MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

广告汪 5.0.0.APK

APP名称:	广告汪
包名:	com.ggw.myapplication
域名线索:	26条
URL线索:	66条
邮箱线索:	1条
分析日期:	2022年2月2日 11:40

文件信息

文件名: guanggaowang.apk
文件大小: 14.07MB
MD5值: 50d03703f8300cd56121b0dfa8413c4b
SHA1值: 6b36bbe143a413314f4a2b8282ef44b8af091f9b
SHA256值: 16c1e99cabb12448f6658206b820e53b4a4416572dfbb6e6a4fbc2244bd753b4

APP 信息

App名称: 广告汪
包名: com.ggw.myapplication
主活动**Activity:** io.dcloud.PandoraEntry
安卓版本名称: 5.0.0
安卓版本: 500

域名线索

域名	是否危险域名	服务器信息
api.rqmob.com	good	**IP:** 54.254.165.169 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
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
ask.dcloud.net.cn	good	IP: 124.239.227.208 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717 查看地图: Google Map
schemas.android.com	good	没有服务器地理信息.
tdid.m.qq.com	good	IP: 182.254.51.126 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
crbug.com	good	IP: 216.239.32.29 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
analytics.map.qq.com	good	IP: 182.254.63.54 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
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
mi.ssp.qq.com	good	IP: 121.51.191.89 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
wspeed.qq.com	good	没有服务器地理信息.
v.gdt.qq.com	good	IP: 182.254.58.224 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
t.gdt.qq.com	good	IP: 183.3.225.119 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
stream.mobihtml5.com	good	没有服务器地理信息.
96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com	good	IP: 47.93.95.208 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
www.dcloud.io	good	IP: 222.85.26.233 所属国家: China 地区: Henan 城市: Zhengzhou 纬度: 34.757778 经度: 113.648613 查看地图: Google Map
m3w.cn	good	IP: 124.239.227.208 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717 查看地图: Google Map
d.gdt.qq.com	good	IP: 121.51.131.15 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
qzonestyle.gtimg.cn	good	IP: 182.254.48.95 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
stream.dcloud.net.cn	good	IP: 118.31.188.88 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
pmir.3g.qq.com	good	IP: 113.96.208.65 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
imgcache.qq.com	good	IP: 121.51.184.53 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
service.dcloud.net.cn	good	IP: 120.26.1.80 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
static.rqmob.com	good	IP: 101.33.26.180 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
qzs.qq.com	good	IP: 182.254.54.167 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
lbs.map.qq.com	good	IP: 182.254.50.117 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
lame.sf.net	good	**IP:** 204.68.111.100 所属国家: United States of America 地区: California 城市: San Diego 纬度: 32.799797 经度: -117.137047 查看地图: Google Map

URL线索

URL信息	Url所在文件
http://pmir.3g.qq.com	com/tencent/turingfd/sdk/ams/au/aj.java
https://tdid.m.qq.com?mc=2	com/tencent/turingfd/sdk/ams/au/aq.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/activate	com/qq/e/comm/services/a.java
http://sdk.e.qq.com/launch	com/qq/e/comm/services/a.java
http://qzonestyle.gtimg.cn/qzone/biz/gdt/mob/sdk/v2/android03/js-release/%s/native.js	com/qq/e/comm/plugin/gdtnativead/j.java

