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

**一份礼物（ 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 | 一份礼物 |
| 版本 | 1.0 |
| 包名 | com.imult.musicbears |
| 域名线索 | 3条 |
| URL线索 | 1条 |
| APP图标 |  |
| 分析日期 | 2025年7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 | opaoguonai.apk |
| 文件大小 | 9.57MB |
| MD5值 | 5c9540ff3f1e7efba20941970054ade7 |
| SHA1值 | 365e8ded23fe3f164db51b05712ad0748053f03a |
| SHA256值 | 668905c12bac73e3280cd7336f122f0f447eb80ba9274312225ebce2e07f46b1 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 一份礼物 |
| 包名 | com.imult.musicbears |
| 主活动Activity | org.apache.LoadingActivity |
| 安卓版本名称 | 1.0 |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| gjapplog.ucweb.com | IP: 157.185.189.158 所属国家: Canada 地区: Ontario 城市: North York  |
| errlog.umeng.com | IP: 223.109.148.180 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| applog.uc.cn | IP: 116.132.219.180 所属国家: China 地区: Hebei 城市: Shijiazhuang  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://applog.uc.cn/collect  | lib/arm64-v8a/libcrashsdk.so  |
| https://gjapplog.ucweb.com/collect  | lib/arm64-v8a/libcrashsdk.so  |
| https://errlog.umeng.com  | lib/arm64-v8a/libcrashsdk.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: C=cn, ST=ak, L=ak, O=androidkiller, OU=androidkiller, CN=androidkiller 签名算法: rsassa\_pkcs1v15 有效期自: 2014-12-23 06:27:44+00:00 有效期至: 2069-09-25 06:27:44+00:00 发行人: C=cn, ST=ak, L=ak, O=androidkiller, OU=androidkiller, CN=androidkiller 序列号: 0x661d0629 哈希算法: sha256 md5值: 6230025aa9d683803c2bec499f6be89b sha1值: ac4c35dbb80e320ac5e432f4991fd81798191c68 sha256值: 927d5aa90736d7b8d1b1f06978bb3697395caf14f794544158f37abd0f21df6d sha512值: 50a756bf495b76d7583b0d1970eb4bfd7b7a7f4754bd57f486a2ba9996b7ccb8a4f88fdcf16189634909819b2b35e81654a4f687b591778a9328cb3bdf27036a**

## **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.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\_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.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.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\_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.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.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\_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 |

## **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。**