MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

湘建网
www.cnxjw.cn

湘建网 1.0.7.APK

APP名称:	湘建网
包名:	cn.hnhttp.cnxjw
域名线索:	18条
URL线索:	26条
邮箱线索:	1条
分析日期:	2022年2月3日 11:24

文件信息

文件名: xiangjianwang583659.apk
文件大小: 6.81MB
MD5值: 24907035cc4253cd3dcabc1ccc5ed538
SHA1值: b0dd317efe37533458645e7a20ba8f7ea835a24a
SHA256值: 6e97bb8e2386e1b1b7e310e91b68927f7a116152abc90dc0a16fa70025458870

APP 信息

App名称: 湘建网
包名: cn.hnhttp.cnxjw
主活动**Activity:** com.uzmap.pkg.LauncherUI
安卓版本名称: 1.0.7
安卓版本: 7

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
tbsrecovery.imtt.qq.com	good	**IP:** 109.244.244.237 **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
mdc.html5.qq.com	good	**IP:** 175.27.9.46 **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
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
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

域名	是否危险域名	服务器信息
mqqad.html5.qq.com	good	**IP:** 0.0.0.1 **所属国家:** - **地区:** - **城市:** - **纬度:** 0.000000 **经度:** 0.000000 **查看地图:** Google Map
www.ccil.org	good	**IP:** 172.217.163.51 **所属国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.405991 **经度:** -122.078514 **查看地图:** Google Map
s.apicloud.com	good	没有服务器地理信息.
pms.mb.qq.com	good	**IP:** 121.51.158.70 **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
debugx5.qq.com	good	**IP:** 175.27.9.46 **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
as.apicloud.com	good	没有服务器地理信息.
debugtbs.qq.com	good	**IP:** 175.27.9.46 **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
log.tbs.qq.com	good	**IP:** 109.244.244.37 **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
www.qq.com	good	**IP:** 175.27.8.138 **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
soft.tbs.imtt.qq.com	good	**IP:** 121.51.175.84 **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

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
cfg.imtt.qq.com	good	**IP:** 121.51.158.70 **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
schemas.android.com	good	没有服务器地理信息.

URL线索

URL信息	Url所在文件
www.qq.com	com/tencent/smtt/sdk/m.java
https://pms.mb.qq.com/rsp204	com/tencent/smtt/sdk/m.java
https://debugtbs.qq.com	com/tencent/smtt/sdk/WebView.java
https://debugx5.qq.com	com/tencent/smtt/sdk/WebView.java

URL信息	Url所在文件
https://debugtbs.qq.com?10000	com/tencent/smtt/sdk/WebView.java
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=50079	com/tencent/smtt/sdk/stat/MttLoader.java
https://mdc.html5.qq.com/mh?channel_id=50079&u=	com/tencent/smtt/sdk/stat/MttLoader.java
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=11041	com/tencent/smtt/sdk/ui/dialog/d.java
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=11047	com/tencent/smtt/sdk/ui/dialog/d.java
https://log.tbs.qq.com/ajax?c=pu&v=2&k=	com/tencent/smtt/utils/n.java
https://log.tbs.qq.com/ajax?c=pu&tk=	com/tencent/smtt/utils/n.java
https://log.tbs.qq.com/ajax?c=dl&k=	com/tencent/smtt/utils/n.java
https://cfg.imtt.qq.com/tbs?v=2&mk=	com/tencent/smtt/utils/n.java
https://log.tbs.qq.com/ajax?c=ul&v=2&k=	com/tencent/smtt/utils/n.java
https://mqqad.html5.qq.com/adjs	com/tencent/smtt/utils/n.java
https://log.tbs.qq.com/ajax?c=ucfu&k=	com/tencent/smtt/utils/n.java
https://tbsrecovery.imtt.qq.com/getconfig	com/tencent/smtt/utils/n.java
https://soft.tbs.imtt.qq.com/17421/tbs_res_imtt_tbs_DebugPlugin_DebugPlugin.tbs	com/tencent/smtt/utils/d.java
http://www.ccil.org/~cowan/tagsoup/properties/schema	com/deepe/a/f/l.java

URL信息	Url所在文件
http://schemas.android.com/apk/res/android	com/apicloud/third/gif/GifTextureView.java
http://schemas.android.com/apk/res/android	com/apicloud/third/gif/GifTextView.java
http://schemas.android.com/apk/res/android	com/apicloud/third/gif/GifViewUtils.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_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.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。

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=(50856700@qq.com), OU=(50856700@qq.com), CN=(y50856700)
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-12-16 00:21:37+00:00
Valid To: 2121-11-22 00:21:37+00:00
Issuer: C=(zh), ST=(Beijing), L=(Beijing), O=(50856700@qq.com), OU=(50856700@qq.com), CN=(y50856700)
Serial Number: 0x3dc74772
Hash Algorithm: sha256
md5: 30b362f44b2d03a780629c187e0f4911
sha1: 3569e5195c5638ec592f92843d2d6a84cf547130
sha256: 21177d44f386fd9f6771d0260a144907d224b51352022aa7ea361d31790a20d2
sha512: c49b3a486d5343282ec30897d180012fb8b8c6cfadfe6c36f1ddd0ebb60a11b1421523f96d331ca03f0e214be8df0d6e5b9c1b6d0de48341d1ac4854f8b9f411
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: e721c9c5d17cabc9448ea1c43ffbfd9e2a91b9864d099a3f60f323bcdb3d69e4

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
Build.PRODUCT check
Build.BOARD check
possible Build.SERIAL check
subscriber ID check</td></tr>
<tr><td>编译器</td><td>r8</td></tr>
</table>
</td></tr>
</table>