MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

花猫引流 2.1.APK

APP名称:	花猫引流
包名:	com.huamao.application
域名线索:	13条
URL线索:	13条
邮箱线索:	0条
分析日期:	2022年2月2日 20:08

文件信息

文件名: hmyinl.apk
文件大小: 5.0MB
MD5值: 6e352b187a001c9535c18a8052faebcd
SHA1值: b7e68b467552d1ec9c1e7832bb774e5bab478af7
SHA256值: 01fcd065e8cfbba0df9ca2b1a336bf8879ddaac0fb2fce786dbb6142417575f0

APP 信息

App名称: 花猫引流
包名: com.huamao.application
主活动**Activity:** com.huamao.application.app.StartActivity
安卓版本名称: 2.1
安卓版本: 3

域名线索

域名	是否危险域名	服务器信息
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

域名	是否危险域名	服务器信息
hm.datousoft.cn	good	IP: 106.13.34.64 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
wup.imtt.qq.com	good	IP: 182.254.56.113 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
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
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
api.master-pro.cn	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
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
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
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
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

域名	是否危险域名	服务器信息
soft.tbs.imtt.qq.com	good	**IP:** 121.51.175.105 **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
log.tbs.qq.com	good	**IP:** 109.244.244.32 **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
schemas.android.com	good	没有服务器地理信息.

URL线索

URL信息	Url所在文件
http://debugtbs.qq.com	com/tencent/smtt/sdk/WebView.java
http://debugx5.qq.com	com/tencent/smtt/sdk/WebView.java
http://debugtbs.qq.com?10000	com/tencent/smtt/sdk/WebView.java
www.qq.com	com/tencent/smtt/sdk/j.java

URL信息	Url所在文件
http://pms.mb.qq.com/rsp204	com/tencent/smtt/sdk/j.java
http://mdc.html5.qq.com/d/directdown.jsp?channel_id=11047	com/tencent/smtt/sdk/b/a/a.java
http://mdc.html5.qq.com/d/directdown.jsp?channel_id=11041	com/tencent/smtt/sdk/b/a/a.java
http://mdc.html5.qq.com/mh?channel_id=50079&u=	com/tencent/smtt/sdk/a/c.java
http://log.tbs.qq.com/ajax?c=pu&v=2&k=	com/tencent/smtt/utils/n.java
http://log.tbs.qq.com/ajax?c=pu&tk=	com/tencent/smtt/utils/n.java
http://wup.imtt.qq.com:8080	com/tencent/smtt/utils/n.java
http://log.tbs.qq.com/ajax?c=dl&k=	com/tencent/smtt/utils/n.java
http://cfg.imtt.qq.com/tbs?v=2&mk=	com/tencent/smtt/utils/n.java
http://log.tbs.qq.com/ajax?c=ul&v=2&k=	com/tencent/smtt/utils/n.java
http://mqqad.html5.qq.com/adjs	com/tencent/smtt/utils/n.java
http://log.tbs.qq.com/ajax?c=ucfu&k=	com/tencent/smtt/utils/n.java
http://soft.tbs.imtt.qq.com/17421/tbs_res_imtt_tbs_DebugPlugin_DebugPlugin.tbs	com/tencent/smtt/utils/d.java
http://hm.datousoft.cn	com/huamao/application/HomeActivity.java
http://api.master-pro.cn/api/app/upgrade	com/huamao/application/HomeActivity.java

URL信息	Url所在文件
http://hm.datousoft.cn	com/huamao/application/MainActivity.java
http://api.master-pro.cn/api/app/upgrade	com/huamao/application/MainActivity.java
http://api.master-pro.cn/api/app/url	com/huamao/application/app/StartActivity.java
http://api.master-pro.cn/api/auth/token?appid=kwapp	com/huamao/application/app/StartActivity.java
http://schemas.android.com/apk/res/android	d/b/k/r.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
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.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.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

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.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.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.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.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.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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。

签名证书

APK is signed
v1 signature: True
v2 signature: True

v3 signature: False
Found 1 unique certificates
Subject: C=86, ST=china, L=jn, O=sd, OU=sd, CN=kev
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-07-28 15:19:42+00:00
Valid To: 2045-07-22 15:19:42+00:00
Issuer: C=86, ST=china, L=jn, O=sd, OU=sd, CN=kev
Serial Number: 0x754acd73
Hash Algorithm: sha256
md5: 740879b3ec8274109b92eb0c4a614b1c
sha1: 9e9bcebc0516ab85d58e2d809863411e31a6729e
sha256: 0cb90e015684a442e2ca98dcc8541e9e3ee94a5e50bf0358660c74b0387bdcfd
sha512: 055e4275bd0c753644c6ff7719050e5228aa7cb2f71bd3ebc7e5158e917f0947786a2ad4734aa57f4e22c17d54068f91f7f0844d558d0da9d668aaecae56997f
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 83583f7d3fbecd07b909ae1159a2b0a9f281393e5c23eaa93b0619b2f82cb93e

加壳分析

文件列表	分析结果
classes.dex	<table><tr><th>壳列表</th><th>详细情况</th></tr><tr><td>反虚拟机</td><td>Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check subscriber ID check</td></tr><tr><td>编译器</td><td>r8</td></tr></table>