MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

风喵加速器 1.2.0.7.APK

APP名称:	风喵加速器
包名:	com.stnts.fmspeed
域名线索:	36条
URL线索:	43条
邮箱线索:	0条
分析日期:	2022年1月18日 23:08

文件信息

文件名: 75cf439445c38739ab0d5839feb74e10.apk
文件大小: 12.24MB
MD5值: 75cf439445c38739ab0d5839feb74e10
SHA1值: 4a0b4fb9187d61e77d250298466d3dc2918860de
SHA256值: 1c4a9167440e1c1b3bd57f128588dcb6c8d38ba9a1cebade8e8e66abe6333309

APP 信息

App名称: 风喵加速器
包名: com.stnts.fmspeed
主活动**Activity:** com.stnts.fmspeed.LauncherActivity
安卓版本名称: 1.2.0.7
安卓版本: 9

域名线索

域名	是否危险域名	服务器信息
mobilegw-1-64.test.alipay.net	good	没有服务器地理信息.
openmobile.qq.com	good	**IP:** 121.51.23.243 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
datax.baidu.com	good	IP: 111.206.210.170 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
h.trace.qq.com	good	IP: 109.244.244.244 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
imgcache.qq.com	good	IP: 121.51.184.11 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
mobilegw.aaa.alipay.net	good	没有服务器地理信息.
appsupport.qq.com	good	IP: 183.2.143.207 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.116671 经度: 113.250000 查看地图: Google Map

域名	是否危险域名	服务器信息
10.0.45.141	good	**IP:** 10.0.45.141 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000 查看地图: Google Map
cgi.qplus.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
cgi.connect.qq.com	good	**IP:** 183.2.143.207 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.116671 经度: 113.250000 查看地图: Google Map
fx.fmiao.net	good	**IP:** 61.160.243.79 所属国家: China 地区: Jiangsu 城市: Changzhou 纬度: 31.783331 经度: 119.966667 查看地图: Google Map
wspeed.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
client-box.fmiao.net	good	IP: 61.160.243.81 所属国家: China 地区: Jiangsu 城市: Changzhou 纬度: 31.783331 经度: 119.966667 查看地图: Google Map
dssps.stnts.com	good	IP: 116.211.100.21 所属国家: China 地区: Hubei 城市: Wuhan 纬度: 30.583330 经度: 114.266670 查看地图: Google Map
mobilegw.alipaydev.com	good	IP: 110.75.132.131 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.weixin.qq.com	good	IP: 109.244.145.152 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
render.alipay.com	good	IP: 182.40.18.118 所属国家: China 地区: Shandong 城市: Qingdao 纬度: 36.098610 经度: 120.371941 查看地图: Google Map
register.stnts.com	good	IP: 122.144.206.55 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.222219 经度: 121.458061 查看地图: Google Map
h5.m.taobao.com	good	IP: 219.147.75.136 所属国家: China 地区: Heilongjiang 城市: Harbin 纬度: 45.750000 经度: 126.650002 查看地图: Google Map
huatuocode.huatuo.qq.com	good	没有服务器地理信息.
mobilegw.stable.alipay.net	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
wappaygw.alipay.com	good	IP: 203.209.250.6 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
openrcv.baidu.com	good	IP: 111.206.209.112 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
10.0.41.140	good	IP: 10.0.41.140 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000 查看地图: Google Map
hmma.baidu.com	good	IP: 110.242.68.196 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280 查看地图: Google Map

域名	是否危险域名	服务器信息
m.alipay.com	good	IP: 203.209.245.120 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
dxp.baidu.com	good	IP: 110.242.68.94 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280 查看地图: Google Map
mobilegw.alipay.com	good	IP: 203.209.250.2 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
mcgw.alipay.com	good	IP: 203.209.250.50 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
mclient.alipay.com	good	IP: 203.209.250.50 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
dssp.stnts.com	good	IP: 116.211.100.21 所属国家: China 地区: Hubei 城市: Wuhan 纬度: 30.583330 经度: 114.266670 查看地图: Google Map
loggw-exsdk.alipay.com	good	IP: 110.76.3.1 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
open.weixin.qq.com	good	IP: 175.24.209.30 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
speedup.fmiao.net	good	**IP:** 61.160.243.81 所属国家: China 地区: Jiangsu 城市: Changzhou 纬度: 31.783331 经度: 119.966667 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
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

