

APP线索分析报告

报告由模MAPP分析平台(mogua.co)生成



♣ 艾多特护眼专家 1.0.APK

APP名称: 艾多特护眼专家

包名: com.huyanzhuanjia

域名线索: 9条

URL线索: 39条

邮箱线索: 0条

分析日期: 2022年1月18日 23:09

文件名: c62615ad23cae5da46cfe2b4f76b5bc0.apk

文件大小: 3.74MB

MD5值: c62615ad23cae5da46cfe2b4f76b5bc0

SHA1值: 0cb138a8a1c45ca7a6b9544114ec0409d41f7637

SHA256值: c832e18ad90b73a3e7f1dc10f760600060b75ad19aafdce1976ce98d310103de

i APP 信息

App名称: 艾多特护眼专家 包名: com.huyanzhuanjia

主活动**Activity:** io.dcloud.PandoraEntry

安卓版本名称: 1.0 安卓版本: 100

0 域名线索

域名	是否危险域名	服务器信息
open.weixin.qq.com	good	IP: 109.244.144.48 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map
stream.mobihtml5.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com	good	IP: 47.93.95.208 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
stream.dcloud.net.cn	good	IP : 118.31.103.188 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 査看地图: Google Map
schemas.android.com	good	没有服务器地理信息.
service.dcloud.net.cn	good	IP: 120.26.1.80 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
long.open.weixin.qq.com	good	IP: 109.244.217.35 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map

域名	是否危险域名	服务器信息
ask.dcloud.net.cn	good	IP: 124.239.227.208 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717 查看地图: Google Map
m3w.cn	good	IP: 222.85.26.221 所属国家: China 地区: Henan 城市: Zhengzhou 纬度: 34.757778 经度: 113.648613 查看地图: Google Map

₩URL线索

URL信息	Url所在文件
https://open.weixin.qq.com/connect/sdk/qrconnect? appid=%s&noncestr=%s×tamp=%s&scope=%s&signature=%s	com/tencent/mm/opensdk/diffdev/a/b.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/opensdk/diffdev/a/c.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

URL信息	Url所在文件
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifViewUtils.java
http://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/287	io/dcloud/share/IFShareApi.java
http://ask.dcloud.net.cn/article/283	io/dcloud/i/b.java
http://m3w.cn/s/	io/dcloud/common/util/ShortCutUtil.java
http://ask.dcloud.net.cn/article/282	io/dcloud/common/constant/DOMException.java
https://stream.mobihtml5.com/	io/dcloud/common/constant/StringConst.java
https://stream.dcloud.net.cn/	io/dcloud/common/constant/StringConst.java
https://service.dcloud.net.cn/sta/so?p=a&pn=%s&ver=%s&appid=%s	io/dcloud/g/b/c.java
https://96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com/http/rewarded-video/report?p=a&t=	io/dcloud/g/b/h/a.java
https://ask.dcloud.net.cn/article/35627	io/dcloud/g/a/a.java
https://ask.dcloud.net.cn/article/35877	io/dcloud/g/a/a.java
https://ask.dcloud.net.cn/article/36199	Android String Resource

₩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。
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.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

向手机申请的权限	是否危险	类型	详细情况
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.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.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.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.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.RECORD_AUDIO	危 险	录音	允许应用程序访问音频记录路径

向手机申请的权限	是否危险	类型	详细情况
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。
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
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference



APK is signed v1 signature: True v2 signature: True v3 signature: True Found 1 unique certificates

Subject: C=CN, ST=SH, L=SH, O=huyanzhuanjia, OU=huyanzhuanjia, CN=huyanzhuanjia

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2021-07-27 03:38:48+00:00 Valid To: 2031-07-25 03:38:48+00:00

Issuer: C=CN, ST=SH, L=SH, O=huyanzhuanjia, OU=huyanzhuanjia, CN=huyanzhuanjia

Serial Number: 0xa656911 Hash Algorithm: sha256

md5: 54d7200d4a251a9ad2af1414367a55ef

sha1: 912a5ed37bb0eef76b245f51537b05887df81a5e

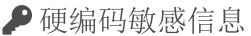
sha256: 1473b157c51256aed4410a57182a304844e49fba8453741ba8176fd07927bf0b

sha512: f43b9a3ed3ef8f5566b212ad1649a28193fa8ef69325e682ea677cce2a6e1b372b51351be899f1e6fabd3bb316478f6364f21c0fff5f43d2704772abbf528aef

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: 1667a6773d3f54f6fa6d126bf0777b961eafaac17d3873f61e2a466a9e668d4f



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"

可能的敏感信息
"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"

■应用内通信

活动(ACTIVITY)	通信(INTENT)
io.dcloud.PandoraEntry	Schemes: h5f6a11ec://,



文件列表	分析结果								
	売列表 详细情况								
classes.dex	及虚拟机 Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.BRAND check Build.PRODUCT check Build.HARDWARE check possible Build.SERIAL check SIM operator check subscriber ID check possible VM check								
	编译器 r8								

报告由 摸瓜平台 自动生成,并非包含所有检测结果,有疑问请联系管理员。

查诈骗APP | 查木马APP | 违法APP分析 | APK代码分析