MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

Visitor Cloud 6.12.APK

APP名称:	Visitor Cloud
包名:	com.wafersystems.visitorwebapp
域名线索:	12条
URL线索:	17条
邮箱线索:	0条
分析日期:	2022年2月2日 23:04

文件信息

文件名: visitorcloud559542.apk
文件大小: 4.87MB
MD5值: 1ca3b11eb09159f28b4537db2611ede6
SHA1值: 9ea2a73e2c7e00f8997526d8fa86a17763a172e0
SHA256值: 063fde8be568f1c8f560d58eb36fccaf3e9f8f3a1db6318aa46cb7ddce78f12d

APP 信息

App名称: Visitor Cloud
包名: com.wafersystems.visitorwebapp
主活动**Activity:** com.wafersystems.visitorwebapp.ui.HomeActivity
安卓版本名称: 6.12
安卓版本: 70

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
www.slf4j.org	good	**IP:** 83.166.144.67 **所属国家:** Switzerland **地区:** Geneve **城市:** Carouge **纬度:** 46.180962 **经度:** 6.139210 **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
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
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

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
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

域名	是否危险域名	服务器信息
github.com	good	**IP:** 20.205.243.166 **所属国家:** United States of America **地区:** Washington **城市:** Redmond **纬度:** 47.682899 **经度:** -122.120903 **查看地图:** Google Map
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:** 109.244.244.37 **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

URL线索

URL信息	Url所在文件
www.qq.com	com/tencent/smtt/sdk/l.java

URL信息	Url所在文件
https://pms.mb.qq.com/rsp204	com/tencent/smtt/sdk/l.java
https://debugtbs.qq.com	com/tencent/smtt/sdk/WebView.java
https://debugx5.qq.com	com/tencent/smtt/sdk/WebView.java
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/m.java
https://log.tbs.qq.com/ajax?c=pu&tk=	com/tencent/smtt/utils/m.java
https://log.tbs.qq.com/ajax?c=dl&k=	com/tencent/smtt/utils/m.java
https://cfg.imtt.qq.com/tbs?v=2&mk=	com/tencent/smtt/utils/m.java
https://log.tbs.qq.com/ajax?c=ul&v=2&k=	com/tencent/smtt/utils/m.java
https://mqqad.html5.qq.com/adjs	com/tencent/smtt/utils/m.java
https://log.tbs.qq.com/ajax?c=ucfu&k=	com/tencent/smtt/utils/m.java

URL信息	Url所在文件
https://tbsrecovery.imtt.qq.com/getconfig	com/tencent/smtt/utils/m.java
https://soft.tbs.imtt.qq.com/17421/tbs_res_imtt_tbs_DebugPlugin_DebugPlugin.tbs	com/tencent/smtt/utils/d.java
http://www.slf4j.org/codes.html#no_static_mdc_binder	org/slf4j/MDC.java
http://www.slf4j.org/codes.html#null_MDCA	org/slf4j/MDC.java
http://www.slf4j.org/codes.html	org/slf4j/LoggerFactory.java
http://www.slf4j.org/codes.html#loggerNameMismatch	org/slf4j/LoggerFactory.java
http://www.slf4j.org/codes.html#multiple_bindings	org/slf4j/LoggerFactory.java
http://www.slf4j.org/codes.html#StaticLoggerBinder	org/slf4j/LoggerFactory.java
http://www.slf4j.org/codes.html#null_LF	org/slf4j/LoggerFactory.java
http://www.slf4j.org/codes.html#replay	org/slf4j/LoggerFactory.java
http://www.slf4j.org/codes.html#substituteLogger	org/slf4j/LoggerFactory.java
http://www.slf4j.org/codes.html#unsuccessfulInit	org/slf4j/LoggerFactory.java
http://www.slf4j.org/codes.html#version_mismatch	org/slf4j/LoggerFactory.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Flowable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Completable.java

URL信息	Url所在文件
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Single.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Maybe.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Observable.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0#error-handling	io/reactivex/exceptions/UndeliverableException.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/exceptions/OnErrorNotImplementedException.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.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.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_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.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.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_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

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=cn, ST=shannxi, L=xian, O=Wafersystems, OU=Wafersystems, CN=Wafer
Signature Algorithm: dsa
Valid From: 2017-07-31 08:37:36+00:00
Valid To: 2017-10-29 08:37:36+00:00
Issuer: C=cn, ST=shannxi, L=xian, O=Wafersystems, OU=Wafersystems, CN=Wafer
Serial Number: 0x37e7ef96
Hash Algorithm: sha1
md5: b17c5fce5a569566af55829ddf67b98d
sha1: 9d4fe70810a6a1faa70c4c3ba90d692cf61b355f
sha256: 88aca2303f40779fe68cce675d87d2fb2cb93702f0326d0ebcb2172db651c781
sha512: 7bc142f427878a51a3f669d1c65b6c48cf8109a4b18fa29ba29ce5bee8b9ffa99786990e67c29fbf125f7d7ad3dcf7a22ed891f5509cc93bbc6eb69ba6f3c7f9
PublicKey Algorithm: dsa
Bit Size: 1024
Fingerprint: c1505424539d15ea21df99217d37afb3680cc7d6285c9b0472f9a02ed5d8e47b

硬编码敏感信息

可能的敏感信息
"key_tb_count" : "key_tb_count"

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.FINGERPRINT check 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>