URL线索

URL信息	Url所在文件
https://render.alipay.com/p/s/i?scheme=%s	com/alipay/sdk/app/OpenAuthTask.java

URL信息	Url所在文件
https://mobilegw.alipay.com/mgw.htm	com/alipay/sdk/cons/a.java
https://mobilegw.alipaydev.com/mgw.htm	com/alipay/sdk/cons/a.java
https://mcgw.alipay.com/sdklog.do	com/alipay/sdk/cons/a.java
https://loggw-exsdk.alipay.com/loggw/logUpload.do	com/alipay/sdk/cons/a.java
http://m.alipay.com/?action=h5quit	com/alipay/sdk/cons/a.java
https://wappaygw.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/cons/a.java
https://mclient.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/cons/a.java
https://h5.m.taobao.com/mlapp/olist.html	com/alipay/sdk/data/a.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw.aaa.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw-1-64.test.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw.stable.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
https://fx.fmiao.net/mobile/qs.html?timespan=%d&channel=%s&version=%s	com/stnts/fmspeed/HelpQActivity.java
https://fx.fmiao.net/	com/stnts/fmspeed/GameFragment.java
https://fx.fmiao.net/mobile?timespan=%d	com/stnts/fmspeed/AboutActivity.java

URL信息	Url所在文件
https://fx.fmiao.net/mobile/mobile.html?timespan=%d	com/stnts/fmspeed/AboutActivity.java
https://register.stnts.com/new/v2/security/show.do	com/stnts/fmspeed/SafeActivity.java
https://fx.fmiao.net/mobile?timespan=%d	com/stnts/fmspeed/LoginActivity.java
https://fx.fmiao.net/mobile/mobile.html?timespan=%d	com/stnts/fmspeed/LoginActivity.java
http://dssp.stnts.com:8888/?opt=put&type=json	com/stnts/fmspeed/NetModul/NetWorkModel.java
https://api.weixin.qq.com/sns/oauth2/access_token	com/stnts/fmspeed/NetModul/NetWorkModel.java
https://api.weixin.qq.com/sns/oauth2/refresh_token	com/stnts/fmspeed/NetModul/NetWorkModel.java
https://api.weixin.qq.com/sns/userinfo	com/stnts/fmspeed/NetModul/NetWorkModel.java
https://fx.fmiao.net/mobile/guide/index.html?rom=%s&timespan=%d	com/stnts/fmspeed/Manager/ConfigManager.java
https://speedup.fmiao.net	com/stnts/fmspeed/Manager/DomainConfig.java
http://10.0.41.140:9094	com/stnts/fmspeed/Manager/DomainConfig.java
https://client-box.fmiao.net	com/stnts/fmspeed/Manager/DomainConfig.java
http://10.0.41.140:9077	com/stnts/fmspeed/Manager/DomainConfig.java
https://fx.fmiao.net/mobile/mobile.html?timespan=%d	com/stnts/fmspeed/Control/PolicyDialog.java
https://fx.fmiao.net/mobile?timespan=%d	com/stnts/fmspeed/Control/PolicyDialog.java

URL信息	Url所在文件
https://dssps.stnts.com/?opt=put&type=json	com/stnts/analytics/android/sdk/net/RequestClient.java
http://10.0.45.141:8888/?opt=put&type=json	com/stnts/analytics/android/sdk/net/RequestClient.java
https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s	com/tencent/mm/opensdk/diffdev/a/b.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/opensdk/diffdev/a/c.java
https://openmobile.qq.com/oauth2.0/me	com/tencent/connect/UnionInfo.java
https://openmobile.qq.com/oauth2.0/m_authorize?	com/tencent/connect/auth/AuthAgent.java
https://openmobile.qq.com/user/user_login_statis	com/tencent/connect/auth/AuthAgent.java
https://openmobile.qq.com/v3/user/get_info	com/tencent/connect/auth/AuthAgent.java
https://appsupport.qq.com/cgi-bin/qzapps/mapp_addapp.cgi	com/tencent/connect/auth/AuthAgent.java
https://imgcache.qq.com/ptlogin/static/qzsjump.html?	com/tencent/connect/auth/a.java
https://openmobile.qq.com/oauth2.0/m_jump_by_version?	com/tencent/connect/common/BaseApi.java
https://imgcache.qq.com/ptlogin/static/qzsjump.html?	com/tencent/connect/common/BaseApi.java
https://cgi.qplus.com/report/report	com/tencent/connect/avatar/ImageActivity.java
https://imgcache.qq.com/open/mobile/request/sdk_request.html?	com/tencent/open/SocialApiIml.java
https://imgcache.qq.com/open/mobile/invite/sdk_invite.html?	com/tencent/open/SocialApiIml.java

