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

**福袋宝藏（ 1.90.66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 | 福袋宝藏 |
| 版本 | 1.90.66 |
| 包名 | com.overhead.laser.liquor |
| 域名线索 | 32条 |
| URL线索 | 48条 |
| APP图标 |  |
| 分析日期 | 2024年9月17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 | 100207582.apk |
| 文件大小 | 21.75MB |
| MD5值 | fefe4a05f92f34c289b3a0ff9c5bc338 |
| SHA1值 | 98b309ac42aea3231d5669ab8331d0c6c1143245 |
| SHA256值 | 85d7ada7848350d4851aeaf6e5855762c25136d35ef39d0afe4c12d61ba6e7db |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 福袋宝藏 |
| 包名 | com.overhead.laser.liquor |
| 主活动Activity | com.app.pancake.ui.SplashActivity |
| 安卓版本名称 | 1.90.66 |
| 安卓版本 | 19066 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| open.e.kuaishou.com | IP: 116.136.162.35  所属国家: China  地区: Nei Mongol  城市: Hohhot |
| utoken.umeng.com | IP: 223.109.148.139  所属国家: China  地区: Jiangsu  城市: Nanjing |
| mores.toponad.com | IP: 123.126.74.194  所属国家: China  地区: Beijing  城市: Beijing |
| schemas.android.com | 没有服务器地理信息. |
| open.weixin.qq.com | IP: 220.196.154.28  所属国家: China  地区: Jiangsu  城市: Wuxi |
| i.snssdk.com | IP: 120.52.77.207  所属国家: China  地区: Hebei  城市: Langfang |
| pitk.birdgesdk.com | IP: 39.108.103.199  所属国家: China  地区: Guangdong  城市: Shenzhen |
| style-browse-openapi.test.gifshow.com | IP: 103.102.202.41  所属国家: China  地区: Beijing  城市: Beijing |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| errlog.umeng.com | IP: 223.109.148.180  所属国家: China  地区: Jiangsu  城市: Nanjing |
| apps.bytesfield.com | IP: 116.136.187.92  所属国家: China  地区: Nei Mongol  城市: Hohhot |
| px-intl.ucweb.com | IP: 157.185.188.1  所属国家: Canada  地区: Ontario  城市: North York |
| errlogos.umeng.com | IP: 47.246.110.96  所属国家: Singapore  地区: Singapore  城市: Singapore |
| pslog.umeng.com | IP: 59.82.60.44  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| alogus.umeng.com | IP: 223.109.148.130  所属国家: China  地区: Jiangsu  城市: Nanjing |
| apps.bytesfield-b.com | IP: 116.136.187.93  所属国家: China  地区: Nei Mongol  城市: Hohhot |
| apps.samsung.com | IP: 124.134.127.227  所属国家: China  地区: Shandong  城市: Jinan |
| apps.oceanengine.com | IP: 116.136.187.93  所属国家: China  地区: Nei Mongol  城市: Hohhot |
| ulogs.umengcloud.com | IP: 223.109.148.179  所属国家: China  地区: Jiangsu  城市: Nanjing |
| ulogs.umeng.com | IP: 223.109.148.176  所属国家: China  地区: Jiangsu  城市: Nanjing |
| px.ucweb.com | IP: 116.132.217.40  所属国家: China  地区: Hebei  城市: Shijiazhuang |
| developer.umeng.com | IP: 59.82.60.43  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| www.samsungapps.com | IP: 54.229.93.185  所属国家: Ireland  地区: Dublin  城市: Dublin |
| p1-lm.adkwai.com | IP: 218.12.71.55  所属国家: China  地区: Hebei  城市: Shijiazhuang |
| plbslog.umeng.com | IP: 36.156.202.75  所属国家: China  地区: Jiangsu  城市: Yangzhou |
| play.google.com | IP: 172.217.163.46  所属国家: United States of America  地区: California  城市: Mountain View |
| alogsus.umeng.com | IP: 223.109.148.130  所属国家: China  地区: Jiangsu  城市: Nanjing |
| xmlpull.org | IP: 185.199.109.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| aa.birdgesdk.com | IP: 120.78.94.142  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| long.open.weixin.qq.com | IP: 112.65.193.170  所属国家: China  地区: Shanghai  城市: Shanghai |
| static.yximgs.com | IP: 101.73.101.237  所属国家: China  地区: Hebei  城市: Shijiazhuang |
| sf6-ttcdn-tos.pstatp.com | IP: 121.17.252.117  所属国家: China  地区: Hebei  城市: Hengshui |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://mores.toponad.com/image/default/bg2\_vertical\_720x1280.jpg | com/anythink/basead/i/d.java |
