MoGua

国家反诈中心 2.0.14.APK 分析报告

APP名称:	国家反诈中心

包名:	com.hicorenational.antifraud
域名线索:	15条
URL线索:	4条
邮箱线索:	1条
分析日期:	2025年6月10日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: com.hicorenational.antifraud_2.0.14.apk
文件大小: 40.67MB
MD5值: 5396d1945aec0a1703bb36e8139a4e2f
SHA1值: 8628e85560db37e44b3184b26f98503f51bb57df
SHA256值: 0ce8a8abecbe72094270d34d35d359a9f3de826c5dec6b9dd70b3df4f08b7bc8

APP 信息

App名称: 国家反诈中心
包名: com.hicorenational.antifraud
主活动Activity: ui.activity.WelcomeActivity
安卓版本名称: 2.0.14
安卓版本: 162

域名线索

域名	服务器信息
grs.dbankcloud.eu	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 **纬度**: 34.353611 **经度**: 107.375275
data-drcn.push.dbankcloud.com	**IP**: 49.4.40.58 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572

metrics5.data.hicloud.com	**IP**: 159.138.203.215 **所属国家**: Russian Federation **地区**: Sverdlovskaya oblast' **城市**: Yekaterinburg **纬度**: 56.857498 **经度**: 60.612499
api.platform.hihonorcloud.com	**IP**: 101.42.129.17 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
data-drru.push.dbankcloud.com	**IP**: 159.138.202.31 **所属国家**: Russian Federation **地区**: Sverdlovskaya oblast' **城市**: Yekaterinburg **纬度**: 56.857498 **经度**: 60.612499
grs.dbankcloud.cn	**IP**: 121.36.116.8 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
metrics-dra.dt.hicloud.com	**IP**: 94.74.88.100 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
metrics5.dt.dbankcloud.ru	**IP**: 159.138.203.215 **所属国家**: Russian Federation **地区**: Sverdlovskaya oblast' **城市**: Yekaterinburg

	纬度: 56.857498 **经度**: 60.612499
data-dra.push.dbankcloud.com	**IP**: 119.8.163.189 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
metrics2.data.hicloud.com	**IP**: 80.158.38.48 **所属国家**: Germany **地区**: Schleswig-Holstein **城市**: Kiel **纬度**: 54.321358 **经度**: 10.134532
data-dre.push.dbankcloud.com	**IP**: 80.158.49.244 **所属国家**: Germany **地区**: Schleswig-Holstein **城市**: Kiel **纬度**: 54.321358 **经度**: 10.134532
metrics1-drcn.dt.dbankcloud.cn	**IP**: 111.202.17.12 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
grs.dbankcloud.asia	**IP**: 49.4.40.185 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
grs.platform.dbankcloud.ru	没有服务器地理信息.

URL线索

URL信息	Url所在文件
https://api.platform.hihonorcloud.com/rest.php	Mogua Engine V1
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://metrics1-drcn.dt.dbankcloud.cn:443	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://metrics5.dt.dbankcloud.ru: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

邮箱线索

邮箱地址	所在文件
gjfzzx@cert.org 将相关材料通过邮件方式发送到gjfzzx@cert.org	Mogua Engine V1

手机线索

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: C=1, ST=1, L=1, O=1, OU=1, CN=1
签名算法: rsassa_pkcs1v15
有效期自: 2019-08-23 07:39:01+00:00
有效期至: 2044-08-16 07:39:01+00:00
发行人: C=1, ST=1, L=1, O=1, OU=1, CN=1
序列号: 0x25d84885
哈希算法: sha256
md5值: 1034c7fd488bb6eff47d8b77c32eb256
sha1值: a06b1601f720d83075dc77c9f0019bf643e671c8
sha256值: 616696297b30fd721f359ea902660a423df0bb5d647d0f68d29048df85afa721
sha512值: 2e47e7aabcef2f879c7b5ea30fe1e327ca440275e71f0b5cb6e5005cd61abc001979b9979c4ff88909bab9d1267dea5865c13df25421d2e3a46f7c2637c21531
公钥算法: rsa
密钥长度: 2048
指纹: 28d850026d67cce172210506f38f89046565cbdabccd6518ca9056a57298afcb

硬编码敏感信息

可能的敏感信息
"chkpwd_host_name" : "hnid.cloud.hihonor.com"
"login_pwd" : "登录密码长度为6-16位，不能是纯数字、字母或字符"

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

	是否		

向手机申请的权限	危险	类型	详细情况
android.permission.READ_PHONE_NUMBERS	危险		允许到设备的读访问的电话号码。这是 READ_PHONE_STATE 授予的功能的一个子集,但对即时应用程序公开
android.permission.READ_CALL_LOG	危险		允许应用程序读取用户的通话日志
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.ACCESS_NOTIFICATION_POLICY	正常		希望访问通知策略的应用程序的标记权限。
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.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.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
android.permission.SYSTEM_OVERLAY_WINDOW	未知	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_SMS	危险	接收短信	允许应用程序接收和处理 SMS 消息。恶意应用程序可能会监视您的消息或将其删除而不向您显示
android.permission.READ_SMS	危险	阅读短信或彩信	允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息

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.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.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.BROADCAST_PACKAGE_ADDED	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_CHANGED	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_INSTALL	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_REPLACED	未知	Unknown permission	Unknown permission from android reference
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序为可移动存储安装和卸载文件系统
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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.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
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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。
com.android.browser.permission.READ_HISTORY_BOOKMARKS	未知	Unknown permission	Unknown permission from android reference
android.permission.REQUEST_DELETE_PACKAGES	正常		允许应用程序请求删除包
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
android.webkit.PermissionRequest	未知	Unknown permission	Unknown permission from android reference
com.google.android.gms.permission.AD_ID	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.vivo.notification.permission.BADGE_ICON	未知	Unknown permission	Unknown permission from android reference
android.permission.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
com.hicorenational.antifraud.permission.PROCESS_PUSH_MSG	未知	Unknown permission	Unknown permission from android reference

com.hicorenational.antifraud.permission.PUSH_PROVIDER	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.hicorenational.antifraud.permission.MIPUSH_RECEIVE	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

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
ui.activity.WelcomeActivity	Schemes: a28ft4://, hicoreantif-national://, hicoregroup-national://, hicorvarfy-national://,
com.tencent.tauth.AuthActivity	Schemes: tencent101934507://,
receiver.UMMipushReceiverActivity	Schemes: agoo://, Hosts: com.hicorenational.antifraud, Paths: /thirdpush,