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

**挖财记账（ 12.9.31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 | 挖财记账 |
| 版本 | 12.9.31 |
| 包名 | com.wacai365 |
| 域名线索 | 21条 |
| URL线索 | 8条 |
| APP图标 |  |
| 分析日期 | 2025年6月26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 | 挖财记账.apk |
| 文件大小 | 51.67MB |
| MD5值 | 0187d9bfef63511c9ee067bd1a7dc831 |
| SHA1值 | 72f5bda813e1053f68b19128971246213219237f |
| SHA256值 | cbdcb65bf2f3690c730fb367530106832b43fc422b2de36c9adf3a2d8c697a81 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 挖财记账 |
| 包名 | com.wacai365 |
| 主活动Activity | com.wacai.launch.LauncherActivity |
| 安卓版本名称 | 12.9.31 |
| 安卓版本 | 471 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| sf3-fe-tos.pglstatp-toutiao.com | IP: 60.9.0.236 所属国家: China 地区: Hebei 城市: Hengshui  |
| grs.dbankcloud.cn | IP: 49.4.45.231 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| data-drcn.push.dbankcloud.com | IP: 49.4.40.58 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| www.wacai.com | IP: 103.98.46.4 所属国家: China 地区: Shaanxi 城市: Xi'an  |
| grs.platform.dbankcloud.ru | 没有服务器地理信息.  |
| metrics2.data.hicloud.com | IP: 80.158.38.48 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  |
| data-drru.push.dbankcloud.com | IP: 159.138.202.31 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| site.wacai.com | IP: 103.98.46.4 所属国家: China 地区: Shaanxi 城市: Xi'an  |
| metrics1-drcn.dt.dbankcloud.cn | IP: 111.202.16.252 所属国家: China 地区: Beijing 城市: Beijing  |
| www.jsdelivr.com | IP: 172.67.208.113 所属国家: United States of America 地区: California 城市: San Francisco  |
| metrics5.dt.dbankcloud.ru | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| www.yuancaiyun.com | IP: 103.98.46.16 所属国家: China 地区: Shaanxi 城市: Xi'an  |
| grs.dbankcloud.com | IP: 60.28.200.159 所属国家: China 地区: Tianjin 城市: Tianjin  |
| data-dre.push.dbankcloud.com | IP: 80.158.49.244 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| grs.dbankcloud.asia | IP: 49.4.40.185 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| common.wacai.com | IP: 103.98.46.4 所属国家: China 地区: Shaanxi 城市: Xi'an  |
| metrics5.data.hicloud.com | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| metrics-dra.dt.hicloud.com | IP: 94.74.88.100 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| 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.wacai.com  | 摸瓜V1引擎  |
| https://www.wacai.com/wap  | 摸瓜V1引擎  |
| https://github.com/vinc3m1  | 摸瓜V1引擎  |
| https://github.com/vinc3m1/RoundedImageView  | 摸瓜V1引擎  |
| https://github.com/vinc3m1/RoundedImageView.git  | 摸瓜V1引擎  |
| https://site.wacai.com/page/12242  | 摸瓜V1引擎  |
| https://www.yuancaiyun.com  | 摸瓜V1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-drcn.dt.dbankcloud.cn:443  | 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  |
| https://www.jsdelivr.com/using-sri-with-dynamic-files  | 摸瓜V2引擎  |
| https://github.com/apvarun/toastify-js  | 摸瓜V2引擎  |
| https://sf3-fe-tos.pglstatp-toutiao.com/obj/csj-sdk-static/csj\_assets/shake.webp  | 摸瓜V2引擎  |
| https://sf3-fe-tos.pglstatp-toutiao.com/obj/csj-sdk-static/csj\_assets/shake\_text.png  | 摸瓜V2引擎  |
| https://sf3-fe-tos.pglstatp-toutiao.com/obj/csj-sdk-static/csj\_assets/swipe\_right.webp  | 摸瓜V2引擎  |
| https://common.wacai.com  | 摸瓜V2引擎  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| kf@wacai.com jzkf@yuancaiyun.com  | 摸瓜V1引擎  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 14234280276  | 摸瓜V2引擎  |
| 14096622808  | 摸瓜V2引擎  |

