MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

乡创网 0.0.24.APK

APP名称:	乡创网
包名:	com.bcreat.znzh
域名线索:	9条
URL线索:	13条
邮箱线索:	1条
分析日期:	2022年2月3日 11:20

文件信息

文件名: xaingchuanw.apk
文件大小: 8.72MB
MD5值: 5fe114cf3f0ca252b7011adbef7e4582
SHA1值: 439db9c63a3982d2300a2ba555a7c276f8b0338b
SHA256值: 8bc7d0a9492dcb5a8037ce524360f752c548ecc96ad96f2393d0961a3a645af1

APP 信息

App名称: 乡创网
包名: com.bcreat.znzh
主活动**Activity:** com.uzmap.pkg.LauncherUI
安卓版本名称: 0.0.24
安卓版本: 24

域名线索

域名	是否危险域名	服务器信息
p.apicloud.com	good	**IP:** 47.93.154.30 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
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
d.apicloud.com	good	IP: 47.94.176.24 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
a.apicloud.com	good	IP: 182.92.145.58 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
s.apicloud.com	good	没有服务器地理信息.
as.apicloud.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
r.apicloud.com	good	IP: 182.92.145.58 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.mch.weixin.qq.com	good	IP: 182.254.22.146 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298 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

URL线索

URL信息	Url所在文件
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/opensdk/diffdev/a/f.java

URL信息	Url所在文件
https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s	com/tencent/mm/opensdk/diffdev/a/d.java
https://api.mch.weixin.qq.com/pay/unifiedorder	com/uzmap/pkg/uzmodules/uzWxPay/PayTask.java
https://api.mch.weixin.qq.com/pay/unifiedorder	com/uzmap/pkg/uzmodules/uzWxPay/GetOrderIdTask.java
https://a.apicloud.com	compile/Properties.java
https://d.apicloud.com	compile/Properties.java
https://s.apicloud.com	compile/Properties.java
https://p.apicloud.com	compile/Properties.java
https://r.apicloud.com	compile/Properties.java
https://as.apicloud.com	compile/Properties.java

邮箱线索

邮箱地址	所在文件
developer@apicloud.com	com/uzmap/pkg/uzcore/b/d.java

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
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。
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_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.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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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

向手机申请的权限	是否危险	类型	详细情况
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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.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

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=(zh), ST=(Beijing), L=(Beijing), O=(719851065@qq.com), OU=(bcreat), CN=(719851065@qq.com)
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-09-11 06:47:00+00:00
Valid To: 2120-08-18 06:47:00+00:00
Issuer: C=(zh), ST=(Beijing), L=(Beijing), O=(719851065@qq.com), OU=(bcreat), CN=(719851065@qq.com)
Serial Number: 0x4b59df24
Hash Algorithm: sha256
md5: f59de950bbadbd7c399b7370aada8fb9
sha1: 362e101b05821def1b445103a2a5e2d6b1375d4d
sha256: 20d171ddf609181492205eaba4a7fe085889ed32e20d6c28abe40475adca0dbc
sha512: 522b8000ed79b29aa2deae0a65089f8e5f0e6d0269232f373423edd13f3e76efd58674f351dbdaffa21c620f0d2fbd1ba83a1cfe7f920e074111a842bf64b084

PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: 0697852fbe4c40c07464ec7d2a4d2f01a3e65e3164f4606a6314f6e25a2db25b

加壳分析

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>反虚拟机</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
possible Build.SERIAL check</td></tr>
<tr><td>编译器</td><td>dx</td></tr>
</table>
</td></tr>
</table>
