

APP线索分析报告

报告由模瓜APP分析平台(mogua.co) 生成



♣ 悦己悦生活 1.0.APK

APP名称: 悦己悦生活

包名: w2a.yueshenghuojoy.cn

域名线索: 23条

URL线索: 47条

邮箱线索: 0条

分析日期: 2022年1月25日 22:58

文件名: yjysh.apk 文件大小: 4.98MB

MD5值: 99863773d34c4eed0cd6ca643227ff07

SHA1值: 4b65b3bc3921db6a61f22b0d7fb96a9e5f351f3f

\$HA256值: 8142b906f13a503f173518c147f589abb80ad059d6538bc41f23358da5c0ab54

i APP 信息

App名称: 悦己悦生活

包名: w2a.yueshenghuojoy.cn

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

安卓版本名称: 1.0 安卓版本: 8

0 域名线索

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

域名	是否危险域名	服务器信息
mobilegw.alipay.com	good	IP: 203.209.255.248 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
api.weixin.qq.com	good	IP: 109.244.145.152 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
m.alipay.com	good	IP: 203.209.245.74 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
mcgw.alipay.com	good	IP: 203.209.250.50 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

域名	是否危险域名	服务器信息
mclient.alipay.com	good	IP: 203.209.250.50 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
loggw-exsdk.alipay.com	good	IP: 110.75.134.9 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
mobilegw.aaa.alipay.net	good	没有服务器地理信息.
mobilegw.alipaydev.com	good	IP: 110.75.132.131 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
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

域名	是否危险域名	服务器信息
render.alipay.com	good	IP: 140.249.240.248 所属国家: China 地区: Shandong 城市: Qingdao 纬度: 36.098610 经度: 120.371941 查看地图: Google Map
service.dcloud.net.cn	good	IP: 47.97.36.120 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
wappaygw.alipay.com	good	IP: 203.209.250.6 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: 109.244.216.15 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
h5.m.taobao.com	good	IP: 140.249.89.233 所属国家: China 地区: Shandong 城市: Jinan 纬度: 36.668331 经度: 116.997223 查看地图: Google Map
mobilegw-1-64.test.alipay.net	good	没有服务器地理信息.
schemas.android.com	good	没有服务器地理信息.
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 查看地图: Google Map
m3w.cn	good	IP: 125.37.206.223 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142220 经度: 117.176666 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: 222.85.26.232 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
mobilegw.stable.alipay.net	good	没有服务器地理信息.
stream.mobihtml5.com	good	没有服务器地理信息.
xmlpull.org	good	IP: 74.50.61.58 所属国家: United States of America 地区: Texas 城市: Dallas 纬度: 32.814899 经度: -96.879204 查看地图: Google Map

URL线索

URL信息	Url所在文件
https://render.alipay.com/p/s/i?scheme=%s	com/alipay/sdk/app/OpenAuthTask.java
https://wappaygw.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
http://wappaygw.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java

URL信息	Url所在文件
https://mclient.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/home/exterfaceAssign.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/home/exterfaceAssign.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/cashier/mobilepay.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/cashier/mobilepay.htm	com/alipay/sdk/app/PayTask.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/sdk/cons/a.java
https://mobilegw.alipaydev.com/mgw.htm	com/alipay/sdk/cons/a.java
https://mcgw.alipay.com/sdklog.do	com/alipay/sdk/cons/a.java
https://loggw-exsdk.alipay.com/loggw/logUpload.do	com/alipay/sdk/cons/a.java
http://m.alipay.com/?action=h5quit	com/alipay/sdk/cons/a.java
https://wappaygw.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/cons/a.java
https://mclient.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/cons/a.java
https://h5.m.taobao.com/mlapp/olist.html	com/alipay/sdk/data/a.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java

