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

**银河期货（ 5.6.10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 | 银河期货 |
| 版本 | 5.6.10 |
| 包名 | com.yinheqihuo.mhdxh |
| 域名线索 | 23条 |
| URL线索 | 5条 |
| APP图标 |  |
| 分析日期 | 2025年6月27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 | 1740720410256.apk |
| 文件大小 | 128.14MB |
| MD5值 | c0455d563a0a602bfc6ddef17db73079 |
| SHA1值 | b2b27276217e3c2c8a38f88c79c0d5e411142e99 |
| SHA256值 | 2dcab22d46bfd372c55bff9605edae2a0dc67c0c9be6669a1685b2b8c437148e |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 银河期货 |
| 包名 | com.yinheqihuo.mhdxh |
| 主活动Activity | com.pengbo.pbmobile.startup.PbStartupActivity |
| 安卓版本名称 | 5.6.10 |
| 安卓版本 | 56100 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| dr-uat.hsyunyi.com | IP: 121.41.136.219  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| grs.dbankcloud.cn | IP: 49.4.45.231  所属国家: China  地区: Guangdong  城市: Guangzhou |
| dr.hsyunyi.com | IP: 121.41.139.91  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| data-drcn.push.dbankcloud.com | IP: 121.36.117.8  所属国家: China  地区: Beijing  城市: Beijing |
| app5bus.cfmmc.com | IP: 111.203.222.3  所属国家: China  地区: Beijing  城市: Beijing |
| grs.platform.dbankcloud.ru | 没有服务器地理信息. |
| metrics2.data.hicloud.com | IP: 80.158.2.190  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 |
| android.googlesource.com | IP: 192.178.163.82  所属国家: United States of America  地区: California  城市: Mountain View |
| data-drru.push.dbankcloud.com | IP: 159.138.202.31  所属国家: Russian Federation  地区: Sverdlovskaya oblast'  城市: Yekaterinburg |
| metrics1-drcn.dt.dbankcloud.cn | IP: 111.202.16.252  所属国家: China  地区: Beijing  城市: Beijing |
| metrics5.dt.dbankcloud.ru | IP: 159.138.203.215  所属国家: Russian Federation  地区: Sverdlovskaya oblast'  城市: Yekaterinburg |
| grs.dbankcloud.com | IP: 60.28.193.195  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 |
| vopen.hscloud.cn | IP: 121.41.141.198  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| grs.dbankcloud.asia | IP: 49.4.35.251  所属国家: China  地区: Guangdong  城市: Guangzhou |
| apptest5bus.cfmmc.com | IP: 210.12.36.4  所属国家: China  地区: Beijing  城市: Beijing |
| www.apache.org | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| pbwenda.pobo.net.cn | IP: 210.14.65.65  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| 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 |
| sandbox.hscloud.cn | IP: 122.112.132.188  所属国家: China  地区: Guangdong  城市: Guangzhou |
| 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 |
| --- | --- |
| https://pbwenda.pobo.net.cn:13443 | 摸瓜V1引擎 |
| https://app5bus.cfmmc.com | 摸瓜V1引擎 |
| https://apptest5bus.cfmmc.com | 摸瓜V1引擎 |
| https://dr.hsyunyi.com/cwrp/1.0.0/htrpauth-server | 摸瓜V1引擎 |
| https://vopen.hscloud.cn/cwrp/1.0.0/htrpauth-server | 摸瓜V1引擎 |
| https://vopen.hscloud.cn | 摸瓜V1引擎 |
| https://dr.hsyunyi.com | 摸瓜V1引擎 |
| https://sandbox.hscloud.cn | 摸瓜V1引擎 |
| https://dr-uat.hsyunyi.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 |
| play.googleapis.com | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res-auto | 摸瓜V3引擎 |
| http://www.apache.org/licenses/LICENSE-2.0 | 摸瓜V3引擎 |
| http://schemas.android.com/aapt | 摸瓜V3引擎 |
| https://android.googlesource.com/toolchain/llvm | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android | 摸瓜V3引擎 |
| https://android.googlesource.com/toolchain/llvm-project | 摸瓜V3引擎 |
| https://android.googlesource.com/toolchain/clang | 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: CN=pobo 签名算法: rsassa\_pkcs1v15 有效期自: 2015-05-04 00:46:45+00:00 有效期至: 2045-04-26 00:46:45+00:00 发行人: CN=pobo 序列号: 0x5546c175 哈希算法: sha1 md5值: 6980e41eeaac460dcddfde30a43e1055 sha1值: 35a471439c05abba46fe3e681fc0cd3fd46e71d4 sha256值: 78b701a441ee28b34bb786cdd086680e229f79336db74bccedbcb84c2181e34d sha512值: 0bf82f2d317afe0720d491cf09a959d622ec73b29c6b0bb087dd49b2fa072fb843b230ea86ceab24adf52f3545bb344771598a97c003021d3a9e1a64c0be4d14 公钥算法: rsa 密钥长度: 1024 指纹: 8d890591bd753fa39f4a97778e54642780d70f22cace9c6d06f49810229362f8**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "IDS\_JYMiMa" : "交易密码" |
| "IDS\_MiMa" : "密码" |
| "IDS\_MiMaXiuGai" : "密码修改" |
| "IDS\_MiMa\_Current" : "请输入当前密码" |
| "IDS\_MiMa\_XiuGai\_Success" : "您已成功修改密码" |
| "IDS\_Mima\_Type" : "密码类型" |
| "IDS\_QueRenMima" : "确认密码" |
| "IDS\_ShouShiMiMa" : "手势密码" |
| "IDS\_TiaoGuoShouShiMiMa" : "跳过手势密码" |
| "IDS\_TongXunMiMa" : "通讯密码" |
| "IDS\_XinMima" : "新密码" |
| "IDS\_XiuGaiMiMa" : "修改密码" |
| "IDS\_YinHangMiMa" : "银行密码" |
| "IDS\_ZiJinMiMa" : "资金密码" |
| "IDS\_con\_selector\_key" : "监控价" |
| "IDS\_hq\_login\_password" : "登录密码" |
| "face\_auth\_announce" : "由阿里实人认证提供服务" |
| "face\_detect\_auth\_begin\_cancel" : "放弃" |
| "face\_detect\_auth\_begin\_ok" : "开始验证" |
| "face\_detect\_auth\_begin\_title" : "安全验证" |
| "face\_detect\_auth\_pass" : "验证通过" |
| "face\_detect\_token\_expired\_or\_invalid" : "认证token无效或已过期" |
| "face\_detect\_token\_repeate\_submit" : "认证已通过，重复提交。" |
| "identity\_privacy\_authorization\_statement" : " 本APP运营方为确保用户身份真实性，向您提供更好的安全保障，您可以通过提交身份证等身份信息或面部特征等生物识别信息（均属个人敏感信息）来完成具体产品服务所需要或必要的实人认证。上述信息将使用与验证用户身份真实性。 我们会采用行业领先的技术来保护您提供的个人信息，并使用加密、限权等方式避免其被用于其他用途。 点击同意则表示本人同意我们根据以上方式和目的收集、使用及存储您提供的本人身份材料、面部特征等信息用于实人认证。" |
| "identity\_privacy\_authorization\_statement\_title" : "授权声明" |
| "jsapi\_user" : "com.hundsun.JSAPI.UserJSAPI" |
| "restore\_session" : "您有正在进行的会话，进入会话" |
| "trademenu\_password" : "密码修改" |