URL信息	Url所在文件
http://t.gdt.qq.com/conv/src/6/conv	com/qq/e/comm/plugin/q/b.java
http://qzonestyle.gtimg.cn/qzone/biz/gdt/mob/sdk/v2/android01/interstitial.html	com/qq/e/comm/plugin/q/a.java
http://imgcache.qq.com/qzone/biz/gdt/dev/sdk/cdn/resources/common/SdkNativeAdLogo.png	com/qq/e/comm/plugin/intersitial2/e.java
http://qzonestyle.gtimg.cn/qzone/biz/gdt/mob/sdk/v2/android01/appdetail.html	com/qq/e/comm/plugin/c/b.java
http://qzonestyle.gtimg.cn/qzone/biz/gdt/mob/sdk/v2/android01/banner.html	com/qq/e/comm/plugin/c/a.java
http://imgcache.qq.com/qzone/biz/gdt/dev/sdk/cdn/resources/common/SdkSplashAdLogo.png	com/qq/e/comm/plugin/util/bc.java
http://imgcache.qq.com/qzone/biz/gdt/dev/sdk/cdn/resources/common/SdkNativeAdLogo.png	com/qq/e/comm/plugin/util/bc.java
http://imgcache.qq.com/qzone/biz/gdt/dev/sdk/cdn/resources/common/SdkRewardAdLogo.png	com/qq/e/comm/plugin/util/bc.java
http://imgcache.qq.com/qzone/biz/gdt/dev/sdk/cdn/resources/common/SspSplashAdLogo.png	com/qq/e/comm/plugin/util/bc.java
https://static.rqmob.com/ssp_splash_english_ad_logo_2x.png	com/qq/e/comm/plugin/util/bc.java
https://static.rqmob.com/ssp_native_english_ad_log_2x.png	com/qq/e/comm/plugin/util/bc.java
http://imgcache.qq.com/qzone/biz/gdt/dev/sdk/cdn/resources/common/SspNativeAdLogo.png	com/qq/e/comm/plugin/util/bc.java
http://imgcache.qq.com/qzone/biz/gdt/dev/sdk/cdn/resources/common/SspRewardAdLogo.png	com/qq/e/comm/plugin/util/bc.java
http://d.gdt.qq.com/fcg-bin/gdt_appdetail.fcg?ico=1&op_appid=	com/qq/e/comm/plugin/util/d.java
http://d.gdt.qq.com/fcg-bin/gdt_appdetail.fcg?ico=1&appid=	com/qq/e/comm/plugin/util/d.java

URL信息	Url所在文件
http://qzs.qq.com/union/res/union_cdn/page/images/loading_2x.gif	com/qq/e/comm/plugin/m/k.java
http://v.gdt.qq.com/gdt_stats.fcg	com/qq/e/comm/plugin/ab/c/j.java
https://api.rqmob.com/config?version=2	com/qq/e/comm/plugin/r/a/d.java
https://api.rqmob.com/config	com/qq/e/comm/plugin/r/a/d.java
https://mi.ssp.qq.com/config?version=2	com/qq/e/comm/plugin/r/a/d.java
https://mi.ssp.qq.com/config	com/qq/e/comm/plugin/r/a/d.java
http://qzonestyle.gtimg.cn/qzone/biz/gdt/mob/sdk/v2/android01/download.html	com/qq/e/comm/plugin/j/a.java
http://%s/%s	com/qq/e/comm/plugin/x/C0065a.java
http://sdk.e.qq.com	com/qq/e/comm/plugin/w/C0064h.java
http://sdk.e.qq.com/getad	com/qq/e/comm/plugin/w/C0064h.java
http://sdk.e.qq.com/disp	com/qq/e/comm/plugin/w/C0064h.java
http://sdk.e.qq.com/click	com/qq/e/comm/plugin/w/C0064h.java
http://sdk.e.qq.com/msg	com/qq/e/comm/plugin/w/C0064h.java
https://qzs.qq.com/union/res/union_temp_v2/page/ANTempMob/tempMob.c57c184b4f1591947314638.html	com/qq/e/comm/plugin/z/c.java
https://qzs.qq.com/union/res/union_temp_v2/page/ANTempMob/tempMob.dca5a5e918.js	com/qq/e/comm/plugin/z/c.java

URL信息	Url所在文件
https://qzs.qq.com/union/res/union_temp_v2/page/ANTempMob/tempMob.package.json	com/qq/e/comm/plugin/z/c.java
http://imgcache.qq.com/qzone/biz/gdt/dev/sdk/cdn/resources/common/SdkRewardBrowseAdLogo.png	com/qq/e/comm/plugin/rewardvideo/b/b.java
https://sdk.e.qq.com	com/qq/e/comm/plugin/y/C0074w.java
https://analytics.map.qq.com/tr?mllc	c/t/maploc/lite/tsa/aa.java
https://lbs.map.qq.com/loc	c/t/maploc/lite/tsa/h.java
https://analytics.map.qq.com/?sf2	c/t/maploc/lite/tsa/w.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifViewUtils.java
http://ask.dcloud.net.cn/article/283	io/dcloud/feature/b.java
http://ask.dcloud.net.cn/article/35058	io/dcloud/feature/audio/AudioRecorderMgr.java
https://96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com/http/splash-screen/report	io/dcloud/feature/ad/dcloud/ADHandler.java
http://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.java
http://m3w.cn/s/	io/dcloud/common/util/ShortCutUtil.java
http://www.dcloud.io/streamapp/streamapp.apk	io/dcloud/common/util/ShortCutUtil.java