| https://mores.toponad.com/image/default/bg1\_horizontal\_1280x720.jpg | com/anythink/basead/i/d.java |
| http://xmlpull.org/v1/doc/features.html | com/anythink/basead/i/b/b.java |
| https://play.google.com | com/anythink/basead/mraid/MraidBaseWebView.java |
| https://play.google.com/store/apps/details?id= | com/anythink/core/basead/a/c.java |
| https:///gdpr/PrivacyPolicySetting.html | com/anythink/core/common/h.java |
| https:///hostsetting/dmlist/index.html | com/anythink/core/common/f/a.java |
| https:///hostsetting/mumbai/index.html | com/anythink/core/common/f/a.java |
| https:///gdpr/PrivacyPolicySetting.html | com/anythink/core/common/f/a.java |
| https://adx | com/anythink/core/common/f/a.java |
| https:///hostsetting/mumbai/index.html | com/anythink/core/common/f/c.java |
| https:///hostsetting/dmlist/index.html | com/anythink/core/common/f/c.java |
| https:///gdpr/PrivacyPolicySetting.html | com/anythink/core/common/c/i.java |
| https:///hostsetting/dmlist/index.html | com/anythink/core/common/c/i.java |
| https:///hostsetting/mumbai/index.html | com/anythink/core/common/c/i.java |
| https://mores.toponad.com/image/adx\_animate/animate5\_recommend1.png | com/anythink/core/d/a.java |
| https://mores.toponad.com/image/adx\_animate/animate5\_recommend2.png | com/anythink/core/d/a.java |
| https://mores.toponad.com/image/adx\_animate/animate5\_recommend3.png | com/anythink/core/d/a.java |
| https://mores.toponad.com/image/adx\_animate/animate5\_recommend4.png | com/anythink/core/d/a.java |
| https://i.snssdk.com/ | com/bytedance/sdk/openadsdk/downloadnew/core/AdBaseConstants.java |
| https://errlog.umeng.com/api/crashsdk/logcollect | com/efs/sdk/base/core/f/c.java |
| https://errlog.umeng.com/api/crashsdk/logcollect | com/efs/sdk/base/core/controller/ControllerCenter.java |
| https://errlogos.umeng.com/api/crashsdk/logcollect | com/efs/sdk/base/core/controller/ControllerCenter.java |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/offline\_components/tk/ks\_so-tachikomaNoSoRelease-3.3.65-b0263a1df2-545.zip | com/kwad/components/offline/c/c.java |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/tachikoma/3.3.58/ks\_tk\_so\_v8\_lite\_3358 | com/kwad/components/offline/c/b/a.java |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/tachikoma/3.3.58/ks\_tk\_so\_v8\_3358 | com/kwad/components/offline/c/b/a.java |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/tachikoma/3.3.58/ks\_tk\_so\_v7\_lite\_3358 | com/kwad/components/offline/c/b/a.java |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/tachikoma/3.3.58/ks\_tk\_so\_v7\_3358 | com/kwad/components/offline/c/b/a.java |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/offline\_components/obiwan/ks\_so-obiwanNoSoRelease-3.3.56-445ef4f109-409.zip | com/kwad/components/offline/b/b.java |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/offline\_components/adLive/ks\_so-adLiveNoSoRelease-3.3.64-be215cc537-546.zip | com/kwad/components/offline/a/b.java |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/adLive/ks\_so-adLiveArm64v8aRelease-3.3.44.2-e8fbb3a5f8-666.apk | com/kwad/components/offline/a/a/a.java |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/adLive/ks\_so-adLiveArmeabiv7aRelease-3.3.44.2-e8fbb3a5f8-666.apk | com/kwad/components/offline/a/a/a.java |
