** | 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

本报告由南明离火移动安全分析平台生成

2	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
3	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
4	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
5	该文件是World Writable。任何应用程序都可以写入文件	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	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
7	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
8	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
9	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

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

10	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
11	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
12	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
13	默认情况下，调用Cipher.getInstance("AES")将返回AES ECB模式。众所周知，ECB模式很弱，因为它导致相同明文块的密文相同	高危	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-2	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

动态库分析

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

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/libmain.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）攻击更难成功地执行。	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	No RELRO high 此共享对象未启用 RELRO。整个 GOT（.got 和 .got.plt）都是可写的。如果没有此编译器标志，全局变量上的缓冲区溢出可能会覆盖 GOT 条目。使用选项 -z relro,-z,now 启用完整 RELRO，仅使用 -z,relro 启用部分 RELRO。	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

行为分析

编号	行为	标签	文件
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

本报告由南明离火移动安全分析平台生成

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
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
00153	通过 HTTP 发送二进制数据	http	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
00013	读取文件并将其放入流中	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
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
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
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
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
00091	从广播中检索数据	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
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
00130	获取当前WIFI信息	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
00128	查询用户账户信息	信息收集 账号	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
00121	创建目录	文件 命令	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
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
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

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

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
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
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
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
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
00012	读取数据并放入缓冲流	文件	升级会员：解锁高级权限

敏感权限分析

类型	匹配	权限
恶意软件常用权限	2/30	android.permission.WAKE_LOCK android.permission.VIBRATE
其它常用权限	5/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE com.google.android.c2dm.permission.RECEIVE 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。

域名检测

域名	状态	中国境内	位置信息
config-alpha.yvolver.com	安全	否	No Geolocation information available.
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
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

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

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
market.android.com	安全	否	**IP地址:** 142.251.116.118 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 山景城 **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图
ingest.vungle.com	安全	否	**IP地址:** 52.3.170.51 **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
config-staging.yvolver.com	安全	否	No Geolocation information available.
d.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
schemas.applovin.com	安全	否	No Geolocation information available.
api.vungle.com	安全	否	**IP地址:** 34.196.191.95 **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
www.yvolver.com	安全	否	**IP地址:** 104.21.78.14 **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
adc3-launch.adcolony.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

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

word-cookies-54791714.firebaseio.com	安全	否	**IP地址:** 34.120.206.254 **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
a.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
lol.vungle.com	安全	否	No Geolocation information available.
www.vungle.com	安全	否	**IP地址:** 141.193.213.10 **国家:** 美国 **地区:** 得克萨斯州 **城市:** 奥斯丁 **纬度:** 30.271158 **经度:** -97.741619 **查看:** Google 地图
config-dev.yvolver.com	安全	否	No Geolocation information available.
config-prod.yvolver.com	安全	否	No Geolocation information available.
wd.adcolony.com	安全	否	**IP地址:** 130.211.8.42 **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
config-swap.yvolver.com	安全	否	No Geolocation information available.

URL链接分析

URL信息	源码文件
• http://jsonfx.net/ • http://javascript.crockford.com/jsmin.html • http://www.ascendercorp.com/typedesigners.html • http://scripts.sil.org/OFL • http://www.ascendercorp.com/	自研引擎-A
• https://config-alpha.yvolver.com/api/public/app/config • http://config-dev.yvolver.com/api/public/app/config • https://config-prod.yvolver.com/api/public/app/config • https://config-swap.yvolver.com/api/public/app/config • https://config-staging.yvolver.com/api/public/app/config	com/adcolony/sdk/bn.java
• javascript:nativebridge.resultforcallback	com/adcolony/sdk/cq.java
• file:///android_res/	com/chartboost/sdk/impl/as.java

