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

**米多赚钱（ 1.8.0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 | 米多赚钱 |
| 版本 | 1.8.0 |
| 包名 | com.sakura.mizhuan |
| 域名线索 | 18条 |
| URL线索 | 6条 |
| APP图标 |  |
| 分析日期 | 2025年7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 | base.apk |
| 文件大小 | 25.94MB |
| MD5值 | 5bb8f35d4d20da6e1d648abdba9968e3 |
| SHA1值 | 95007417fc68583a248a8f9a3f6d37f2aa523214 |
| SHA256值 | 1fb8db6b0a5012297f9a5faeefea8341f09bcd23ba7d8ddf5c6353d96b0ac06d |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 米多赚钱 |
| 包名 | com.sakura.mizhuan |
| 主活动Activity | com.sakura.mizhuan.activity.FlashActivity |
| 安卓版本名称 | 1.8.0 |
| 安卓版本 | 180 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| metrics5.data.hicloud.com | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| gcc.gnu.org | IP: 8.43.85.97 所属国家: United States of America 地区: North Carolina 城市: Raleigh  |
| www.mob.com | IP: 180.188.26.28 所属国家: China 地区: Zhejiang 城市: Taizhou  |
| metrics5.dt.dbankcloud.ru | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| www.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| grs.dbankcloud.com | IP: 60.28.193.195 所属国家: China 地区: Tianjin 城市: Tianjin  |
| grs.platform.dbankcloud.ru | 没有服务器地理信息.  |
| metrics1.data.hicloud.com | IP: 111.202.16.252 所属国家: China 地区: Beijing 城市: Beijing  |
| metrics2.data.hicloud.com | IP: 80.158.38.48 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| metrics-dra.dt.hicloud.com | IP: 94.74.88.100 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| data-dre.push.dbankcloud.com | IP: 80.158.49.244 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| data-dra.push.dbankcloud.com | IP: 119.8.163.189 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| grs.dbankcloud.cn | IP: 121.36.116.8 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  |
| metrics.dt.dbankcloud.ru | IP: 159.138.204.140 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| grs.dbankcloud.asia | IP: 49.4.40.185 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| data-drru.push.dbankcloud.com | IP: 159.138.202.31 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| grs.dbankcloud.eu | 没有服务器地理信息.  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://www.mob.com/policy/en>http://www.mob.com/policy/en</a>.  | 摸瓜V1引擎  |
| http://www.mob.com/about/policy>http://www.mob.com/about/policy</a>  | 摸瓜V1引擎  |
| https://www.mob.com  | 摸瓜V1引擎  |
| http://www.mob.com/about/policy/en>http://www.mob.com/about/policy/en</a>.If  | 摸瓜V1引擎  |
| http://www.mob.com/policy/zh>http://www.mob.com/policy/zh</a>  | 摸瓜V1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://metrics5.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics.dt.dbankcloud.ru  | 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://metrics5.dt.dbankcloud.ru:6447  | 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.asia  | 摸瓜V2引擎  |
| https://grs.platform.dbankcloud.ru  | 摸瓜V2引擎  |
| https://grs.dbankcloud.eu  | 摸瓜V2引擎  |
| http://schemas.android.com/aapt  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/android  | 摸瓜V3引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V3引擎  |
| http://gcc.gnu.org/bugs.html):  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res-auto  | 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=CN, ST=Guangdong, L=Shenzhen, O=Seabeach, OU=Seabeach, CN=admin 签名算法: rsassa\_pkcs1v15 有效期自: 2019-12-23 03:52:53+00:00 有效期至: 2044-12-16 03:52:53+00:00 发行人: C=CN, ST=Guangdong, L=Shenzhen, O=Seabeach, OU=Seabeach, CN=admin 序列号: 0x1ec1871b 哈希算法: sha256 md5值: 0e228cc812c2ce9ce2eb135e0dd3b6fe sha1值: 3597c9c6eea1bee153ad047fa37deee0ebb346d8 sha256值: 1e6c9674298f943faf965b79f311886b7ceff7088d6338239a4013412859c19b sha512值: c5ad60b8d96691039c34e022fc54baef36f19ab049aa7384f398f89ff7d285064c42cdf29a95431085c765b2b3b6d463a16bc5b28165f86682ec3f92acb16e60 公钥算法: rsa 密钥长度: 2048 指纹: 1cfd6dae63e5ac4ba56eaf46cf569778661d453720fb8f75c90402b8d13394a0**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "Modify\_user\_name" : "修改用户名"  |
| "mobcommon\_authorize\_dialog\_accept" : "Accept"  |
| "mobcommon\_authorize\_dialog\_content" : "In order to provide you with Mobservice, please check our service policy. For details, please click <a href=http://www.mob.com/policy/en>http://www.mob.com/policy/en</a>. If you agree with our service policy, please click accept, if you do not agree with our service policy, please click reject"  |
| "mobcommon\_authorize\_dialog\_reject" : "Reject"  |
| "mobcommon\_authorize\_dialog\_title" : "Terms of Use"  |
| "mobdemo\_authorize\_dialog\_content" : "为了给您提供Mobservice相关产品服务，请您详细查看我们的隐私政策，详见<a href=http://www.mob.com/about/policy>http://www.mob.com/about/policy</a>。如您同意我们的隐私政策，请点击“接受”，如您不同意我们的隐私政策，请点击“拒绝”。"  |
| "mobdemo\_authorize\_dialog\_title" : "服务授权"  |
| "ssdk\_cmcc\_auth" : "手机认证服务由中国移动提供"  |
| "ssdk\_cmcc\_login\_one\_key" : "本机号码一键登录"  |
| "ssdk\_instapaper\_pwd" : "密码"  |
| "ssdk\_weibo\_oauth\_regiseter" : "应用授权"  |
| "mobcommon\_authorize\_dialog\_accept" : "Accept"  |
| "mobcommon\_authorize\_dialog\_content" : "In order to provide you with Mobservice, please check our service policy. For details, please click <a href=http://www.mob.com/policy/en>http://www.mob.com/policy/en</a>. If you agree with our service policy, please click accept, if you do not agree with our service policy, please click reject"  |
| "mobcommon\_authorize\_dialog\_reject" : "Reject"  |
| "mobcommon\_authorize\_dialog\_title" : "Terms of Use"  |
| "mobdemo\_authorize\_dialog\_content" : "In order to provide you with Mobservice related products and services, please check our privacy policy in detail, see details<a href=http://www.mob.com/about/policy/en>http://www.mob.com/about/policy/en</a>.If you agree with our privacy policy, please click accept. If you disagree with our privacy policy, please click reject."  |
| "mobdemo\_authorize\_dialog\_title" : "service authority"  |
| "ssdk\_cmcc\_auth" : "Provided by China Mobile"  |
| "ssdk\_cmcc\_login\_one\_key" : "PhoneNum Login"  |
| "ssdk\_instapaper\_pwd" : "Password"  |
| "ssdk\_weibo\_oauth\_regiseter" : "Authorization"  |
| "mobcommon\_authorize\_dialog\_accept" : "同意"  |
| "mobcommon\_authorize\_dialog\_content" : "为了给您提供Mobservice相关产品服务，请您详细查看我们的隐私政策，详见<a href=http://www.mob.com/policy/zh>http://www.mob.com/policy/zh</a>。如您同意我们的隐私政策，请点击“接受”，如您不同意我们的隐私政策，请点击“拒绝”。"  |
| "mobcommon\_authorize\_dialog\_reject" : "拒绝"  |
| "mobcommon\_authorize\_dialog\_title" : "服务授权"  |