## **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\_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\_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.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\_IGNORE\_BATTERY\_OPTIMIZATIONS | 正常 |  | 应用程序必须持有的权限才能使用 Settings.ACTION\_REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS。 |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.RECORD\_VIDEO | 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.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\_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.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.KILL\_BACKGROUND\_PROCESSES | 正常 | 杀死后台进程 | 允许应用程序杀死其他应用程序的后台进程,即使内存不低 |
| 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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.USE\_FINGERPRINT | 正常 | allow use of指纹 | 该常量在 API 级别 28 中已被弃用。应用程序应改为请求 USE\_BIOMETRIC |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.RESTART\_PACKAGES | 正常 | 杀死后台进程 | 允许应用程序杀死其他应用程序的后台进程,即使内存不低 |
| 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 |
| 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.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.READ\_MEDIA\_IMAGES | 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.hardware.camera | 未知 | Unknown permission | Unknown permission from android reference |
| android.hardware.camera.autofocus | 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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| com.yinheqihuo.mhdxh.permission.JPUSH\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.RECEIVE\_USER\_PRESENT | 未知 | Unknown permission | Unknown permission from android reference |
| com.yinheqihuo.mhdxh.permission.MIPUSH\_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.SYSTEM\_ALERT\_WINDOW | 危险 | 显示系统级警报 | 允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕 |
| cn.cyberidentity.certification.AUTH | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BLUETOOTH | 正常 | 创建蓝牙连接 | 允许应用程序连接到配对的蓝牙设备 |
| android.permission.READ\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_PRIVILEGED\_PHONE\_STATE | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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 |
| 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。 |
| com.yinheqihuo.mhdxh.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| com.yinheqihuo.mhdxh.permission.PUSH\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| 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.pengbo.pbmobile.startup.PbStartupActivity | **Schemes**: pobopush\_yinheqihuo://, yinheqihuo://,  **Hosts:** com.pengbo.pbmobile.sdk,  **Paths:** /notify\_detail, |
| com.tencent.tauth.AuthActivity | **Schemes**: \ 1106497990://, |
| com.esign.esignsdk.h5.H5Activity | **Schemes**: esign://,  **Hosts:** facesdk, |

**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。**