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

**香港一卡通（ 1.1.15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 | 香港一卡通 |
| 版本 | 1.1.15 |
| 包名 | com.cmbchina.mbankhk |
| 域名线索 | 31条 |
| URL线索 | 16条 |
| APP图标 |  |
| 分析日期 | 2025年8月2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 | 香港一卡通手机银行\_1.1.15\_Apkpure.apk |
| 文件大小 | 155.45MB |
| MD5值 | 9480e5ba65169903fdfe5a6c6e39c519 |
| SHA1值 | 68a25fcca54de8d34263fadd176a751aa24a0d92 |
| SHA256值 | 372f3eec25afca457f1d2f416519361f1c89a3ca958337638e82d4595147f85a |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 香港一卡通 |
| 包名 | com.cmbchina.mbankhk |
| 主活动Activity | com.cmbchina.cmf.ui.splash.SplashActivity |
| 安卓版本名称 | 1.1.15 |
| 安卓版本 | 32 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| bit.ly | IP: 67.199.248.10 所属国家: United States of America 地区: New York 城市: New York City  |
| grs.dbankcloud.eu | 没有服务器地理信息.  |
| data-dre.push.dbankcloud.com | IP: 80.158.49.244 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| store-dra.hispace.dbankcloud.com | IP: 222.73.142.42 所属国家: China 地区: Shanghai 城市: Shanghai  |
| store-at-dre.hispace.dbankcloud.com | 没有服务器地理信息.  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| metrics.dt.dbankcloud.ru | IP: 159.138.204.140 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| g.co | IP: 142.251.43.14 所属国家: United States of America 地区: California 城市: Mountain View  |
| metrics-dra.dt.hicloud.com | IP: 94.74.88.100 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| grs.dbankcloud.cn | IP: 49.4.40.185 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| angular.io | IP: 151.101.65.195 所属国家: United States of America 地区: California 城市: San Francisco  |
| m.cmbchina.com | IP: 116.7.243.51 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| store-drru.hispace.dbankcloud.com | IP: 159.138.205.168 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| data-drcn.push.dbankcloud.com | IP: 118.194.33.160 所属国家: China 地区: Shanghai 城市: Shanghai  |
| central.jaf.cmbchina.cn | 没有服务器地理信息.  |
| grs.dbankcloud.com | IP: 113.201.107.90 所属国家: China 地区: Shaanxi 城市: Baoji  |
| cmb-index.weijuju.com | 没有服务器地理信息.  |
| market.cmbchina.com | IP: 125.39.103.211 所属国家: China 地区: Tianjin 城市: Tianjin  |
| data-drru.push.dbankcloud.com | IP: 159.138.202.31 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| store-dre.hispace.dbankcloud.com | IP: 222.73.142.45 所属国家: China 地区: Shanghai 城市: Shanghai  |
| www.baidu.com | IP: 110.242.68.3 所属国家: China 地区: Hebei 城市: Baoding  |
| play.google.com | IP: 93.46.8.90 所属国家: Italy 地区: Lombardia 城市: Milan  |
| grs.dbankcloud.asia | IP: 121.36.116.8 所属国家: China 地区: Beijing 城市: Beijing  |
| store-drcn.hispace.dbankcloud.cn | IP: 111.202.16.109 所属国家: China 地区: Beijing 城市: Beijing  |
| data-dra.push.dbankcloud.com | IP: 119.8.163.189 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| metrics1.data.hicloud.com | IP: 111.202.17.12 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: 80.158.38.48 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| metrics5.data.hicloud.com | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| material.angular.io | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| appgallery.cloud.huawei.com | IP: 121.36.118.136 所属国家: China 地区: Beijing 城市: Beijing  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://m.cmbchina.com  | Mogua Engine V1  |
| https://play.google.com/store/apps/details?id=  | Mogua Engine V1  |
| https://appgallery.cloud.huawei.com  | Mogua Engine V1  |
| https://metrics1.data.hicloud.com:6447  | Mogua Engine V2  |
| https://metrics-dra.dt.hicloud.com:6447  | Mogua Engine V2  |
| https://metrics2.data.hicloud.com:6447  | Mogua Engine V2  |
| https://metrics5.data.hicloud.com:6447  | Mogua Engine V2  |
| https://grs.dbankcloud.com  | Mogua Engine V2  |
| https://grs.dbankcloud.cn  | Mogua Engine V2  |
| https://grs.dbankcloud.asia  | Mogua Engine V2  |
| https://grs.platform.dbankcloud.ru  | Mogua Engine V2  |
| https://grs.dbankcloud.eu  | Mogua Engine V2  |
| https://store-at-dre.hispace.dbankcloud.com/hwmarket/api/  | Mogua Engine V2  |
| https://data-drcn.push.dbankcloud.com  | Mogua Engine V2  |
