MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

便捷天气通 1.0.APK

APP名称:	便捷天气通
包名:	com.itsm.boyuan.weather
域名线索:	10条
URL线索:	15条
邮箱线索:	0条
分析日期:	2022年1月26日 18:46

文件信息

文件名: bjtqt.apk
文件大小: 2.81MB
MD5值: a3b2ab061571ba61e67864433af2fc00
SHA1值: a0950eca2eac66c1118e68c8acae590614f04972
SHA256值: 66d5b0920d87a9e6364a23153eefe2643b3c106524275dab814a15d60630552c

APP 信息

App名称: 便捷天气通
包名: com.itsm.boyuan.weather
主活动**Activity:** com.itsm.boyuan.weather.SplashActivity
安卓版本名称: 1.0
安卓版本: 1

域名线索

域名	是否危险域名	服务器信息
sapi.skyhookwireless.com	good	**IP:** 54.169.126.245 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289670 经度: 103.850067 查看地图: Google Map
lba.baidu.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
sdk.e.qq.com	good	IP: 58.250.137.37 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
loc.map.baidu.com	good	IP: 111.206.209.175 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
static.jesgoo.com	good	IP: 47.104.9.193 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
rcv.moogos.com	good	IP: 101.37.130.145 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
c.isdspeed.qq.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
itsdata.map.baidu.com	good	**IP:** 111.206.209.180 **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
wspeed.qq.com	good	没有服务器地理信息.
op.juhe.cn	good	**IP:** 203.107.54.210 **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

URL线索

URL信息	Url所在文件
http://static.jesgoo.com	com/jesgoo/sdk/a/a.java
http://static.jesgoo.com/sdk/msdk/%s	com/jesgoo/sdk/dsp/AdDspConfig.java
http://rcv.moogos.com/newsdk?	com/jesgoo/sdk/dsp/c.java
http://op.juhe.cn/onebox/weather/query?cityname=	com/example/qinlei/http/HttpGetData.java

URL信息	Url所在文件
http://lba.baidu.com/	com/baidu/location/BDLocation.java
http://loc.map.baidu.com/sdk.php	com/baidu/location/h/i.java
http://loc.map.baidu.com/user_err.php	com/baidu/location/h/i.java
http://loc.map.baidu.com/oqur.php	com/baidu/location/h/i.java
http://loc.map.baidu.com/tcu.php	com/baidu/location/h/i.java
http://loc.map.baidu.com/rtbu.php	com/baidu/location/h/i.java
http://loc.map.baidu.com/iofd.php	com/baidu/location/h/i.java
https://sapi.skyhookwireless.com/wps2/location	com/baidu/location/h/i.java
http://loc.map.baidu.com/wloc	com/baidu/location/h/i.java
http://loc.map.baidu.com/sdk_ep.php	com/baidu/location/h/i.java
http://itsdata.map.baidu.com/long-conn-gps/sdk.php	com/baidu/location/c/k.java
http://loc.map.baidu.com/statloc	com/baidu/location/c/f.java
http://loc.map.baidu.com/cc.php	com/baidu/location/c/e.java
http://%s/%s	com/baidu/location/e/e.java
http://loc.map.baidu.com/offline_loc	com/baidu/location/e/d.java

URL信息	Url所在文件
http://op.juhe.cn/onebox/weather/query?cityname=	com/itsm/boyuan/http/HttpGetData.java
http://wspeed.qq.com/w.cgi	com/qq/e/comm/services/RetCodeService.java
http://c.isdspeed.qq.com/code.cgi	com/qq/e/comm/services/RetCodeService.java
http://sdk.e.qq.com/err	com/qq/e/comm/services/a.java
http://sdk.e.qq.com/launch	com/qq/e/comm/services/a.java
http://sdk.e.qq.com/activate	com/qq/e/comm/services/a.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.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_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

向手机申请的权限	是否危险	类型	详细情况
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.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.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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕
android.permission.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息

签名证书

APK is signed
v1 signature: True

v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: CN=guo
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2017-08-09 03:41:10+00:00
Valid To: 2042-08-03 03:41:10+00:00
Issuer: CN=guo
Serial Number: 0x2293fca9
Hash Algorithm: sha256
md5: 87ceb7a31621a96b80bc2fbce57c4947
sha1: 8b935269945145c973f9d7b02763f0248adc9e20
sha256: 7a65467c1806eb6ce439fa5c985676bf1bfbea3f8eb830f8ea290305597b8bc0
sha512: 6798532bea714444e608599e62db94ac74e0ca919e488aab7a0ead1591d1b951529da8e98bb15937b3930080f11a6a5c8af36aaa1e086878f91ab785654494ab

Exodus威胁情报

名称	分类	URL链接
Baidu Location		https://reports.exodus-privacy.eu.org/trackers/97

加壳分析

文件列表	分析结果

<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.MODEL check
Build.MANUFACTURER check
subscriber ID check</td></tr>
<tr><td>编译器</td><td>dx (possible dexmerge)</td></tr>
<tr><td>Manipulator Found</td><td>dexmerge</td></tr>
</table>
</td></tr>
<tr><td>extra/core.jar!classes.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>编译器</td><td>dx</td></tr>
</table>
</td></tr>
<tr><td>extra/core.jar!extra/libcore.jar!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>possible Build.SERIAL check</td></tr>
<tr><td>编译器</td><td>dx</td></tr>
</table>
</td></tr>
</table>
