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

**3D大白鲨（ 1.0.5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 | 3D大白鲨 |
| 版本 | 1.0.5 |
| 包名 | com.safetest.shark |
| 域名线索 | 16条 |
| URL线索 | 18条 |
| APP图标 |  |
| 分析日期 | 2025年4月3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 | 02e112947aa19a577fd9d825531bd74797bbf5825a74e9918d4027bbd24bb49b.apk |
| 文件大小 | 10.68MB |
| MD5值 | 6c61f091cade306bc0706c5b86cfa769 |
| SHA1值 | c00e464bd4b7c43609667c9d046508045bba0a4e |
| SHA256值 | 02e112947aa19a577fd9d825531bd74797bbf5825a74e9918d4027bbd24bb49b |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 3D大白鲨 |
| 包名 | com.safetest.shark |
| 主活动Activity | com.safetest.shark.HungryShark |
| 安卓版本名称 | 1.0.5 |
| 安卓版本 | 6 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| proxy.youdraw.cn | IP: 104.21.57.40 所属国家: United States of America 地区: California 城市: San Francisco  |
| roa.myspace.com | IP: 34.111.176.156 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| staging.geocade.com | IP: 76.223.54.146 所属国家: United States of America 地区: Washington 城市: Seattle  |
| market.android.com | IP: 142.250.217.78 所属国家: United States of America 地区: California 城市: Mountain View  |
| apps.facebook.com | IP: 65.49.26.99 所属国家: United States of America 地区: Missouri 城市: Saint Louis  |
| www.scoreloop.com | IP: 209.74.67.18 所属国家: United States of America 地区: Minnesota 城市: Rogers  |
| media-router-flurry3.prod.media.wg1.b.yahoo.com | IP: 98.136.147.17 所属国家: United States of America 地区: New York 城市: New York City  |
| api.facebook.com | IP: 69.63.181.12 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| schemas.android.com | 没有服务器地理信息.  |
| data.flurry.com | IP: 69.147.80.15 所属国家: United States of America 地区: New York 城市: New York City  |
| maps.google.com | IP: 142.251.215.238 所属国家: United States of America 地区: California 城市: Mountain View  |
| www.facebook.com | IP: 31.13.84.34 所属国家: Austria 地区: Wien 城市: Vienna  |
| api.scoreloop.com | 没有服务器地理信息.  |
| gad.ju6666.com | IP: 38.55.63.20 所属国家: United States of America 地区: California 城市: Los Angeles  |
| www.adwo.com | IP: 49.232.84.161 所属国家: China 地区: Beijing 城市: Beijing  |
| r2.adwo.com | IP: 42.62.76.40 所属国家: China 地区: Beijing 城市: Beijing  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://gad.ju6666.com/adserver/android/2.0/GetAd  | com/ju6/c.java  |
| http://gad.ju6666.com/adserver/android/2.0/GetAd&  | com/ju6/c.java  |
| http://gad.ju6666.com/adserver/android/2.0/GetAd?  | com/ju6/c.java  |
| http://gad.ju6666.com/adserver/android/2.0/Re  | com/ju6/c.java  |
| https://api.scoreloop.com/bayeux  | com/scoreloop/client/android/core/model/Client.java  |
| https://roa.myspace.com/roa/09/messaging/login/  | com/scoreloop/client/android/core/ui/MySpaceAuthViewController.java  |
| https://roa.myspace.com/roa/09/messaging/login  | com/scoreloop/client/android/core/ui/c.java  |
| http://apps.facebook.com/scoreloop/scoreloop/sdk  | com/scoreloop/client/android/core/ui/FacebookAuthViewController.java  |
| https://api.scoreloop.com/bayeux/android/v2  | com/scoreloop/client/android/core/server/Server.java  |
| https://www.scoreloop.com/android/updates  | com/scoreloop/client/android/core/server/Server.java  |
| http://api.facebook.com/restserver.php  | com/a/a/g.java  |
| http://www.facebook.com/connect/prompt\_permissions.php  | com/a/a/o.java  |
| http://www.facebook.com/login.php  | com/a/a/l.java  |
| http://r2.adwo.com/ad  | com/adwo/adsdk/O.java  |
| http://www.adwo.com  | com/adwo/adsdk/AdwoAdBrowserActivity.java  |
| http://market.android.com  | com/adwo/adsdk/w.java  |
| https://market.android.com  | com/adwo/adsdk/w.java  |
| http://maps.google.com/maps?q=  | com/adwo/adsdk/C0007g.java  |
| http://schemas.android.com/apk/res/com.atools.battery  | com/adwo/adsdk/AdwoAdView.java  |
| http://data.flurry.com/aar.do  | com/flurry/android/FlurryAgent.java  |
| https://data.flurry.com/aar.do  | com/flurry/android/FlurryAgent.java  |
| http://staging.geocade.com/scores/submitScore  | com/slg/j2me/game/HiscoreTable.java  |
| http://proxy.youdraw.cn/api/proxy  | defpackage/n.java  |
| data.flurry.com  | 摸瓜V3引擎  |
| media-router-flurry3.prod.media.wg1.b.yahoo.com  | 摸瓜V3引擎  |

### **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=US, OU=Google Inc. 签名算法: rsassa\_pkcs1v15 有效期自: 2011-05-04 03:31:13+00:00 有效期至: 2110-04-10 03:31:13+00:00 发行人: C=US, OU=Google Inc. 序列号: 0x4dc0c881 哈希算法: sha1 md5值: e5f287c2c568278d3ec52dee3593d6c2 sha1值: 473da98f656202ce4f62b221bd36a58a6f93986d sha256值: f090c58c4b3679cb1d9a972ff068c3776d7055053d9f6dfa2934b3dc227f20d6 sha512值: d39a37eea1e7483fb492a5348231c7a970058b1953384d0110949424a5b020e3fca2125b404ac974fd9d9dbd3b0d55911184de5c24f8bb32ecbb50dd85bf8834**

## **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 |
| --- | --- | --- | --- |
| 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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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\_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.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\_SMS | 危险 | 阅读短信或彩信 | 允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息 |
| android.permission.WRITE\_SMS | 危险 | 编辑短信或彩信 | 允许应用程序写入存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会删除您的消息 |

## **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。**