| https://data-dra.push.dbankcloud.com  | Mogua Engine V2  |
| https://data-dre.push.dbankcloud.com  | Mogua Engine V2  |
| https://data-drru.push.dbankcloud.com  | Mogua Engine V2  |
| https://store-drcn.hispace.dbankcloud.cn/hwmarket/api/  | Mogua Engine V2  |
| https://store-dra.hispace.dbankcloud.com/hwmarket/api/  | Mogua Engine V2  |
| https://store-dre.hispace.dbankcloud.com/hwmarket/api/  | Mogua Engine V2  |
| https://store-drru.hispace.dbankcloud.com/hwmarket/api/  | Mogua Engine V2  |
| https://metrics1.data.hicloud.com:6447  | Mogua Engine V2  |
| https://metrics-dra.dt.hicloud.com:6447  | Mogua Engine V2  |
| https://metrics5.data.hicloud.com:6447  | Mogua Engine V2  |
| https://metrics.dt.dbankcloud.ru  | Mogua Engine V2  |
| https://material.angular.io/guide/theming  | Mogua Engine V2  |
| http://cmf/zhaohu  | Mogua Engine V2  |
| http://cmf/clipboard  | Mogua Engine V2  |
| http://www.baidu.com  | Mogua Engine V2  |
| http://cmf/secureStorage  | Mogua Engine V2  |
| http://cmf/deviceInfo  | Mogua Engine V2  |
| http://cmf/keyboard  | Mogua Engine V2  |
| http://cmf/statusbar  | Mogua Engine V2  |
| http://cmf/topBarUI  | Mogua Engine V2  |
| http://g.co/ng/security  | Mogua Engine V2  |
| https://angular.io/docs/ts/latest/api/common/index/NgFor-directive.html  | Mogua Engine V2  |
| http://bit.ly/IWukam  | Mogua Engine V2  |
| http://www.w3.org/2000/svg  | Mogua Engine V2  |
| http://www.w3.org/1999/xhtml  | Mogua Engine V2  |
| http://www.w3.org/1999/xlink  | Mogua Engine V2  |
| http://www.w3.org/XML/1998/namespace  | Mogua Engine V2  |
| http://www.w3.org/2000/xmlns/  | Mogua Engine V2  |
| http://central.jaf.cmbchina.cn:80/artifactory/api/npm/group-npm/@za30/zhaohu-im/-/@za30/zhaohu-im-1.9.24.tgz  | Mogua Engine V2  |
| http://a  | Mogua Engine V2  |
| http://a/c%20d  | Mogua Engine V2  |
| https://market.cmbchina.com/MPage/online/210910112740454/cmbhk.html  | Mogua Engine V2  |
| http://cmbls/functionjump  | Mogua Engine V2  |
| https://cmb-index.weijuju.com/4/index.html  | Mogua Engine V2  |
| https://www.baidu.com  | Mogua Engine V2  |
| https://market.cmbchina.com/MPage/online/210910112740454/cmbhk.html  | Mogua Engine V2  |
| https://market.cmbchina.com/personal/webapp/html/docs/license/service-detail.html  | Mogua Engine V2  |
| https://market.cmbchina.com/MPage/online/210806152450230/vtef.html  | Mogua Engine V2  |
| https://market.cmbchina.com/MPage/online/210910112740454/cmbhk.html  | Mogua Engine V2  |

### **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: True 找到 1 个唯一证书 主题: C=China, ST=Hong Kong, L=Hong Kong, O=CMB, OU=CMBHK, CN=CMB Hong Kong 签名算法: rsassa\_pkcs1v15 有效期自: 2019-05-06 00:57:06+00:00 有效期至: 2044-04-29 00:57:06+00:00 发行人: C=China, ST=Hong Kong, L=Hong Kong, O=CMB, OU=CMBHK, CN=CMB Hong Kong 序列号: 0x786ec7ce 哈希算法: sha256 md5值: fbe455aaca685d49fd3dbee6c8150cc0 sha1值: 47796999a6baa19bd5cce742d15f99534b6a2c26 sha256值: f1f7ce78028897015c42c0f2be82f4bd3ac6e451fd167061246cc18c52cfe84c sha512值: b0f5ee36d99f0a9fc0d1525094c5ce1f2e42acb0b70f1ea5d60072cae3cbd22bfac934e0effca6ee4a6f5105a68c230a82593ed91fded7129bcf1015bcf5e98f 公钥算法: rsa 密钥长度: 2048 指纹: 87f82e87136390c9559321325a07957933761192faa3b26cfda27c77756a7a56**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "bank\_auth\_cancel" : "授权取消"  |
| "bank\_auth\_failed" : "授权失败"  |
| "bank\_auth\_param\_null" : "传入参数为空"  |
| "bank\_auth\_waiting" : "正在授权，请耐心等待"  |
| "cancel\_more\_auth" : "取消"  |
| "face\_authorized\_msg" : "拒绝人脸识别验证将会无法继续操作，确定拒绝吗？"  |
| "keyboard\_secret" : "配置安全键盘密钥"  |
| "keyboard\_secret\_info" : "自定义安全键盘密钥不能为空"  |
| "login\_bank\_auth" : "招商银行App快捷登录"  |
| "login\_netcom\_password" : "一网通密码"  |
| "login\_pwd" : "密码登录"  |
| "login\_retry\_password" : "重试密码登录"  |
| "login\_risk\_password" : "为了您的信息安全，请进行登录密码验证"  |
| "more\_auth\_btn" : "切换账号或登录方式"  |
| "more\_auth\_verify\_btn" : "更多"  |
| "netcom\_bio\_login\_auth\_failed" : "指纹验证失败，请稍后重试"  |
| "netcom\_bio\_login\_bff\_auth\_failed" : "指纹已失效，请采用其他方式登录成功后重新设置"  |
| "netcom\_login\_auth\_page\_title" : "登录认证"  |
| "safe\_keyboard\_secret\_title" : "请输入安全键盘密钥"  |
| "keyboard\_secret" : "配置安全鍵盤密鑰"  |
| "keyboard\_secret\_info" : "自定義安全鍵盤密鑰不能為空"  |
