Evaluation Warning: The document was created with Spire.Doc for Python.

**爆单商场（ 1.0版本）   
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。  
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | 爆单商场 |
| 版本 | 1.0 |
| 包名 | com.baodanshangcheng |
| 域名线索 | 16条 |
| URL线索 | 13条 |
| APP图标 |  |
| 分析日期 | 2025年6月21日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | 爆单商城[1].apk |
| 文件大小 | 3.31MB |
| MD5值 | 183215655e8d51905cbdc5e83222d900 |
| SHA1值 | bb7f4ba70b84ef22c21101c34ce24c257bfc95f3 |
| SHA256值 | 46f6d94137c8e395e90b755bf70aa09d043367d60814ff98f3ea68a784411cf6 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 爆单商场 |
| 包名 | com.baodanshangcheng |
| 主活动Activity | com.e4a.runtime.android.StartActivity |
| 安卓版本名称 | 1.0 |
| 安卓版本 | 0 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| alogsus.umeng.com | IP: 223.109.148.177  所属国家: China  地区: Jiangsu  城市: Nanjing |
| aspect-upush.umeng.com | IP: 223.109.148.176  所属国家: China  地区: Jiangsu  城市: Nanjing |
| resolve.umeng.com | IP: 223.109.148.179  所属国家: China  地区: Jiangsu  城市: Nanjing |
| www.123cha.com | IP: 180.108.106.103  所属国家: China  地区: Jiangsu  城市: Suzhou |
| ulogs.umengcloud.com | IP: 223.109.148.179  所属国家: China  地区: Jiangsu  城市: Nanjing |
| alogus.umeng.com | IP: 223.109.148.130  所属国家: China  地区: Jiangsu  城市: Nanjing |
| utoken.umeng.com | IP: 223.109.148.171  所属国家: China  地区: Jiangsu  城市: Nanjing |
| ucc.umeng.com | IP: 203.119.213.102  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| ulogs.umeng.com | IP: 223.109.148.176  所属国家: China  地区: Jiangsu  城市: Nanjing |
| schemas.android.com | 没有服务器地理信息. |
| bbs.e4asoft.compath | 没有服务器地理信息. |
| cnlogs.umeng.com | IP: 223.109.148.176  所属国家: China  地区: Jiangsu  城市: Nanjing |
| pslog.umeng.com | IP: 59.82.29.162  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| api.fanyi.baidu.com | IP: 110.242.68.186  所属国家: China  地区: Hebei  城市: Baoding |
| bbs.e4asoft.com | IP: 124.222.214.172  所属国家: China  地区: Beijing  城市: Beijing |
| developer.umeng.com | IP: 59.82.31.154  所属国家: China  地区: Zhejiang  城市: Hangzhou |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://bbs.e4asoft.com;path=/ | com/e4a/runtime/C0245.java |
| http://www.123cha.com/ | com/e4a/runtime/C0245.java |
| http://api.fanyi.baidu.com/api/trans/vip/translate?q= | com/e4a/runtime/C0245.java |
| http://bbs.e4asoft.com/openapi\_unsafe.php | com/e4a/runtime/MySQL.java |
| http://schemas.android.com/apk/res/android | com/e4a/runtime/components/impl/android/p002Tools\_PermissionTools/AndroidManifestParser.java |
| http://developer.umeng.com/docs/66650/cate/66650 | com/umeng/analytics/pro/l.java |
| https://aspect-upush.umeng.com/occa/v1/event/report | com/umeng/analytics/pro/aq.java |
| https://cnlogs.umeng.com/ext\_event | com/umeng/analytics/pro/aq.java |
| https://cnlogs.umeng.com/uapp\_ekverr\_logs | com/umeng/analytics/pro/aq.java |
| https://resolve.umeng.com/resolve | com/umeng/analytics/pro/by.java |
| https://ucc.umeng.com/v2/inn/fetch | com/umeng/analytics/pro/ar.java |
| https://developer.umeng.com/docs/66632/detail/ | com/umeng/commonsdk/debug/UMLogUtils.java |
| https://developer.umeng.com/docs/119267/detail/182050 | com/umeng/commonsdk/debug/UMLogCommon.java |
| https://developer.umeng.com/docs/119267/detail/118637 | com/umeng/commonsdk/debug/UMLogCommon.java |
| https://ulogs.umeng.com | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://alogus.umeng.com | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://alogsus.umeng.com | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://ulogs.umengcloud.com | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://pslog.umeng.com | com/umeng/commonsdk/vchannel/a.java |
| https://pslog.umeng.com/ | com/umeng/commonsdk/vchannel/a.java |
| https://ulogs.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://alogus.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://utoken.umeng.com | com/umeng/umzid/ZIDManager.java |

