MoGua

测智网 4.1.APK 分析报告

APP名称:	测智网

包名:	plus.H58F5A77A
域名线索:	8条
URL线索:	17条
邮箱线索:	0条
分析日期:	2025年6月8日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: base.apk
文件大小: 4.41MB
MD5值: f4b488ef7bc4b5d92433d81343ec8947
SHA1值: dd8aa38a8c7526b58ff010a6c6902dd54207e995
SHA256值: 8885d5aef9e878f9276b5e287f03a07711458c80f20403d17a739fb4ff1eae2f

APP 信息

App名称: 测智网
包名: plus.H58F5A77A
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 4.1
安卓版本: 410

域名线索

域名	服务器信息
stream.dcloud.net.cn	**IP**: 43.142.22.58 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
ask.dcloud.net.cn	**IP**: 123.125.244.81 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
schemas.android.com	**IP**: 127.0.0.1 **所属国家**: - **地区**: -

	城市: - **纬度**: 0.000000 **经度**: 0.000000
ns.adobe.com	没有服务器地理信息.
iqeq.com.cn	**IP**: 121.40.22.124 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com	没有服务器地理信息.
stream.mobihtml5.com	没有服务器地理信息.
m3w.cn	**IP**: 119.167.249.90 **所属国家**: China **地区**: Shandong **城市**: Qingdao **纬度**: 36.098610 **经度**: 120.371941

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
http://m3w.cn/s/	io/dcloud/common/util/ShortCutUtil.java
https://stream.mobihtml5.com/	io/dcloud/common/constant/StringConst.java

https://stream.dcloud.net.cn/	io/dcloud/common/constant/StringConst.java
http://ask.dcloud.net.cn/article/282	io/dcloud/common/constant/DOMException.java
https://ask.dcloud.net.cn/article/35058	io/dcloud/feature/audio/AudioRecorderMgr.java
https://96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com/http/splash-screen/report	io/dcloud/feature/gg/dcloud/ADHandler.java
http://ask.dcloud.net.cn/article/283	io/dcloud/h/b.java
https://ask.dcloud.net.cn/article/35627	io/dcloud/f/b/a.java
https://ask.dcloud.net.cn/article/35877	io/dcloud/f/b/a.java
https://96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com/http/rewarded-video/report?p=a&t=	io/dcloud/f/c/h/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://ask.dcloud.net.cn/article/36199	摸瓜V1引擎
https://iqeq.com.cn/yhxx2.html\	摸瓜V2引擎
https://iqeq.com.cn/yszc2.html\	摸瓜V2引擎

邮箱线索

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=china, ST=sz, L=sz, O=hdrj, OU=hdrj, CN=guan
签名算法: rsassa_pkcs1v15
有效期自: 2022-11-29 08:39:18+00:00
有效期至: 2122-11-05 08:39:18+00:00
发行人: C=china, ST=sz, L=sz, O=hdrj, OU=hdrj, CN=guan
序列号: 0x248e6c75
哈希算法: sha256
md5值: 3bdd65b2b2b7dc8d491e2d22faa09a4d
sha1值: 3d43285b83c861db8d0c4ad99af3b15c14fbb23b
sha256值: 84adfaf4892e54f70d3d2e92a9374888c300044e739d0038cde3e565af25373a
sha512值: 981664b86d88f64508f35a3cee4e616b9dd51de2a9e73aed5aa0742fb72b2372a297064bf7ab1e5ff135d437629d9c8a17e2af4b720b4180237c9422c4d32781
公钥算法: rsa
密钥长度: 2048
指纹: 460b8986172684d193eec084f626ecff2e6a3df6d0f10f33d9fe3bb7414c818c

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.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.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.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。
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

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
io.dcloud.PandoraEntry	Schemes: h58f5a77a://,
