



MoGua

Invesco 1.0.APK 分析报告



APP名称:

Invesco

包名:	plus.H5D24C780
域名线索:	24条
URL线索:	36条
邮箱线索:	2条
分析日期:	2025年6月12日
分析平台:	摸瓜APK反编译平台

文件名: Invesco.apk
文件大小: 66.76MB
MD5值: 5dee4fe1babb63765803e988b06ff87e
SHA1值: 1f5ea5de49a577a5e99065f4c9b22e4a425d06fe
SHA256值: 28e65d48ba05e03b7fea68148ccebad055f4b454a09dd9bbad69bb700f38c64e

i APP 信息

App名称: Invesco
包名: plus.H5D24C780
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 1.0
安卓版本: 100

🔍 域名线索

域名	服务器信息
raw.githubusercontent.com	IP: 185.199.108.133 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
ethstats.net	没有服务器地理信息.
example.com	IP: 96.7.128.198 所属国家: United States of America 地区: California 城市: El Segundo 纬度: 33.919201 经度: -118.416580

imchat.wejnkvs.xyz	IP: 0.0.0.0 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
avatars.githubusercontent.com	IP: 185.199.108.133 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
github.com	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
feross.org	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
bsc-mainnet.nodereal.io	IP: 15.197.203.147 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199
eips.ethereum.org	IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647

	经度: -79.891724
fontawesome.comn	没有服务器地理信息.
www.rinkeby.io	没有服务器地理信息.
m3w.cn	IP: 116.196.151.14 所属国家: China 地区: Zhejiang 城市: Jinhua 纬度: 30.013470 经度: 120.288658
kovan-testnet.github.io	IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
fontawesome.com	IP: 104.18.22.52 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
fonts.googleapis.com	IP: 114.250.69.33 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
ns.adobe.com	没有服务器地理信息.
	IP: 15.197.167.90 所属国家: United States of America

vuejs.org	地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199
er.dcloud.io	没有服务器地理信息.
api.wejnkvs.xyz	IP: 154.12.20.134 所属国家: United States of America 地区: Arizona 城市: Phoenix 纬度: 33.448231 经度: -112.074051
ask.dcloud.net.cn	IP: 220.194.123.111 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
schemas.android.com	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
er.dcloud.net.cn	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
links.ethers.org	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000

	经度: 0.000000
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

 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/p/r.java
https://ask.dcloud.net.cn/article/35877	io/dcloud/p/r.java
https://ask.dcloud.net.cn/article/283	io/dcloud/p/h1.java
https://er.dcloud.io/rv	io/dcloud/p/d0.java

https://er.dcloud.net.cn/rv	io/dcloud/p/d0.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://ask.dcloud.net.cn/article/36199	摸瓜V1引擎
https://api.wejnkvs.xyz ,	摸瓜V2引擎
https://avatars.githubusercontent.com ,	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://bsc-mainnet.nodereal.io/v1/1f653eb20ddd495cb007f9c67f87c4c4	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://vuejs.org/error-reference/	摸瓜V2引擎
https://feross.org/opensource >	摸瓜V2引擎
https://feross.org >	摸瓜V2引擎
https://raw.githubusercontent.com/stefanpenner/es6-promise/master/LICENSE	摸瓜V2引擎
https://fontawesome.com \n	摸瓜V2引擎
https://fontawesome.com/license/free	摸瓜V2引擎
https://bsc-mainnet.nodereal.io/v1/1f653eb20ddd495cb007f9c67f87c4c4	摸瓜V2引擎

https://github.com/zloirock/core-js/blob/v3.39.0/LICENSE	摸瓜V2引擎
https://github.com/zloirock/core-js	摸瓜V2引擎
https://a	摸瓜V2引擎
https://a/c%20d?a=1&c=3	摸瓜V2引擎
https://a@b	摸瓜V2引擎
https://x	摸瓜V2引擎
https://github.com/systemjs/systemjs/blob/main/docs/errors.md	摸瓜V2引擎
https://imchat.wejnkvds.xyz/index/index/home?	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://fonts.googleapis.com/css2?family=Noto+Sans+SC:wght@100..900&display=swap	摸瓜V2引擎
https://vuejs.org/error-reference/	摸瓜V2引擎
https://feross.org/opensource >	摸瓜V2引擎
https://feross.org >	摸瓜V2引擎
https://raw.githubusercontent.com/stefanpenner/es6-promise/master/LICENSE	摸瓜V2引擎

https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://links.ethers.org/v5-errors-	摸瓜V2引擎
https://github.com/crypto-browserify/crypto-browserify	摸瓜V2引擎
https://example.com	摸瓜V2引擎
https://github.com/uuidjs/uuid	摸瓜V2引擎
https://github.com/goerli/testnet	摸瓜V2引擎
https://kovan-testnet.github.io/website/	摸瓜V2引擎
https://ethstats.net/	摸瓜V2引擎
https://www.rinkeby.io	摸瓜V2引擎
https://github.com/ethereum/ropsten	摸瓜V2引擎
https://github.com/ethereum/go-ethereum/pull/23730	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-1153	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-1559	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-2315	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-2537	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-2565	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-2718	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-2929	摸瓜V2引擎

https://eips.ethereum.org/EIPS/eip-2930	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-3198	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-3529	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-3540	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-3541	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-3607	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-3651	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-3670	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-3675	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-3855	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-3860	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-4345	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-4399	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-5133	摸瓜V2引擎
https://github.com/ethereum/execution-specs/blob/master/network-upgrades/mainnet-upgrades/arrow-glacier.md	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-2070	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-609	摸瓜V2引擎

