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

**Galaxy Empire（ 1.9.36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 | Galaxy Empire |
| 版本 | 1.9.36 |
| 包名 | com.tap4fun.ge |
| 域名线索 | 15条 |
| URL线索 | 9条 |
| APP图标 |  |
| 分析日期 | 2025年6月19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 | base.apk |
| 文件大小 | 47.19MB |
| MD5值 | 3d3bfa1bd77019ec6479685bbe897dc5 |
| SHA1值 | e3e5f7fa59bc804b553bdf9f703a8e79cd2d8118 |
| SHA256值 | cfea85feeb17bc5c1573dc9856e75b783a31b5e0d85f469a475917b58abaf4c6 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | Galaxy Empire |
| 包名 | com.tap4fun.ge |
| 主活动Activity | com.tap4fun.spartanwar.GameActivity |
| 安卓版本名称 | 1.9.36 |
| 安卓版本 | 3496 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| itunes.apple.com | IP: 116.196.129.226  所属国家: China  地区: Zhejiang  城市: Jinhua |
| push.gateway.tap4fun.com | IP: 47.251.114.208  所属国家: United States of America  地区: California  城市: Los Angeles |
| api.appsflyer.com | IP: 3.166.244.64  所属国家: United States of America  地区: Washington  城市: Seattle |
| oc.umeng.co | 没有服务器地理信息. |
| alog.umeng.com | IP: 223.109.148.176  所属国家: China  地区: Jiangsu  城市: Nanjing |
| support.google.com | IP: 142.250.217.110  所属国家: United States of America  地区: California  城市: Mountain View |
| track.appsflyer.com | IP: 18.65.216.28  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| graph.facebook.com | IP: 174.37.243.85  所属国家: United States of America  地区: District of Columbia  城市: Washington |
| tap4fun.helpshift.com | IP: 44.206.140.0  所属国家: United States of America  地区: Virginia  城市: Ashburn |
| oc.umeng.com | IP: 59.82.23.79  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| play.google.com | IP: 93.46.8.90  所属国家: Italy  地区: Lombardia  城市: Milan |
| data.flurry.com | 没有服务器地理信息. |
| alog.umeng.co | 没有服务器地理信息. |
| 6612.engine.mobileapptracking.com | IP: 3.173.197.101  所属国家: United States of America  地区: Washington  城市: Seattle |
| www.amazon.com | IP: 3.166.209.186  所属国家: United States of America  地区: Washington  城市: Seattle |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://www.amazon.com/gp/mas/get-appstore/android/ref=mas\_mx\_mba\_iap\_dl | com/amazon/device/iap/internal/b/b.java |
| https://track.appsflyer.com/api/v2.3/androidevent?buildnumber=1.7&app\_id= | com/appsflyer/AppsFlyerLib.java |
| https://api.appsflyer.com/install\_data/v3/ | com/appsflyer/AppsFlyerLib.java |
| http://data.flurry.com/aap.do | com/flurry/sdk/ew.java |
| https://data.flurry.com/aap.do | com/flurry/sdk/ew.java |
| http://%s | com/tap4fun/spartanwar/utils/network/ExtHttpConnection.java |
| http://play.google.com/store/apps/details? | com/tap4fun/spartanwar/utils/network/ExtHttpConnection.java |
| http://push.gateway.tap4fun.com | com/tap4fun/spartanwar/google/gcm/GCMUtils.java |
| http://push.gateway.tap4fun.com/gcm/register.json | com/tap4fun/spartanwar/google/gcm/GCMUtils.java |
| http://push.gateway.tap4fun.com/gcm/unregister.json | com/tap4fun/spartanwar/google/gcm/GCMUtils.java |
| http://alog.umeng.com/app\_logs | com/umeng/analytics/g.java |
| http://alog.umeng.co/app\_logs | com/umeng/analytics/g.java |
| http://oc.umeng.com/check\_config\_update | com/umeng/analytics/g.java |
| http://oc.umeng.co/check\_config\_update | com/umeng/analytics/g.java |
| http://support.google.com/googleplay/?hl=%lang%&dl=%region%&topic=1046718 | 摸瓜V1引擎 |
| api.appsflyer.com | 摸瓜V3引擎 |
| alog.umeng.com | 摸瓜V3引擎 |
| track.appsflyer.com | 摸瓜V3引擎 |
| graph.facebook.com | 摸瓜V3引擎 |
| tap4fun.helpshift.com | 摸瓜V3引擎 |
| data.flurry.com | 摸瓜V3引擎 |
| alog.umeng.co | 摸瓜V3引擎 |
| 6612.engine.mobileapptracking.com | 摸瓜V3引擎 |
| http://itunes.apple.com/en/app/galaxy-empire/id462506975?l=en&mt=8 | lib/armeabi-v7a/libgalaxyempire.so |
| https://itunes.apple.com/us/app/galaxy-empire-evolved/id824657976?ls=1&mt=8 | lib/armeabi-v7a/libgalaxyempire.so |

### **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: O=Tap4Fun, OU=Android Team, CN=GalaxyEmpire 签名算法: rsassa\_pkcs1v15 有效期自: 2012-07-20 11:02:50+00:00 有效期至: 2162-06-14 11:02:50+00:00 发行人: O=Tap4Fun, OU=Android Team, CN=GalaxyEmpire 序列号: 0x50093ada 哈希算法: sha1 md5值: b969d9dca60eceff99116b55ce135d4b sha1值: 32913b47829dbe197822a50561ac6ec77af8b6c5 sha256值: 145b54bcefd817198002edf21eaae7e96d8623f681802e6dfb387f15331e0dd0 sha512值: 03204ccff44603606f5aa925cafe2fd60c8c8de6696a73deb6ea66e5a18703ef40ac45843cad100f12e122328d2dd3e1a4602f96341cfaa6595efb44eccb2a57**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "flurry\_api\_key" : "84MJHPT2SCWGMZKBVQC4" |
| "tapjoy\_secret\_key\_evolved" : "y9gK9wxrdavINOlNE4gr" |
| "tapjoy\_secret\_key" : "iK8zGUsIfkK26AJIRvXy" |
| "mat\_conversion\_key" : "ac00fede56f4326b0f50780d31491513" |
| "umeng\_key" : "512dc5a45270155873000009" |
| "appsflyerkey" : "sFg5sWnDDyejXHN8ugzZMU" |

## **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 |
| --- | --- | --- | --- |
| 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.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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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 |
| 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.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 |
| com.android.vending.BILLING | 未知 | Unknown permission | Unknown permission from android reference |
| com.tap4fun.ge.permission.C2D\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.c2dm.permission.RECEIVE | 合法 | C2DM 权限 | 云到设备消息传递的权限 |
| 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.GET\_ACCOUNTS | 危险 | 列出帐户 | 允许访问账户服务中的账户列表 |

## **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。**