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

**中金wealth（ null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 | 中金wealth |
| 版本 | null |
| 包名 | JdnNdnnm.fimjnuJndkahoiJdmHe.hlahmNdwjjUs |
| 域名线索 | 5条 |
| URL线索 | 3条 |
| APP图标 |  |
| 分析日期 | 2025年6月16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 | 28.39MB |
| MD5值 | 1c97b969666f942db2afd903acab572e |
| SHA1值 | a8164960d7671179ec68f14fbfb8a5759ec310c2 |
| SHA256值 | 2eec95b25b5c08efa1c2668cd0d5eaf691c7ee23b1893d34f5272bd8110829fc |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 中金wealth |
| 包名 | JdnNdnnm.fimjnuJndkahoiJdmHe.hlahmNdwjjUs |
| 主活动Activity | com.westpm.hlahl.ui.activity.OpeningActivity |
| 安卓版本名称 | null |
| 安卓版本 |  |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| www.migu.cn | IP: 117.135.165.90 所属国家: China 地区: Shanghai 城市: Shanghai  |
| 172.20.10.4 | IP: 172.20.10.4 所属国家: - 地区: - 城市: -  |
| gzbdy.gz.bcebos.com | IP: 153.3.238.105 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| cdbdy.cd.bcebos.com | IP: 182.61.129.20 所属国家: China 地区: Beijing 城市: Beijing  |
| bjbdy.bj.bcebos.com | IP: 113.200.2.111 所属国家: China 地区: Shaanxi 城市: Yulin  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://172.20.10.4:8080/food  | com/westpm/hlahl/util/Constant.java  |
| https://www.migu.cn/ilndex.html  | com/westpm/hlahl/ui/activity/webActivity.java  |
| https://gzbdy.gz.bcebos.com/ab0423.json  | com/westpm/hlahl/ui/activity/OpeningActivity.java  |
| https://cdbdy.cd.bcebos.com/ab0423.json  | com/westpm/hlahl/ui/activity/OpeningActivity.java  |
| https://bjbdy.bj.bcebos.com/ab0423.json  | com/westpm/hlahl/ui/activity/OpeningActivity.java  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| 123456789@qq.com  | com/westpm/hlahl/ui/activity/OpeningActivity.java  |

### **4.4 手机号线索**

## **5. 签名证书**

**APK已签名 v1 签名: False v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: C=ssxiremydgiyl, ST=xcfvpxjkwxhmz, L=ouokprvhlrffu, O=nzx1747961622302, OU=lzl1747961622302, CN=TG@apkfangdujiagu 签名算法: rsassa\_pkcs1v15 有效期自: 2025-05-23 00:53:42+00:00 有效期至: 2075-05-11 00:53:42+00:00 发行人: C=ssxiremydgiyl, ST=xcfvpxjkwxhmz, L=ouokprvhlrffu, O=nzx1747961622302, OU=lzl1747961622302, CN=TG@apkfangdujiagu 序列号: 0x554db02a 哈希算法: sha1 md5值: d559a37e1c87fc4ef80a57f8df893d6e sha1值: a1ebe2d435cd26f262151ab792918b6a6e3fe56c sha256值: 0dafc26a1dc67c6243294f06289057535fedac9f62b2cc18cdfb2661e8792e8c sha512值: 03d0dc3f1d8277ea47eaeaa69efe7152ebbadd7f221e96255ffcc12c5e70be3a6b50dbdfa5b93df70e3450506b660efdb93756d9475b4c91c2f8f212b24a4c97 公钥算法: rsa 密钥长度: 1024 指纹: df667abb0a39ae48162488bcc25b716856d3574310472604ad2f0697a91f51ad**

## **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.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\_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.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.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.NETWORK\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.MANAGE\_EXTERNAL\_STORAGE | 危险 | 允许应用程序广泛访问范围存储中的外部存储 | 允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用 |
| 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\_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.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 |
| com.android.launcher.permission.READ\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| com.android.launcher.permission.WRITE\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_VISUAL\_USER\_SELECTED | 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。**