| https://github.com/lingochamp/FileDownloader/wiki/filedownloader.properties | com/kwad/framework/filedownloader/services/a.java |
| https://style-browse-openapi.test.gifshow.com//rest/e/internal/adBrowse | com/kwad/sdk/h.java |
| https://open.e.kuaishou.com/rest/e/v3/open/sdk2 | com/kwad/sdk/api/loader/u.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/ks\_so-appStatusArm64v8aRelease-3.3.14.apk | com/kwad/sdk/collector/d.java |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/ks\_so-appStatusArmeabiv7aRelease-3.3.14.apk | com/kwad/sdk/collector/d.java |
| http://%s:%d/%s | com/kwad/sdk/core/videocache/f.java |
| https://github.com/danikula/AndroidVideoCache/issues/88. | com/kwad/sdk/core/videocache/h.java |
| https://github.com/danikula/AndroidVideoCache/issues/43. | com/kwad/sdk/core/videocache/h.java |
| https://github.com/danikula/AndroidVideoCache/issues. | com/kwad/sdk/core/videocache/h.java |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/so/exception/202305301754/ks\_so-exceptionArm64v8aRelease-3.3.47-e8fbb3a5f8-666.apk | com/kwad/sdk/crash/g.java |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/so/exception/202305301754/ks\_so-exceptionArmeabiv7aRelease-3.3.47-e8fbb3a5f8-666.apk | com/kwad/sdk/crash/g.java |
| http://apps.samsung.com/appquery/appDetail.as?appId= | com/kwad/sdk/utils/d.java |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/kmac/ks\_kmac64 | com/kwad/sdk/kgeo/c.java |
| https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDk/kmac/ks\_kmac32 | com/kwad/sdk/kgeo/c.java |
| https://sf6-ttcdn-tos.pstatp.com/obj/ad-tetris-site/personal-privacy-page.html | com/ss/android/downloadlib/addownload/compliance/AppPrivacyPolicyActivity.java |
| https://apps.oceanengine.com/customer/api/app/pkg\_info? | com/ss/android/downloadlib/addownload/compliance/wo.java |
| https://apps.bytesfield.com | com/ss/android/downloadlib/addownload/compliance/un.java |
| https://apps.bytesfield-b.com | com/ss/android/downloadlib/addownload/compliance/un.java |
| https://www.samsungapps.com/appquery/appDetail.as?appId= | com/ss/android/downloadlib/z/hb.java |
| https://i.snssdk.com/ | com/ss/android/downloadad/api/constant/AdBaseConstants.java |
| http://developer.umeng.com/docs/66650/cate/66650 | com/umeng/analytics/pro/j.java |
| https://developer.umeng.com/docs/119267/detail/182050 | com/umeng/commonsdk/debug/UMLogCommon.java |
| https://developer.umeng.com/docs/66632/detail/ | com/umeng/commonsdk/debug/UMLogUtils.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://plbslog.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://ulogs.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://alogus.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://pslog.umeng.com | com/umeng/commonsdk/vchannel/a.java |
| https://pslog.umeng.com/ | com/umeng/commonsdk/vchannel/a.java |
| https://utoken.umeng.com/api/postZdata/v4 | com/umeng/umzid/ZIDManager.java |
| https://utoken.umeng.com/api/updateZdata/v4 | com/umeng/umzid/ZIDManager.java |
| https://aa.birdgesdk.com/v1/d\_api | com/tramini/plugin/a/b/a.java |
| https://pitk.birdgesdk.com/v1/ptk | com/tramini/plugin/a/b/a.java |
| https://rr | com/tramini/plugin/a/f/a.java |
| https://errlogos.umeng.com/upload | com/uc/crashsdk/e.java |
| https://errlog.umeng.com/upload | com/uc/crashsdk/e.java |
| https://px-intl.ucweb.com | com/uc/crashsdk/a/h.java |
| https://px.ucweb.com | com/uc/crashsdk/a/h.java |
| https://errlogos.umeng.com/api/crashsdk/logcollect | com/uc/crashsdk/a/h.java |
