MoGua

CoinMetro 4.7.6.APK 分析报告

APP名称: CoinMetro

包名:	uni.UNI60DF751
域名线索:	9条
URL线索:	60条
邮箱线索:	13条
分析日期:	2024年11月7日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: Coinmetro.apk
文件大小: 33.38MB
MD5值: c24320aad02fc88c7ba9314d99d030c8
SHA1值: 818f683f15ee3fb83619615adf3d357e6b897bfe
SHA256值: 71bfebdca3bdba320cbfbdb29270d89813cf3be51e6a0fe7e89f313c1e8f3d95

APP 信息

App名称: CoinMetro
包名: uni.UNI60DF751
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 4.7.6
安卓版本: 5160

域名线索

域名	服务器信息
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.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
service.dcloud.net.cn	**IP**: 42.192.39.19 **所属国家**: China **地区**: Beijing

	城市: Beijing **纬度**: 39.907501 **经度**: 116.397102
www.google.com	**IP**: 31.13.94.36 **所属国家**: Argentina **地区**: Ciudad Autonoma de Buenos Aires **城市**: Buenos Aires **纬度**: -34.603600 **经度**: -58.381554
api.coingold.net	**IP**: 172.66.42.231 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
ask.dcloud.net.cn	**IP**: 116.196.150.32 **所属国家**: China **地区**: Zhejiang **城市**: Jinhua **纬度**: 30.013470 **经度**: 120.288658
bit.ly	**IP**: 67.199.248.10 **所属国家**: United States of America **地区**: New York **城市**: New York City **纬度**: 40.750134 **经度**: -73.997009
api.hflgc.com	**IP**: 154.82.100.62 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
	IP: 172.66.40.163

quilljs.com	**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
https://ask.dcloud.net.cn/article/36199	摸瓜V1引擎
https://bit.ly/2ZqJzkp	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.coingold.net/api/v1/depth	摸瓜V2引擎
https://api.coingold.net/api/v1/aggTrades	摸瓜V2引擎
https://api.coingold.net/api/v1/depth?symbol=	摸瓜V2引擎
https://service.dcloud.net.cn/uniapp/feedback.html	摸瓜V2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://quilljs.com	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎

https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.coingold.net/api/v1/depth?symbol=	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.coingold.net/api/v1/depth?symbol=	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎

https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.coingold.net/api/v1/depth?symbol=	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.coingold.net/api/v1/depth?symbol=	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.coingold.net/api/v1/depth?symbol=	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.coingold.net/api/v1/depth?symbol=	摸瓜V2引擎

https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.coingold.net/api/v1/depth?symbol=	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.coingold.net/api/v1/depth?symbol=	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.coingold.net/api/v1/depth?symbol=	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.coingold.net/api/v1/depth?symbol=	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎
https://api.coingold.net/api/v1/depth?symbol=	摸瓜V2引擎
https://api.hflgc.com/api/user/	摸瓜V2引擎

邮箱线索

邮箱地址	所在文件
touxiang@2x.png	摸瓜V2引擎
reli@2x.png fanhui@2x.png	摸瓜V2引擎
touxiang@2x.png	摸瓜V2引擎
reli@2x.png	摸瓜V2引擎
logo@2x.png	摸瓜V2引擎
touxiang@2x.png huiyuanjibie@2x.png	摸瓜V2引擎
kapian@2x.png	摸瓜V2引擎
reli@2x.png fanhui@2x.png	摸瓜V2引擎
reli@2x.png fanhui@2x.png	摸瓜V2引擎
reli@2x.png fanhui@2x.png	摸瓜V2引擎
reli@2x.png	摸瓜V2引擎
reli@2x.png fanhui@2x.png	摸瓜V2引擎
bg@2x.png	摸瓜V2引擎

手机线索

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=8dbb4aa1, ST=8dbb4aa1, L=8dbb4aa1, O=8dbb4aa1, OU=8dbb4aa1, CN=8dbb4aa1
签名算法: rsassa_pkcs1v15
有效期自: 2024-09-01 11:02:40+00:00
有效期至: 2124-08-08 11:02:40+00:00
发行人: C=8dbb4aa1, ST=8dbb4aa1, L=8dbb4aa1, O=8dbb4aa1, OU=8dbb4aa1, CN=8dbb4aa1
序列号: 0x3dc1ba57
哈希算法: sha256
md5值: 0ea17eeab5ddeab1a6201dda3a0249f5
sha1值: b76ab4c8e2c3e1c17c76e4e8a58c50c8da2da3b3
sha256值: 61ec5c82dbfe7ef23c22621324f4ff728fbf884301dceb4f801ef564483fc48f
sha512值: 3fa1eae4f50d72bbe2e253fa93eac26f1776aabccf25f28d97e00e669d0f27f50eccd625265bb8d13c13565aa73e03bfcd09481c1d07851f16cde33675509d7d
公钥算法: rsa
密钥长度: 1024
指纹: b6b1c0391288a221324cbc495acbb21e0c8f67d5251533a52c574a62ef598d51

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_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_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_IMAGES	未知	Unknown permission	Unknown permission from android reference
		Unknown	

android.permission.READ_MEDIA_VIDEO	未知	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
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.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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器

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.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