## **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=CH, ST=Zhejiang, L=Hangzhou, O=caimi, OU=caimi, CN=wacai.clm 签名算法: rsassa\_pkcs1v15 有效期自: 2010-01-13 15:32:49+00:00 有效期至: 2119-07-21 15:32:49+00:00 发行人: C=CH, ST=Zhejiang, L=Hangzhou, O=caimi, OU=caimi, CN=wacai.clm 序列号: 0x4b4de7a1 哈希算法: sha1 md5值: 1fa31b6ee1f447c250b12150ef5966f2 sha1值: 729f7d8388117240846a6831b60e6e703def636c sha256值: a0703131214f853d9f056642c0d8048e299f2c2a03408117adbed665f627b9a3 sha512值: b9a9a88d385bb5f68a85fda8bf92ebcdbff22ed8fa65c29658ee325bbfd888126b8959502e402252ddd950b14c578eaa7e11920141a6ee6fc0ab855beb0df1e3 公钥算法: rsa 密钥长度: 1024 指纹: 15dbd4fc4d7657374cfed772f6a4f8e9e61187df189b66e9bf2333648af7e51e**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "PSWNotRegisterUser" : "您没有登录过挖财帐号，无法进行重置。"  |
| "changePassword" : "已设置"  |
| "cs\_not\_auth" : "未授权"  |
| "default\_user\_name" : "财宝宝"  |
| "library\_roundedimageview\_author" : "Vince Mi"  |
| "library\_roundedimageview\_authorWebsite" : "https://github.com/vinc3m1"  |
| "local\_password" : "手势密码"  |
| "loginPassword" : "登录密码"  |
| "lr\_find\_pwd" : "找回密码"  |
| "lr\_find\_pwd\_by\_email" : "通过绑定邮箱找回"  |
| "lr\_find\_pwd\_by\_phone" : "通过绑定手机找回"  |
| "lr\_find\_pwd\_use\_phone" : "手机找回密码"  |
| "lr\_forget\_pwd" : "忘记密码?"  |
| "lr\_password" : "密 码"  |
| "lr\_reset\_pwd" : "修改密码"  |
| "lr\_reset\_pwd\_success" : "修改成功"  |
| "modifyLocalPassword" : "修改手势密码"  |
| "resetPassword" : "尝试次数已用完，去重置密码吧 >"  |
| "rp\_wx\_authinfo\_invalid" : "微信验证数据不完整"  |
| "server\_auth\_failed" : "服务器身份验证失败,请稍后再试"  |
| "setPassword" : "去设置"  |
| "txtForgetPassword" : "忘记密码"  |

## **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.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.READ\_LOGS | 危险 | 读取敏感日志数据 | 允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息 |
| 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.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 |
| com.wacai365.permission.MIPUSH\_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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.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.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.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 |
| com.wacai365.openadsdk.permission.TT\_PANGOLIN | 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 |
| android.permission.POST\_NOTIFICATIONS | 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.wacai365.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| com.wacai365.permission.PUSH\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| com.hihonor.push.permission.READ\_PUSH\_NOTIFICATION\_INFO | 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。 |
| android.permission.SCHEDULE\_EXACT\_ALARM | 正常 |  | 允许应用程序使用精确的警报调度 API 来执行对时间敏感的后台工作 |
| getui.permission.GetuiService.com.wacai365 | 未知 | Unknown permission | Unknown permission from android reference |
| com.vivo.notification.permission.BADGE\_ICON | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ACCESS\_BACKGROUND\_LOCATION | 危险 | 后台访问位置 | 允许应用程序在后台访问位置 |
| com.asus.msa.SupplementaryDID.ACCESS | 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 |
| freemme.permission.msa | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.wacai.launch.LauncherActivity | **Schemes**: wacai://, wacaiopen://,  |
| com.tencent.tauth.AuthActivity | **Schemes**: tencent100245713://,  |

**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。**