MoGua

中金wealth null.APK 分析报告

APP名称: 中金wealth

包名:	JdnNdnnm.fimjnuJndkahoiJdmHe.hlahmNdwjjUs
域名线索:	5条
URL线索:	3条
邮箱线索:	1条
分析日期:	2025年6月15日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: base.apk
文件大小: 28.39MB
MD5值: 1c97b969666f942db2afd903acab572e
SHA1值: a8164960d7671179ec68f14fbfb8a5759ec310c2
SHA256值: 2eec95b25b5c08efa1c2668cd0d5eaf691c7ee23b1893d34f5272bd8110829fc

APP 信息

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:

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 **纬度**: 31.224333 **经度**: 121.468948
172.20.10.4	**IP**: 172.20.10.4 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
gzbdy.gz.bcebos.com	**IP**: 153.3.238.105 **所属国家**: China **地区**: Jiangsu

	城市: Nanjing **纬度**: 32.061668 **经度**: 118.777992
cdbdy.cd.bcebos.com	**IP**: 182.61.129.20 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
bjbdy.bj.bcebos.com	**IP**: 113.200.2.111 **所属国家**: China **地区**: Shaanxi **城市**: Yulin **纬度**: 38.290562 **经度**: 109.749443

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

邮箱线索

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

手机线索

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

硬编码敏感信息

加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

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	允许应用程序写入外部存储

		内容	
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

应用内通信