



MoGua

翰荣证券 24.07.15.APK 分析报告



APP名称:

翰荣证券

包名:	com.hrzq.hrzq
域名线索:	21条
URL线索:	24条
邮箱线索:	0条
分析日期:	2025年6月1日
分析平台:	摸瓜APK反编译平台

文件名: com.hrzq.hrzq.apk

文件大小: 63.2MB

MD5值: f48905a1e82d6cb9a0924c0944005e90

SHA1值: 10cbdb772ff595d3195e26d39bac3fbb749e9481

SHA256值: 307d6fceb960d950008c24d1d2269e536f88ec7508b8acf34b9ec1065092d292

i APP 信息

App名称: 翰荣证券

包名: com.hrzq.hrzq

主活动Activity: io.dcloud.PandoraEntry

安卓版本名称: 24.07.15

安卓版本: 240715

🔍 域名线索

域名	服务器信息
api.m.taobao.com	IP: 140.205.162.6 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
api.orzudtcua.cn	IP: 0.0.0.0 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
	IP: 172.67.152.251 所属国家: United States of America 地区: California

npms.io	城市: San Francisco 纬度: 37.775700 经度: -122.395203
www.apache.org	IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
er.dcloud.net.cn	IP: 43.142.62.113 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
m3w.cn	IP: 116.196.152.179 所属国家: China 地区: Zhejiang 城市: Jinhua 纬度: 30.013470 经度: 120.288658
at.alicdn.com	IP: 125.38.11.206 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
apis.map.qq.com	IP: 116.130.223.114 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102

www.baidu.com	IP: 110.242.68.3 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
www.google.com	IP: 199.16.158.9 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446
ns.adobe.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 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
er.dcloud.io	没有服务器地理信息.
ask.dcloud.net.cn	IP: 101.72.254.86 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717

api.rhpvnjitz.cn	IP: 0.0.0.0 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
schemas.android.com	没有服务器地理信息.
matomo.ybmall.net	没有服务器地理信息.
api.xkagcehry.cn	IP: 0.0.0.0 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
quilljs.com	IP: 172.66.43.93 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
service.dcloud.net.cn	IP: 111.229.199.57 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102

URL线索

URL信息	Url所在文件

http://ns.adobe.com/xap/1.0/\u0000	io/dcloud/common/util/ExifInterface.java
https://m3w.cn/s/	io/dcloud/common/util/ShortCutUtil.java
https://ask.dcloud.net.cn/article/282	io/dcloud/common/constant/DOMException.java
https://er.dcloud.io/sc	io/dcloud/feature/gg/dcloud/ADHandler.java
https://er.dcloud.net.cn/sc	io/dcloud/feature/gg/dcloud/ADHandler.java
https://ask.dcloud.net.cn/article/35058	io/dcloud/feature/audio/AudioRecorderMgr.java
https://ask.dcloud.net.cn/article/35627	io/dcloud/e/b/a.java
https://ask.dcloud.net.cn/article/35877	io/dcloud/e/b/a.java
https://er.dcloud.io/rv	io/dcloud/e/c/h/b.java
https://er.dcloud.net.cn/rv	io/dcloud/e/c/h/b.java
https://ask.dcloud.net.cn/article/283	io/dcloud/g/b.java
https://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifViewUtils.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextView.java
https://github.com/L-JINBIN/ApkSignatureKillerEx	bin/mt/signature/KillerApplication.java
https://ask.dcloud.net.cn/article/36199	摸瓜V1引擎
https://apis.map.qq.com/jsapi?qt=translate&type=1&points=	摸瓜V2引擎

https://apis.map.qq.com/uri/v1/routeplan?type=drive&to=	摸瓜V2引擎
https://www.google.com/maps/?daddr=	摸瓜V2引擎
https://www.google.com/maps/	摸瓜V2引擎
https://quilljs.com/	摸瓜V2引擎
https://quilljs.com	摸瓜V2引擎
https://npms.io/search?q=ponyfill.	摸瓜V2引擎
https://matomo.ybmall.net	摸瓜V2引擎
https://www.baidu.com	摸瓜V2引擎
https://\$	摸瓜V2引擎
https://api.m.taobao.com/rest/api3.do?api=mtop.common.getTimestamp	摸瓜V2引擎
https://api.rhpvnjitz.cn	摸瓜V2引擎
https://api.xkagehry.cn	摸瓜V2引擎
https://api.orzudtcua.cn	摸瓜V2引擎
https://at.alicdn.com/t/font_2225171_8kdcwk4po24.ttf)	摸瓜V2引擎
https://service.dcloud.net.cn/uniapp/feedback.html	摸瓜V2引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
https://github.com/ecomfe/zrender/blob/master/LICENSE.txt	摸瓜V2引擎

邮箱线索

手机线索

签名证书

无法读取代码签名证书.

硬编码敏感信息

可能的敏感信息
"dcloud_common_user_refuse_api" : "the user denies access to the API"
"dcloud_io_without_authorization" : "not authorized"
"dcloud_oauth_authentication_failed" : "failed to obtain authorization to log in to the authentication service"
"dcloud_oauth_empower_failed" : "the Authentication Service operation to obtain authorized logon failed"
"dcloud_oauth_logout_tips" : "not logged in or logged out"
"dcloud_oauth_oauth_not_empower" : "oAuth authorization has not been obtained"
"dcloud_oauth_token_failed" : "failed to get token"
"dcloud_permissions_reauthorization" : "reauthorize"
"dcloud_common_user_refuse_api" : "用户拒绝该API访问"

"dcloud_io_without_authorization" : "没有获得授权"
"dcloud_oauth_authentication_failed" : "获取授权登录认证服务操作失败"
"dcloud_oauth_empower_failed" : "获取授权登录认证服务操作失败"
"dcloud_oauth_logout_tips" : "未登录或登录已注销"
"dcloud_oauth_oauth_not_empower" : "尚未获取oauth授权"
"dcloud_oauth_token_failed" : "获取token失败"
"dcloud_permissions_reauthorization" : "重新授权"

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.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.READ_MEDIA_IMAGES	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.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.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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.GET_ACCOUNTS	危险	列出帐户	允许访问账户服务中的账户列表

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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.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.READ_MEDIA_VISUAL_USER_SELECTED	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
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

应用内通信

活动(ACTIVITY)	通信(INTENT)
...	Schemes: hbuilder://,

io.dcloud.PandoraEntry	Mime Types: image/*,
io.dcloud.PandoraEntryActivity	Schemes: ://,

报告由 [摸瓜APK反编译平台](#) 自动生成，并非包含所有检测结果，有疑问请联系管理员。