URL信息	Url所在文件
http://mobilegw.aaa.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw-1-64.test.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw.stable.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
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://xmlpull.org/v1/doc/features.html#indent-output	com/ta/utdid2/core/persistent/XmlUtils.java
http://xmlpull.org/v1/doc/features.html#indent-output	com/ta/utdid2/core/persistent/FastXmlSerializer.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
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/ad/dcloud/ADHandler.java
https://api.weixin.qq.com/sns/auth?access_token=%s&openid=%s	io/dcloud/feature/oauth/weixin/WeiXinOAuthService.java
https://api.weixin.qq.com/sns/oauth2/access_token? appid=%s&secret=%s&code=%s&grant_type=authorization_code	io/dcloud/feature/oauth/weixin/WeiXinOAuthService.java
https://api.weixin.qq.com/sns/userinfo?access_token=%s&openid=%s⟨=zh_CN	io/dcloud/feature/oauth/weixin/WeiXinOAuthService.java

URL信息	Url所在文件
-------	---------

https://api.weixin.qq.com/sns/oauth2/refresh_token? appid=%s&grant_type=refresh_token&refresh_token=%s	io/dcloud/feature/oauth/weixin/WeiXinOAuthService.java
http://ask.dcloud.net.cn/article/283	io/dcloud/h/b.java
http://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.java
https://service.dcloud.net.cn/sta/so?p=a&pn=%s&ver=%s&appid=%s	io/dcloud/f/b/c.java
https://service.dcloud.net.cn/pdz	io/dcloud/f/b/f/a.java
https://96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com/http/rewarded-video/report?p=a&t=	io/dcloud/f/b/f/a.java
https://ask.dcloud.net.cn/article/35627	io/dcloud/f/a/a.java
https://ask.dcloud.net.cn/article/35877	io/dcloud/f/a/a.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://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

向手机申请的权限	是否危险	类型	详细情况
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
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_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

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



v1 signature: True v2 signature: True v3 signature: True

Found 1 unique certificates

Subject: C=CN, ST=BJ, L=HD, O=Android, OU=Android, CN=Android Debug

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2021-04-12 08:27:53+00:00 Valid To: 2121-03-19 08:27:53+00:00

Issuer: C=CN, ST=BJ, L=HD, O=Android, OU=Android, CN=Android Debug

Serial Number: 0x363bc393 Hash Algorithm: sha256

md5: 06838cc840093b9d4689fc419ba1a3f3

sha1: 97c84101b9141c130dd75d7428a2922518c36dcd

sha256: b01d06180d003e79c7b9088993b8e5ae7a19b0da1161aa097c7f398a6f514fa7

sha512: 67720eb20639d1f5f9c8b7b201b185ea4364f6a89bedd35aa1d273002c16d65a7739f59679510d3b96c1f2c3dd3136d9a34451cb679251a86ff4cafdc18314bf

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: b27ac6d7a4586417c251be6e44179616262379e57da2d1e19db0995be0ddf509



可能的敏感信息 "dcloud_common_user_refuse_api": "the user denies access to the API" "dcloud_feature_confusion_exception_no_key_input": "no public key input" "dcloud_feature_confusion_exception_no_private_key_input": "no private key input" "dcloud_feature_oauth_weixin_plugin_description": "wechat" "dcloud_io_without_authorization": "not authorized" "dcloud_oauth_authentication_failed": "failed to obtain authorization to log in to the authentication service"

可能的敏感信息 "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_feature_confusion_exception_no_key_input": "公钥数据为空" "dcloud_feature_confusion_exception_no_private_key_input": "私钥数据为空" "dcloud_feature_oauth_weixin_plugin_description":"微信" "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"

可能的敏感信息

"dcloud_permissions_reauthorization" : "重新授权"

你加壳分析

文件列表	分析结果	
classes.dex	意列表 详细情况 Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check Build.TAGS check SIM operator check network operator name check device ID check subscriber ID check ro.product.device check ro.kernel.qemu check emulator file check possible VM check	
	编译器 r8	

查诈骗APP | 查木马APP | 违法APP分析 | APK代码分析