### **4.3 邮箱线索**

### **4.4 手机号线索**

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: False v3 签名: False 找到 1 个唯一证书 主题: C=, ST=, L=, O=, OU=, CN= 签名算法: rsassa\_pkcs1v15 有效期自: 2025-06-14 13:30:22+00:00 有效期至: 5023-06-18 13:30:22+00:00 发行人: C=, ST=, L=, O=, OU=, CN= 序列号: 0x7ab8d7f1 哈希算法: sha512 md5值: ef579647b3f01cb96f8813b4510fa821 sha1值: 35418924f6e207ee073e43f14f15b2acc58dd9d5 sha256值: 351c237857a8701c341b81d1002219ac19c7fae873eea1364c696777319fcac9 sha512值: 46accd906f95006b900bd8c557f0f8f0d833cec8e592ef7e822c2936fb8656ed909ce778efea630e47badde515a597c14a152219849f6c1f23a49b5572bf61ed**

## **6. 硬编码敏感信息**

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看 |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看 |  |  |

## **9. 此APP的危险动作**

| 向手机申请的权限 | 是否危险 | 类型 | 详细情况 |
| --- | --- | --- | --- |
| com.android.launcher.permission.READ\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.CHANGE\_CONFIGURATION | 系统需要 | 更改您的 UI 设置 | 允许应用程序更改当前配置,例如语言环境或整体字体大小 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.SYSTEM\_ALERT\_WINDOW | 危险 | 显示系统级警报 | 允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕 |
| android.permission.MOUNT\_UNMOUNT\_FILESYSTEMS | 危险 | 装载和卸载文件系统 | 允许应用程序为可移动存储安装和卸载文件系统 |
| 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.SYSTEM\_OVERLAY\_WINDOW | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.REQUEST\_INSTALL\_PACKAGES | 危险 | 允许应用程序请求安装包。 | 恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。 |
| android.permission.ACCESS\_FINE\_LOCATION | 危险 | 精细定位（GPS） | 访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量 |
| android.permission.ACCESS\_COARSE\_LOCATION | 危险 | 粗定位 | 访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置 |
| android.permission.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| android.permission.ACCESS\_NETWORK\_STATE | 正常 | 查看网络状态 | 允许应用程序查看所有网络的状态 |
| android.permission.GET\_TASKS | 危险 | 检索正在运行的应用程序 | 允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息 |
| android.permission.WAKE\_LOCK | 正常 | 防止手机睡眠 | 允许应用程序防止手机进入睡眠状态 |
| android.permission.ACCESS\_WIFI\_STATE | 正常 | 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\_EXTERNAL\_STORAGE | 危险 | 读取外部存储器内容 | 允许应用程序从外部存储读取 |
| android.permission.READ\_PHONE\_STATE | 危险 | 读取电话状态和身份 | 允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等 |
| com.android.launcher.permission.INSTALL\_SHORTCUT | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.MANAGE\_EXTERNAL\_STORAGE | 危险 | 允许应用程序广泛访问范围存储中的外部存储 | 允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用 |
| android.permission.QUERY\_ALL\_PACKAGES | 正常 |  | 允许查询设备上的任何普通应用程序,无论清单声明如何 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.CAMERA | 危险 | 拍照和录像 | 允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像 |
| android.permission.MODIFY\_AUDIO\_SETTINGS | 正常 | 更改您的音频设置 | 允许应用程序修改全局音频设置,例如音量和路由 |
| android.permission.READ\_AUDIO\_STATS | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

**报告由**  [**摸瓜APK反编译平台**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**