本报告由南明离火移动安全分析平台生成

• 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/cb.java
• javascript:chartboost.eventhandler.handlenativeevent	com/chartboost/sdk/impl/bs.java
• https://live.chartboost.com	com/chartboost/sdk/impl/az.java
• https://adc3-launch.adcolony.com/v4/launch	com/adcolony/sdk/h.java
• javascript:nativebridge.resultforcallback • javascript:finishserverrewardtransaction • javascript:finishdigitalredemptiontransaction • http://www.yvolver.com • javascript:updatedigitalredemptionstatus • javascript:handlebackbutton	com/adcolony/sdk/bi.java
• http://market.android.com/	com/chartboost/sdk/impl/bla.java
• https://.facebook.com	com/adcolony/sdk/bg.java
• http://www.yvolver.com • javascript:finishdigitalredemptiontransaction	com/adcolony/sdk/ca.java
• http://schemas.applovin.com/android/1.0	com/applovin/adview/AppLovinAdView.java
• https://wd.adcolony.com/logs	com/adcolony/sdk/w.java
• https://www.vungle.com/privacy/	com/vungle/publisher/ak.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
• https://word-cookies-54791714.firebaseio.com	自研引擎-S

FIREBASE数据库分析

标题	严重程度	描述信息
应用与Firebase数据库通信	信息	该应用与位于 https://word-cookies-54791714.firebaseio.com 的 Firebase 数据库进行通信

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

Firebase远程配置已启用	警告	Firebase远程配置URL （https://firebaseremoteconfig.googleapis.com/v1/projects/694427261032/namespaces/firebase:fetch?key=AIzaSyBhYemRq-WIkKxtBRPbtfF08qn7m7AVFLs） 已启用。请确保这些配置不包含敏感信息。响应内容如下所示:
		
		{
		"entries": {
		"ActionEventConfigDataSet": "[\n {\n \"key\": \"AEO_PTIME_CV30\",\n \"cv30BoundaryValue\": 30\n },\n {\n \"key\": \"AEO_SESS_CV30\",\n \"cv30BoundaryValue\": 10\n },\n {\n \"key\": \"AEO_LEVEL_CV30\",\n \"cv30BoundaryValue\": 23\n },\n {\n \"key\": \"AEO_CONT_CV30\",\n \"cv30BoundaryValue\": 1\n },\n {\n \"key\": \"AEO_INADS_CV30\",\n \"cv30BoundaryValue\": 4\n },\n {\n \"key\": \"AEO_RVADS_CV30\",\n \"cv30BoundaryValue\": 1\n },\n {\n \"key\": \"AEO_PURCHASE_CV30\",\n \"cv30BoundaryValue\": 1\n },\n {\n \"key\": \"AEO_GETC_CV30\",\n \"cv30BoundaryValue\": 155\n },\n {\n \"key\": \"AEO_USEC_CV30\",\n \"cv30BoundaryValue\": 82\n }\n]",
		"churn": "",
		"cp_count": "8",
		"cp_order": "wordtiles->lollipoplinkmatch->blocktrianglepuzzletangram -> blockpuzzlestarfinder -> bubblepop -> bunnypopbubble -> rolltheballunrollme -> linepuzzlepipeart ",
		"give_welcome_back_present": "false",
		"store_popup_display_descending": "false",
		"version_suggestions": "[{ \"semanticVersion\": \"22.0316.00\", \"versionCode\": 181, \"updatePriority\": 5, \"message\": \"A new version of the game is available in the <color=#529C2C>Store </color>!\\n\\nPlease update to the <color=#529C2C>Latest Version </color> for the best experience.\" }]"
		},
		"state": "UPDATE",
		"templateVersion": "33"
		}

第三方SDK

SDK名称	开发者	描述信息
AdColony	AdColony	适用于 Android 的 AdColony 移动广告 SDK。
Google Play Games plugin for Unity	Google	使游戏开发人员能在使用 Unity® 编写的游戏中集成 Google Play Games API。
Audience Network SDK	Facebook	The Audience Network allows you to monetize your Android apps with Facebook ads. An interstitial ad is a full screen ad that you can show in your app. Typically interstitial ads are shown when there is a transition in your app. For example -- after finishing a level in a game or after loading a story in a news app.
Google Play Services	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。
Firebase Analytics	Google	Google Analytics（分析）是一款免费的应用衡量解决方案，可提供关于应用使用情况和用户互动度的分析数据。

追踪器

名称	类别	网址
AdColony	Advertisement	https://reports.exodus-privacy.eu.org/trackers/90

本报告由南明离火移动安全分析平台生成

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
Facebook Ads	Advertisement	https://reports.exodus-privacy.eu.org/trackers/65
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Flurry	Analytics, Advertisement	https://reports.exodus-privacy.eu.org/trackers/25
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
IAB Open Measurement	Advertisement, Identification	https://reports.exodus-privacy.eu.org/trackers/328
Kochava	Advertisement, Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/127
Vungle	Advertisement	https://reports.exodus-privacy.eu.org/trackers/169