| https://errlog.umeng.com/api/crashsdk/logcollect | com/uc/crashsdk/a/h.java |
| https://errlogos.umeng.com | com/uc/crashsdk/a/d.java |
| https://errlog.umeng.com | com/uc/crashsdk/a/d.java |
| https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s | com/tencent/mm/opensdk/diffdev/a/c.java |
| https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s | com/tencent/mm/opensdk/diffdev/a/b.java |
| http://schemas.android.com/apk/res/android | f/a/a/g.java |
| https://errlog.umeng.com/api/crashsdk/logcollect | lib/arm64-v8a/libcrashsdk.so |
| https://errlogos.umeng.com/api/crashsdk/logcollect | lib/arm64-v8a/libcrashsdk.so |
| https://errlog.umeng.com | lib/arm64-v8a/libcrashsdk.so |
| https://errlogos.umeng.com | lib/arm64-v8a/libcrashsdk.so |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| .apk@classes.dex | com/kuaishou/weapon/p0/ac.java |
| danikula@gmail.com | com/kwad/sdk/core/videocache/h.java |

### **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: True 找到 1 个唯一证书 主题: C=CN, ST=GD, L=ShangHai, O=Tencent, OU=3G, CN=WilsonWu 签名算法: rsassa\_pkcs1v15 有效期自: 2024-06-21 09:05:29+00:00 有效期至: 2572-01-20 09:05:29+00:00 发行人: C=CN, ST=GD, L=ShangHai, O=Tencent, OU=3G, CN=WilsonWu 序列号: 0x7731b7dc 哈希算法: sha256 md5值: 0feab83a98eecf803e1d2297a0c8c512 sha1值: f6848b0c9c5ba6e58b384b325c8f09d2d66fffbe sha256值: 67de77a225d9b59cb2d50b6af7dc30a604f438df536556a98150cac4ee4156ad sha512值: 69d338c854f8f38a9eb51d2dac3e4ef218ef531fae042e4a90df68e5aa69b37957f00f9e50eec2f16d0aa0a498fa563e5bb32b1a910679e09ac84986a88b11e9 公钥算法: rsa 密钥长度: 2048 指纹: 65e74c4dd5fbf7823b8b79e77a2204d129d5adc9ca3b00baef547f63860a434d**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "anythink\_myoffer\_feedback\_violation\_of\_laws" : "Illegal" |
| "anythink\_myoffer\_feedback\_violation\_of\_laws" : "违规违法" |

## **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.BLUETOOTH\_ADMIN | 正常 | 蓝牙管理 | 允许应用程序发现和配对蓝牙设备。 |
| 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\_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\_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.READ\_PRIVILEGED\_PHONE\_STATE | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.CHANGE\_WIFI\_STATE | 正常 | 更改Wi-Fi状态 | 允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改 |
| android.permission.CHANGE\_NETWORK\_STATE | 正常 | 更改网络连接 | 允许应用程序更改网络连接状态。 |
| 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.WRITE\_SETTINGS | 危险 | 修改全局系统设置 | 允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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 |
| 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.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 |
| com.overhead.laser.liquor.openadsdk.permission.TT\_PANGOLIN | 未知 | Unknown permission | Unknown permission from android reference |
| com.overhead.laser.liquor.permission.KW\_SDK\_BROADCAST | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BLUETOOTH\_CONNECT | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BLUETOOTH | 正常 | 创建蓝牙连接 | 允许应用程序连接到配对的蓝牙设备 |
| android.permission.BLUETOOTH\_SCAN | 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.google.android.gms.permission.AD\_ID | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.REORDER\_TASKS | 正常 | 重新排序正在运行的应用程序 | 允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| freemme.permission.msa | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |

## **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。**