URL信息	Url所在文件
http://stream.dcloud.net.cn/resource/sitemap/v2?appid=	io/dcloud/common/a/d.java
http://ask.dcloud.net.cn/article/35627	io/dcloud/common/a/a.java
https://ask.dcloud.net.cn/article/35877	io/dcloud/common/a/a.java
https://service.dcloud.net.cn/sta/so?p=a&pn=%s&ver=%s&appid=%s	io/dcloud/common/core/b.java
https://service.dcloud.net.cn/pdz	io/dcloud/common/core/b/a.java
https://96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com/http/rewarded-video/report?p=a&t=	io/dcloud/common/core/b/a.java
http://ask.dcloud.net.cn/article/282	io/dcloud/common/constant/DOMException.java
https://stream.mobihtml5.com/	io/dcloud/common/constant/StringConst.java
https://stream.dcloud.net.cn/	io/dcloud/common/constant/StringConst.java
https://crbug.com/v8/8520	lib/armeabi-v7a/libweexjss.so
http://lame.sf.net	lib/armeabi-v7a/liblamemp3.so

邮箱线索

邮箱地址	所在文件
.apk@classes.dex	com/tencent/turingfd/sdk/ams/au/bi.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.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.INSTALL_PACKAGES	系统需要	直接安装应用程序	允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序
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.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

向手机申请的权限	是否危险	类型	详细情况
android.permission.BROADCAST_PACKAGE_REMOVED	合法	send package removed broadcast	允许应用程序广播应用程序包已被删除的通知。恶意应用程序可能会使用它来杀死正在运行的任何其他应用程序
android.permission.CALL_PHONE	危险	直接拨打电话号码	允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码
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.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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
android.permission.GET_ACCOUNTS	危险	列出帐户	允许访问账户服务中的账户列表
android.permission.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由
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

向手机申请的权限	是否危险	类型	详细情况
android.permission.READ_CONTACTS	危险	读取联系人数据	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人
android.permission.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.WRITE_CONTACTS	危险	写入联系人数据	允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可以使用它来删除或修改您的联系人数据
android.permission.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。
android.permission.ACCESS_BACKGROUND_LOCATION	危险	后台访问位置	允许应用程序在后台访问位置

向手机申请的权限	是否危险	类型	详细情况
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
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。

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: L=England, O=ggw, OU=ggw, CN=ggw
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-09-21 03:53:47+00:00
Valid To: 2045-09-15 03:53:47+00:00
Issuer: L=England, O=ggw, OU=ggw, CN=ggw
Serial Number: 0x70378e94
Hash Algorithm: sha256
md5: 8b3535f0663c70ddd61a0ed71aefbad3
sha1: f0caeb646aac955e9b3dd9615fa94d1aceccd6ec
sha256: 91c4c3e865d3d47df13e9acf0174fca7255c9a996dbcde6adee734b1c2cfd69f

sha512: 9cc86ca9056c196d2176846fb4e86f7476b839460054ab6eb75ea8bbb04fbf4a7d75070164e661199fffcf6739abc977dcf605659109513ec8838cc7524d7576
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: d03bf9f6e2ad15d3f28d6943150fd00134037e5ba018c86131ac901973be4ef3

加壳分析

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>assets/yaqgdtadv0.sec</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</td></tr>
<tr><td>编译器</td><td>dexlib 2.x</td></tr>
</table>
</td></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
possible Build.SERIAL check
SIM operator check
subscriber ID check
possible VM check</td></tr>
<tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>classes2.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.MANUFACTURER check</td></tr>
<tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>lib/armeabi-v7a/libturingau.so</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>模糊器</td><td>Obfuscator-LLVM version unknown</td></tr>
</table>
</td></tr>
</table>