https://eips.ethereum.org/EIPS/eip-1013	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-779	摸瓜V2引擎
https://github.com/ethereum/execution-specs/blob/master/network-upgrades/mainnet-upgrades/gray-glacier.md	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-606	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-1679	摸瓜V2引擎
https://github.com/ethereum/eth1.0-specs/blob/master/network-upgrades/mainnet-upgrades/london.md	摸瓜V2引擎
https://github.com/ethereum/execution-specs/blob/master/network-upgrades/mainnet-upgrades/merge.md	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-2384	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-1716	摸瓜V2引擎
https://github.com/ethereum/pm/issues/356	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-607	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-608	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://github.com/zloirock/core-js/blob/v3.39.0/LICENSE	摸瓜V2引擎
https://github.com/zloirock/core-js	摸瓜V2引擎
https://a	摸瓜V2引擎
https://a/c%20d?a=1&c=3	摸瓜V2引擎
https://a@b	摸瓜V2引擎

https://x	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://links.ethers.org/v5-errors-	摸瓜V2引擎
https://github.com/crypto-browserify/crypto-browserify	摸瓜V2引擎
https://example.com	摸瓜V2引擎
https://github.com/uuidjs/uuid	摸瓜V2引擎
https://github.com/goerli/testnet	摸瓜V2引擎
https://kovan-testnet.github.io/website/	摸瓜V2引擎
https://ethstats.net/	摸瓜V2引擎
https://www.rinkeby.io	摸瓜V2引擎
https://github.com/ethereum/ropsten	摸瓜V2引擎
https://github.com/ethereum/go-ethereum/pull/23730	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-1153	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-1559	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-2315	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-2537	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-2565	摸瓜V2引擎

https://eips.ethereum.org/EIPS/eip-2718	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-2929	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-2930	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-3198	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-3529	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-3540	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-3541	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-3607	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-3651	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-3670	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-3675	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-3855	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-3860	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-4345	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-4399	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-5133	摸瓜V2引擎
https://github.com/ethereum/execution-specs/blob/master/network-upgrades/mainnet-upgrades/arrow-glacier.md	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-2070	摸瓜V2引擎

https://eips.ethereum.org/EIPS/eip-609	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-1013	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-779	摸瓜V2引擎
https://github.com/ethereum/execution-specs/blob/master/network-upgrades/mainnet-upgrades/gray-glacier.md	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-606	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-1679	摸瓜V2引擎
https://github.com/ethereum/eth1.0-specs/blob/master/network-upgrades/mainnet-upgrades/london.md	摸瓜V2引擎
https://github.com/ethereum/execution-specs/blob/master/network-upgrades/mainnet-upgrades/merge.md	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-2384	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-1716	摸瓜V2引擎
https://github.com/ethereum/pm/issues/356	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-607	摸瓜V2引擎
https://eips.ethereum.org/EIPS/eip-608	摸瓜V2引擎
https://imchat.wejnkvs.xyz/index/index/home?	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎

 邮箱线索

邮箱地址	所在文件
ohjlef6w26qoe4vtudpe@all.goerli ohjlef6w26qoe4vtudpe@all.mainnet ohjlef6w26qoe4vtudpe@all.rinkeby ohjlef6w26qoe4vtudpe@all.ropsten	摸瓜V2引擎
ohjlef6w26qoe4vtudpe@all.goerli ohjlef6w26qoe4vtudpe@all.mainnet ohjlef6w26qoe4vtudpe@all.rinkeby ohjlef6w26qoe4vtudpe@all.ropsten	摸瓜V2引擎

 手机线索

手机号	所在文件
19919152923	摸瓜V2引擎
17179869184	摸瓜V2引擎
19919152923	摸瓜V2引擎
17179869184	摸瓜V2引擎

 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=cn, ST=四川省成都市, L=成都, O=agl科技, OU=agl科技, CN=s
签名算法: rsassa_pkcs1v15
有效期自: 2024-12-14 04:12:43+00:00
有效期至: 2124-11-20 04:12:43+00:00
发行人: C=cn, ST=四川省成都市, L=成都, O=agl科技, OU=agl科技, CN=s
序列号: 0x595fbd91
哈希算法: sha256
md5值: 16f9d5f8b322f46c136553840ea85054
sha1值: 6edd1263af52524e4c7f2850d07c42eb1494c8bb
sha256值: 2d243ded05142a81cfe834d803e47eb7e0449d2cd37b6c8946a1d9bed5f8b7de
sha512值: d31c86d49a1e52b1d483b288a0fb10fac85110e0b1648da039ff4084daad3271424e91413a8dc9cafd3cbc262b9d38501010f0a729f9b9ca190c5ed3f22f1ed
公钥算法: rsa
密钥长度: 1024
指纹: c2f528d459d38f1924482b6c707c75cbabdaa3bdc67e925afe6c3d7bb1e3aa27

 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_tips_certificate" : "certificate"
"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"
"dcloud_tips_certificate" : "证书"

 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.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_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.READ_MEDIA_VISUAL_USER_SELECTED	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.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
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.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_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
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
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.INSTALL_PACKAGES	系统需要	直接安装应用程序	允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序
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.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.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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.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.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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.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。

应用内通信

活动(ACTIVITY)	通信(INTENT)
io.dcloud.PandoraEntry	Schemes: h5d24c780://,