| "safe\_keyboard\_secret\_title" : "請輸入安全鍵盤密鑰"  |
| "keyboard\_secret" : "配置安全键盘密钥"  |
| "keyboard\_secret\_info" : "自定义安全键盘密钥不能为空"  |
| "safe\_keyboard\_secret\_title" : "请输入安全键盘密钥"  |

## **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.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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| android.permission.READ\_PRIVILEGED\_PHONE\_STATE | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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.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.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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.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 |
| com.cmbchina.mbankhk.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.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.ACCESS\_BACKGROUND\_LOCATION | 危险 | 后台访问位置 | 允许应用程序在后台访问位置 |
| 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.USE\_BIOMETRIC | 正常 |  | 允许应用使用设备支持的生物识别模式。 |
| android.permission.CHANGE\_WIFI\_MULTICAST\_STATE | 正常 | 允许Wi-Fi多播接收  | 允许应用程序接收不是直接发送到您设备的数据包。这在发现附近提供的服务时很有用。它比非多播模式使用更多的功率 |
| 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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| com.huawei.pushagent.permission.RICHMEDIA\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| 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.huawei.android.launcher.permission.READ\_SETTINGS | 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.huawei.android.launcher.permission.WRITE\_SETTINGS | 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.huawei.launcher3.permission.WRITE\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| com.huawei.launcher3.permission.READ\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| com.huawei.launcher2.permission.READ\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| com.huawei.launcher2.permission.WRITE\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| com.huawei.launcher.permission.READ\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| com.huawei.launcher.permission.WRITE\_SETTINGS | 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.BLUETOOTH\_ADMIN | 正常 | 蓝牙管理 | 允许应用程序发现和配对蓝牙设备。  |
| com.sec.android.provider.badge.permission.READ | 正常 | 在应用程序上显示通知计数 | 在三星手机的应用程序启动图标上显示通知计数或徽章。 |
| com.sec.android.provider.badge.permission.WRITE | 正常 | 在应用程序上显示通知计数 | 在三星手机的应用程序启动图标上显示通知计数或徽章。 |
| com.htc.launcher.permission.READ\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在 htc 手机的应用程序启动图标上显示通知计数或徽章。 |
| com.htc.launcher.permission.UPDATE\_SHORTCUT | 正常 | 在应用程序上显示通知计数 | 在 htc 手机的应用程序启动图标上显示通知计数或徽章。 |
| com.sonyericsson.home.permission.BROADCAST\_BADGE | 正常 | 在应用程序上显示通知计数 | 在索尼手机的应用程序启动图标上显示通知计数或徽章。 |
| com.sonymobile.home.permission.PROVIDER\_INSERT\_BADGE | 正常 | 在应用程序上显示通知计数 | 在索尼手机的应用程序启动图标上显示通知计数或徽章。 |
| com.anddoes.launcher.permission.UPDATE\_COUNT | 正常 | 在应用程序上显示通知计数 | 在应用程序启动图标上显示通知计数或徽章 |
| com.majeur.launcher.permission.UPDATE\_BADGE | 正常 | 在应用程序上显示通知计数 | 在应用程序启动图标上显示通知计数或标记为固体。 |
| com.oppo.launcher.permission.READ\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在oppo手机的应用程序启动图标上显示通知计数或徽章。 |
| com.oppo.launcher.permission.WRITE\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在oppo手机的应用程序启动图标上显示通知计数或徽章。 |
| com.meizu.flyme.push.permission.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.cmbchina.mbankhk.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.cmbchina.mbankhk.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.vivo.notification.permission.BADGE\_ICON | 未知 | Unknown permission | Unknown permission from android reference |
| com.cmbchina.mbankhk.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| com.cmbchina.mbankhk.permission.PUSH\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| com.huawei.appmarket.service.commondata.permission.GET\_COMMON\_DATA | 未知 | Unknown permission | Unknown permission from android reference |
| com.meizu.flyme.permission.PUSH | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.cmbchina.cmf.plugins.netcom.banklogin.ReceiveDataActivity | **Schemes**: cmfdemo://,  |

**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。**