URL信息	Url所在文件
https://imgcache.qq.com/open/mobile/sendstory/sdk_sendstory_v1.3.html?	com/tencent/open/SocialApiIml.java
https://imgcache.qq.com	com/tencent/open/SocialApiIml.java
https://openmobile.qq.com/cgi-bin/qunopensdk/unbind	com/tencent/open/SocialOperation.java
https://openmobile.qq.com/cgi-bin/qunopensdk/check_group	com/tencent/open/SocialOperation.java
https://h.trace.qq.com/kv	com/tencent/open/b/b.java
https://wspeed.qq.com/w.cgi	com/tencent/open/b/h.java
https://appsupport.qq.com/cgi-bin/appstage/mstats_batch_report	com/tencent/open/b/h.java
https://huatuocode.huatuo.qq.com	com/tencent/open/b/e.java
https://openmobile.qq.com/	com/tencent/open/utils/HttpUtils.java
https://cgi.connect.qq.com/qqconnectopen/openapi/policy_conf	com/tencent/open/utils/h.java
https://hmma.baidu.com/auto.gif	com/baidu/mobstat/Config.java
http://hmma.baidu.com/app.gif	com/baidu/mobstat/Config.java
https://hmma.baidu.com/app.gif	com/baidu/mobstat/Config.java
http://openrcv.baidu.com/1010/bplus.gif	com/baidu/mobstat/r.java
https://openrcv.baidu.com/1010/bplus.gif	com/baidu/mobstat/r.java

URL信息	Url所在文件
http://datax.baidu.com/xs.gif	com/baidu/mobstat/y.java
https://datax.baidu.com/xs.gif	com/baidu/mobstat/y.java
http://dxp.baidu.com/upgrade	com/baidu/mobstat/y.java
https://dxp.baidu.com/upgrade	com/baidu/mobstat/y.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Flowable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Completable.java
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.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.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.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.CHANGE_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。
android.Manifest.permission.READ_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference

向手机申请的权限	是否危险	类型	详细情况
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.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.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.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
freemme.permission.msa	未知	Unknown permission	Unknown permission from android reference

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=027, ST=hubei, L=wuhan, O=stnts, OU=stnts, CN=qc.liu
Signature Algorithm: rsassa_pkcs1v15

Valid From: 2020-04-27 06:53:27+00:00
Valid To: 2030-04-25 06:53:27+00:00
Issuer: C=027, ST=hubei, L=wuhan, O=stnts, OU=stnts, CN=qc.liu
Serial Number: 0x1fb70ac3
Hash Algorithm: sha256
md5: 93e315a56c206a3acf5038ac83f140e0
sha1: 41dfe650fc95bf5cae70ec66b9344fb2d2e2e28c
sha256: 9dc2473fb48a2bf125a18cd339a54564750fad8b11377a37dec7e1ceac5d282f
sha512: 5297d62a8bb2ba61feb9d98ecb6e9ddd7b2ee3805e4dd1b8c0ad062b6637e7a8af4202597f8533a3ba22dcc0be8886da7ae47c5e80944e1f062165e1fbd2d015
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: 47f2604ac4ceececd05e8dcce4a9468fec73a7f221f0f2021af9ec4fdb24ba8f

Exodus威胁情报

名称	分类	URL链接
Baidu Mobile Stat	Analytics	https://reports.exodus-privacy.eu.org/trackers/101

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.tencent.tauth.AuthActivity	Schemes: \ 1112072240://,

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.HARDWARE check
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check
network operator name check
device ID check
subscriber ID check
ro.product.device check
ro.kernel.qemu check
emulator file check
possible VM check</td></tr>
<tr><td>反调试</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>编译器</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>