## **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.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.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.BROADCAST\_PACKAGE\_ADDED | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BROADCAST\_PACKAGE\_CHANGED | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BROADCAST\_PACKAGE\_INSTALL | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BROADCAST\_PACKAGE\_REPLACED | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |
| 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。 |
| android.permission.READ\_PRIVILEGED\_PHONE\_STATE | 未知 | Unknown permission | Unknown permission from android reference |
| 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.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.PERMISSIONS\_STORAGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.CAMERA | 危险 | 拍照和录像 | 允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像 |
| 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.READ\_MEDIA\_IMAGES | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_AUDIO | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_VIDEO | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.WRITE\_MEDIA\_STORAGE | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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。 |
| com.meizu.flyme.permission.PUSH | 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.sakura.mizhuan.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.sakura.mizhuan.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 |
| com.heytap.mcs.permission.RECIEVE\_MCS\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.sakura.mizhuan.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| com.sakura.mizhuan.permission.PUSH\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| com.sakura.mizhuan.permission.MIPUSH\_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.gms.permission.AD\_ID | 未知 | Unknown permission | Unknown permission from android reference |
| com.vivo.notification.permission.BADGE\_ICON | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.sakura.mizhuan.activity.RenWuDetailActivity | **Schemes**: miduo://, **Hosts:** app, **Path Prefixes:** /TaskDetail,  |

**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。**