MoGua

掌上开户 2.0.0.150116616.APK 分析报告

APP名称:	掌上开户

包名:	com.cairh.khapp.west
域名线索:	9条
URL线索:	12条
邮箱线索:	0条
分析日期:	2025年7月7日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: xbzqzskh.apk
文件大小: 7.97MB
MD5值: 4ee7d3abc601cf623b4c23b3938488f7
SHA1值: 2b0bbc26cfa80dd190a40cd33d2500ad273f0c84
SHA256值: 72306c4cdca819b729717a5702dba6ffd76d099e06a47db786a1c8ec639aaa8c

APP 信息

App名称: 掌上开户
包名: com.cairh.khapp.west
主活动Activity: com.cairh.app.sjkh.MainActivity
安卓版本名称: 2.0.0.15011616
安卓版本: 15011616

域名线索

域名	服务器信息
loc.map.baidu.com	**IP**: 111.206.209.174 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
getbootstrap.com	**IP**: 172.67.30.148 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
sjkh.cairenhui.com	**IP**: 60.190.243.249 **所属国家**: China **地区**: Zhejiang

	城市: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
lba.baidu.com	没有服务器地理信息.
loopj.com	**IP**: 185.199.110.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
git.io	**IP**: 108.160.169.179 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
github.com	**IP**: 20.205.243.166 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
sjkh.west95582.com	**IP**: 221.11.55.188 **所属国家**: China **地区**: Shaanxi **城市**: Xi'an **纬度**: 34.258331 **经度**: 108.928612
www.videolan.org	**IP**: 213.36.253.2 **所属国家**: France **地区**: Ile-de-France **城市**: Paris **纬度**: 48.859077

	经度: 2.293486

URL线索

URL信息	Url所在文件
http://lba.baidu.com/?a=	com/baidu/location/BDLocation.java
http://loc.map.baidu.com/sdk.php	com/baidu/location/c.java
http://loc.map.baidu.com/sdk_ep.php	com/baidu/location/c.java
http://loc.map.baidu.com/user_err.php	com/baidu/location/c.java
http://loc.map.baidu.com/oqur.php	com/baidu/location/c.java
http://loc.map.baidu.com/tcu.php	com/baidu/location/c.java
http://loc.map.baidu.com/fence	com/baidu/location/au.java
http://loc.map.baidu.com/fence	com/baidu/location/a0.java
https://sjkh.cairenhui.com/uploadlog/	com/cairh/app/sjkh/util/FileUploadUtil.java
http://loopj.com/android-async-http)	com/loopj/android/http/AsyncHttpClient.java
http://getbootstrap.com)	摸瓜V2引擎
https://github.com/twbs/bootstrap/blob/master/LICENSE)	摸瓜V2引擎
http://git.io/arlzeA,	摸瓜V2引擎

sjkh.west95582.com	摸瓜V3引擎
http://www.videolan.org/x264.html	lib/armeabi/libmediautil_v6.so
http://www.videolan.org/x264.html	lib/armeabi/libmediautil_v7.so
http://www.videolan.org/x264.html	lib/x86/libmediautil_v7.so

邮箱线索

手机线索

签名证书

APK已签名
v1 签名: True
v2 签名: False
v3 签名: False
找到 1 个唯一证书
主题: C=US, O=Android, CN=Android Debug
签名算法: rsassa_pkcs1v15
有效期自: 2012-12-07 13:47:52+00:00
有效期至: 2042-11-30 13:47:52+00:00
发行人: C=US, O=Android, CN=Android Debug
序列号: 0x50c1f388
哈希算法: sha1
md5值: 6c3a9eb43c020e96b5da55e1d990b357
sha1值: 7b891a2bf4c59ba669d4f9ad2979fca741e7e0fa
sha256值: 0ec9dcb66c4e0515fb6b271dd14fb1d48a7c873d0a65adbe8ea3da49f3c03cfc
sha512值: 9d53bf22f033bb2d1c277decf6629973d1c944e7a9eb47086c13cbbc91dbb9b6c22e4d8c30841c126a012fb20080524fdd45c5d7cf016ec20632dca82b0f1958

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.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.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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.CALL_PHONE	危险	直接拨打电话号码	允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码
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_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.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.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.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_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

应用内通信