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

**花开富贵（ 1.0.1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 | 花开富贵 |
| 版本 | 1.0.1 |
| 包名 | com.mkdw.zhtrf |
| 域名线索 | 10条 |
| URL线索 | 7条 |
| APP图标 |  |
| 分析日期 | 2024年9月20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 | 花开富贵.apk |
| 文件大小 | 26.41MB |
| MD5值 | ddcea0c60cc7fd29b33d4fdadde13bb8 |
| SHA1值 | 1021e1d035f7b1d7539172ccaf8352d26fed3a0b |
| SHA256值 | 85445783b744943477e27be279065921d60092766c7d00e6e5b3933d4b63174a |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 花开富贵 |
| 包名 | com.mkdw.zhtrf |
| 主活动Activity | com.bxw.hall.MainActivity |
| 安卓版本名称 | 1.0.1 |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| config.uca.cloud.unity3d.com | IP: 34.111.113.40 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| www.openssl.org | IP: 34.36.58.177 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| mta.oa.com | IP: 141.144.196.217 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam  |
| pingma.qq.com | IP: 116.147.19.64 所属国家: China 地区: Beijing 城市: Beijing  |
| api.uca.cloud.unity3d.com | IP: 43.156.88.56 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| mta.qq.com | IP: 0.0.0.1 所属国家: - 地区: - 城市: -  |
| 1212.ip138.com | IP: 110.81.155.138 所属国家: China 地区: Fujian 城市: Quanzhou  |
| cdp.cloud.unity3d.com | IP: 101.32.104.143 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| cloudaemon.com | IP: 203.107.45.167 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| d.appjiagu.com | IP: 111.206.126.183 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://1212.ip138.com/ic.asp  | com/cloudaemon/libguandujni/GuanduJNI.java  |
| http://d.appjiagu.com/lc  | com/jg/bh/Constants.java  |
| http://pingma.qq.com:80/mstat/report  | com/tencent/wxop/stat/c.java  |
| http://mta.qq.com/  | com/tencent/wxop/stat/e.java  |
| http://mta.oa.com/  | com/tencent/wxop/stat/e.java  |
| http://cloudaemon.com/howto.html  | lib/armeabi-v7a/libguandu.so  |
| http://www.openssl.org/support/faq.html  | lib/armeabi-v7a/libguandu.so  |
| https://config.uca.cloud.unity3d.com  | lib/armeabi-v7a/libunity.so  |
| https://cdp.cloud.unity3d.com/v1/events  | lib/armeabi-v7a/libunity.so  |
| https://api.uca.cloud.unity3d.com/v1/events  | lib/armeabi-v7a/libunity.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| sales@openvpn.net  | lib/armeabi-v7a/libguandu.so  |

### **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, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com 签名算法: rsassa\_pkcs1v15 有效期自: 2008-02-29 01:33:46+00:00 有效期至: 2035-07-17 01:33:46+00:00 发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com 序列号: 0x936eacbe07f201df 哈希算法: sha1 md5值: e89b158e4bcf988ebd09eb83f5378e87 sha1值: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81 sha256值: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc sha512值: 5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea303977272d17958704d89b7711292a4569**

## **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.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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.RECEIVE\_BOOT\_COMPLETED | 正常 | 开机时自动启动 | 允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度 |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.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.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\_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.BROADCAST\_STICKY | 正常 | 发送粘性广播 | 允许应用程序发送粘性广播,在广播结束后保留。恶意应用程序会导致手机使用过多内存,从而使手机运行缓慢或不稳定 |
| 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.GET\_PACKAGE\_SIZE | 正常 | 测量应用程序存储空间 | 允许应用程序找出任何包使用的空间 |
| 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\_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.MOUNT\_UNMOUNT\_FILESYSTEMS | 危险 | 装载和卸载文件系统 | 允许应用程序为可移动存储安装和卸载文件系统 |
| 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.INTERACT\_ACROSS\_USERS\_FULL | 未知 | Unknown permission | Unknown permission from android reference |
| com.android.launcher.permission.INSTALL\_SHORTCUT | 未知 | Unknown permission | Unknown permission from android reference |
| com.android.launcher.permission.UNINSTALL\_SHORTCUT | 未知 | Unknown permission | Unknown permission from android reference |

## **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。**