密钥凭证

可能的密钥
凭证信息=> "io.fabric.ApiKey" : "de1753aa2790022b9280f90fc63bdcbb1236ccd6"
凭证信息=> "com.google.android.gms.games.APP_ID" : "\ 694427261032"
"google_api_key" : "AIzaSyBhYemRq-WIkKxt3RPbtfF08qn7m7AVFLs"
"google_app_id" : "1:694427261032:android:1f5f1fbde14e50d1"
"google_crash_reporting_api_key" : "AIzaSyBhYemRq-WIkKxt3RPbtfF08qn7m7AVFLs"
"firebase_database_url" : "https://word-cookies-54791714.firebaseio.com"
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
5e8f16062ea3cd2c4a0d547876baa6f38cabf625
a4b7452e2ed8f5f191058ca7bbfd26b0d3814bfc
026ae9c9824b3e483fa6c71fa8bf7ae27816141
3i2ndDfv2rTHiSisAbouNdArYfORhtTPEefj3q2f
470fa2b4ae81cd56ecbcda9735803434cec591fa
7bf3a1e7bd31e612eda3310c2cdb8075c43c6b5

GooglePlay应用信息

本报告由南明离火移动安全分析平台生成

标题: Word Cookies! ®

评分: 4.511837 **安装:** 50,000,000+ **价格:** 0 **Android版本支持:** **分类:** 文字 **Play Store URL:** com.bitmango.go.wordcookies

开发者信息: BitMango, 6249013288401661340, □□□ □□□ □□□ □□□□□645□□ 14, 3□ (□□□□ 13487), https://www.bitmango.com, contactus@bitmango.com,

发布日期: 2023年4月19日 **隐私政策:** Privacy link

关于此应用:

□?欢迎来到 Word Cookies！□? 潜入终极单词益智游戏，用单词饼干满足您对乐趣和挑战的渴望！无论您是单词连接游戏的粉丝还是喜欢单词搜索游戏，我们的游戏都提供令人愉快的谜题组合，旨在提高您的思维并扩大您的词汇量。立即下载并开始您的文字冒险！ 为什么你会喜欢 Word Cookies： 1. 引人入胜的游戏玩法：滑动并连接字母饼干以组成单词并解决令人兴奋的谜题。非常适合单词连接和单词搜索游戏的粉丝！ 2.超过 2000 个关卡：探索数千个具有挑战性的关卡，满足所有技能水平。每个谜题都会带来新的机会来测试您的解字能力。 3.每日奖励：每天玩游戏即可获得特殊奖金和奖励，让乐趣和脑力提升挑战接踵而至。 4.生活玩法：享受轻松的游戏体验，没有时间限制。按照自己的节奏解决谜题，花时间发现隐藏的单词。 5.提示和洗牌：卡在谜题上？使用提示或打乱字母来保持进度，让每个单词游戏会话都充满乐趣。 6.迷人的饼干主题：让自己沉浸在异想天开的饼干主题图形中，让每个级别都让您的眼睛和大脑得到享受。 7.离线模式：随时随地玩，即使没有互联网连接。非常适合快速休息或长途旅行！ 8.跨设备兼容性：在智能手机和平板电脑上享受无缝游戏，因此您最喜欢的单词益智游戏始终触手可及。 特点： 1. 多样的谜题：从简单的单词发现到复杂的挑战，单词饼干为单词连接和单词搜索游戏的粉丝提供了各种引人入胜的谜题。 2.家人和朋友：分享乐趣，挑战你的朋友和家人，打破你的高分。这是通过对文字的热爱建立联系的好方法！ 3.免费游戏：免费玩游戏，可选择应用内购买，以增强您的体验并移除广告。 立即下载 Word Cookies！开始你的单词冒险，享受最好的单词益智游戏之一，享受乐趣和脑力提升挑战的完美结合！ 联系我们：contactus@bitmango.com 隐私政策：https://www.bitmango.com/privacy-policy/ 在 Facebook 上关注我们：https://www.facebook.com/wordcookiesofficial 立即体验 Word Cookies 的乐趣和挑战！

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