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

**赏帮赚（ 5.2.6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 | 赏帮赚 |
| 版本 | 5.2.6 |
| 包名 | com.sbzapp.sbz |
| 域名线索 | 21条 |
| URL线索 | 7条 |
| APP图标 |  |
| 分析日期 | 2025年6月28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 | 110\_e8592039da851ffc2fb5a08ca99d7aab.apk |
| 文件大小 | 6.07MB |
| MD5值 | 799b21bc8338cd2ba77d17edb05a13b6 |
| SHA1值 | 666aab13a1cf6f7163f7ec289ae2c4797b3594a8 |
| SHA256值 | 351bfb4603b732e74155cff9802c5765746a17af658d0702f384f694b3cf7a69 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 赏帮赚 |
| 包名 | com.sbzapp.sbz |
| 主活动Activity | com.lt.app.MainActivity |
| 安卓版本名称 | 5.2.6 |
| 安卓版本 | 526 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| play.google.com | IP: 8.7.198.46 所属国家: United States of America 地区: Louisiana 城市: Monroe  |
| data-dra.push.dbankcloud.com | IP: 119.8.163.189 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| store.hispace.hicloud.com | IP: 123.249.62.130 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| grs.dbankcloud.asia | IP: 49.4.35.251 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| store-drru.hispace.hicloud.com | IP: 159.138.201.153 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| metrics2.data.hicloud.com | IP: 80.158.38.48 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| metrics5.data.hicloud.com | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| store1.hispace.hicloud.com | IP: 123.249.62.130 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| connectivitycheck.gstatic.com | IP: 203.208.50.98 所属国家: China 地区: Beijing 城市: Beijing  |
| metrics-dra.dt.hicloud.com | IP: 94.74.88.100 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| store3.hispace.hicloud.com | IP: 23.210.26.28 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| grs.dbankcloud.cn | IP: 49.4.40.185 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| grs.dbankcloud.eu | 没有服务器地理信息.  |
| data-dre.push.dbankcloud.com | IP: 80.158.49.244 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| store-at-dre.hispace.dbankcloud.com | 没有服务器地理信息.  |
| appgallery.cloud.huawei.com | IP: 121.36.118.136 所属国家: China 地区: Beijing 城市: Beijing  |
| data-drcn.push.dbankcloud.com | IP: 121.36.117.8 所属国家: China 地区: Beijing 城市: Beijing  |
| data-drru.push.dbankcloud.com | IP: 159.138.202.31 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| store2.hispace.hicloud.com | IP: 3.166.228.36 所属国家: United States of America 地区: Washington 城市: Seattle  |
| metrics1.data.hicloud.com | IP: 111.202.16.252 所属国家: China 地区: Beijing 城市: Beijing  |
| grs.dbankcloud.com | IP: 60.28.200.159 所属国家: China 地区: Tianjin 城市: Tianjin  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://play.google.com/store/apps/details?id=  | 摸瓜V1引擎  |
| https://appgallery.cloud.huawei.com  | 摸瓜V1引擎  |
| https://store.hispace.hicloud.com/hwmarket/api/  | 摸瓜V1引擎  |
| https://store-at-dre.hispace.dbankcloud.com/hwmarket/api/  | 摸瓜V2引擎  |
| https://data-drcn.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-dra.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-dre.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-drru.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://metrics1.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics-dra.dt.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics2.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics5.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://store1.hispace.hicloud.com/hwmarket/api/  | 摸瓜V2引擎  |
| https://store2.hispace.hicloud.com/hwmarket/api/  | 摸瓜V2引擎  |
| https://store3.hispace.hicloud.com/hwmarket/api/  | 摸瓜V2引擎  |
| https://store-drru.hispace.hicloud.com/hwmarket/api/  | 摸瓜V2引擎  |
| https://grs.dbankcloud.com  | 摸瓜V2引擎  |
| https://grs.dbankcloud.cn  | 摸瓜V2引擎  |
| https://grs.dbankcloud.eu  | 摸瓜V2引擎  |
| https://grs.dbankcloud.asia  | 摸瓜V2引擎  |
| android.googleapis.com  | 摸瓜V3引擎  |
| connectivitycheck.gstatic.com  | 摸瓜V3引擎  |
| infinitedata-pa.googleapis.com  | 摸瓜V3引擎  |
| www.googleapis.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: True v3 签名: False 找到 1 个唯一证书 主题: C=(zh), ST=(Beijing), L=(Beijing), O=(191184182@qq.com), OU=(191184182@qq.com), CN=(b191184182) 签名算法: rsassa\_pkcs1v15 有效期自: 2021-09-28 12:35:15+00:00 有效期至: 2121-09-04 12:35:15+00:00 发行人: C=(zh), ST=(Beijing), L=(Beijing), O=(191184182@qq.com), OU=(191184182@qq.com), CN=(b191184182) 序列号: 0x625f9a67 哈希算法: sha256 md5值: 606fdf9f44cd13e871f179780c746321 sha1值: 7e6afae55126ace0b9bfcc0d8cdd756bd12d385a sha256值: 0d24e73aaaa5cb360518485cea3c419fe0c2bcba055cfb1a7a7a8df3abf21a99 sha512值: 1665471770cceb5be48c909c90d791a5d9fcaff7767485ee5d8d51645d72497fd6381622bc7aa7fe0d922254aad5405fd916a9dd64342e445806a8928b288871 公钥算法: rsa 密钥长度: 1024 指纹: 76579425c720215d63a1f1d08dbe676a035d13bcfcf951de027f99e2b60fd96e**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "p\_ht\_appkey" : "700032473"  |
| "p\_ht\_mz\_appkey" : ""  |
| "p\_ht\_op\_appkey" : ""  |
| "p\_ht\_op\_appsecret" : ""  |
| "p\_ht\_vv\_appkey" : ""  |
| "p\_ht\_xm\_appkey" : ""  |
| "p\_rcpush\_mzAppKey" : ""  |
| "p\_rcpush\_opAppKey" : ""  |
| "p\_rcpush\_opAppSecret" : ""  |
| "p\_rcpush\_vvAppKey" : ""  |
| "p\_rcpush\_xmAppKey" : ""  |
| "p\_weibo\_appkey" : ""  |

## **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.RECEIVE\_USER\_PRESENT | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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.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 |
| com.huawei.android.launcher.permission.CHANGE\_BADGE | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章。 |
| com.sbzapp.sbz.permission.MIPUSH\_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.meizu.flyme.push.permission.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.sbzapp.sbz.push.permission.MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.meizu.c2dm.permission.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.sbzapp.sbz.permission.C2D\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.coloros.mcs.permission.RECIEVE\_MCS\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |
| com.sbzapp.sbz.permission.techain.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.sbzapp.sbz.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| com.sbzapp.sbz.permission.PUSH\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| com.huawei.appmarket.service.commondata.permission.GET\_COMMON\_DATA | 未知 | Unknown permission | Unknown permission from android reference |
| com.meizu.flyme.permission.PUSH | 未知 | Unknown permission | Unknown permission from android reference |
| com.sbzapp.sbz.permission.YM\_APP | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.lt.app.JumpActivity | **Schemes**: ltapp288446://,  |
| com.baidu.techain.push.VivoPushActivity | **Schemes**: vpushscheme://, **Hosts:** com.sbzapp.sbz, **Paths:** /detail,  |

**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。**