MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

至仁同济云 1.0.APK

APP名称:	至仁同济云
包名:	com.gdjztw.yaoqi.gstjyyy
域名线索:	16条
URL线索:	19条
邮箱线索:	2条
分析日期:	2022年1月25日 23:07

文件信息

文件名: zrtjy.apk
文件大小: 6.86MB
MD5值: 0fcf3be60df8ead48a54ccc8c3e826a4
SHA1值: ad867610762738f202440ac051a62aee520d1ac1
SHA256值: 09a7452c9b00eec1125c8f7713d1100f94df2050bcc44b97d93806cd6bbf2a38

APP 信息

App名称: 至仁同济云
包名: com.gdjztw.yaoqi.gstjyyy
主活动**Activity:** com.gdjztw.yaodian.yuanzhilindayaofang.MainActivity
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
astat.bugly.qcloud.com	good	**IP:** 150.109.29.135 所属国家: Korea (Republic of) 地区: Seoul-teukbyeolsi 城市: Seoul 纬度: 37.568260 经度: 126.977829 查看地图: Google Map

域名	是否危险域名	服务器信息
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
ibsbjstar.ccb.com.cn	good	IP: 118.228.48.66 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
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
astat.bugly.cros.wr.pvp.net	good	IP: 170.106.135.32 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.774929 经度: -122.419418 查看地图: Google Map

域名	是否危险域名	服务器信息
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
mobile.unionpay.com	good	没有服务器地理信息.
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
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
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
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
android.bugly.qq.com	good	IP: 109.244.244.137 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
m.gstjyyy.com	good	IP: 120.79.186.232 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
soft.tbs.imtt.qq.com	good	IP: 182.254.59.187 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
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
140.207.168.45	good	**IP:** 140.207.168.45 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

URL线索

URL信息	Url所在文件
http://mobile.unionpay.com/getclient?platform=android&type=securepayplugin	com/unionpay/UPPayAssistEx.java
https://mobile.unionpay.com/getclient?platform=android&type=securepayplugin	com/unionpay/UPPayAssistEx.java
http://140.207.168.45/g/d	com/unionpay/sdk/c.java
https://mobile.unionpay.com/getclient?platform=android&type=securepayplugin	com/unionpay/mobile/android/utils/c.java
http://m.gstjyyy.com/	com/gdjztw/yaodian/yuanzhilindayaofang/b.java

URL信息	Url所在文件
http://m.gstjyyy.com//privacy	com/gdjztw/yaodian/yuanzhilindayaofang/e.java
http://m.gstjyyy.com//userAgreement	com/gdjztw/yaodian/yuanzhilindayaofang/e.java
https://ibsbjstar.ccb.com.cn/	com/ccb/ccbnetpay/a.java
https://ibsbjstar.ccb.com.cn/	com/ccb/ccbnetpay/platform/Platform.java
https://ibsbjstar.ccb.com.cn/CCBIS/ccbMain?	com/ccb/ccbnetpay/platform/Platform.java
https://ibsbjstar.ccb.com.cn/CCBIS/ccbMain	com/ccb/ccbnetpay/platform/Platform.java
https://android.bugly.qq.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
https://astat.bugly.qcloud.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/a.java
https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async	com/tencent/bugly/crashreport/common/strategy/a.java
https://debugtbs.qq.com	com/tencent/smtt/sdk/WebView.java
https://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
http://pms.mb.qq.com/rsp204	com/tencent/smtt/sdk/j.java
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=50079	com/tencent/smtt/sdk/stat/MttLoader.java

URL信息	Url所在文件
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
https://soft.tbs.imtt.qq.com/17421/tbs_res_imtt_tbs_DebugPlugin_DebugPlugin.tbs	com/tencent/smtt/utils/d.java

邮箱线索

邮箱地址	所在文件
permission@gmail.com	com/yanzhenjie/permission/a/c.java

邮箱地址	所在文件
6h@fo.lwft w9oi_2nhels4u@dlilycclglhl.5jlcg_bqh yay@y.u5vcghyy	lib/x86_64/libiconv.so

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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.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_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.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_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.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.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
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.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.NFC	正常	控制近场通信	允许应用程序与近场通信 (NFC) 标签,卡和读卡器进行通信
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
org.simalliance.openmobileapi.SMARTCARD	未知	Unknown permission	Unknown permission from android reference
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器

签名证书

APK is signed
v1 signature: True
v2 signature: True

v3 signature: True
Found 1 unique certificates
Subject: CN=gdjztw.com
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-02-27 03:40:23+00:00
Valid To: 2046-02-21 03:40:23+00:00
Issuer: CN=gdjztw.com
Serial Number: 0x5b138aa1
Hash Algorithm: sha256
md5: 7b7e3892c8768d9de6a2f6a065fec80a
sha1: da73b3894e2b1277b236849c63207e98fa2ee7d5
sha256: 36e0d95a63dc37c4ff6ee48d7e44ade0353ffad98b9f7f3a79245d202d3a28b4
sha512: 6060a6a2acda02afc29778c815815547552cf318d76d549d7bd283dd5e54725345ec682cdcc32527e4d1a2ba31ae95f5f69a97316567a54b2eb0054465d36fdb
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 84ad95dd4e8e40bba0fdd57a79e6a26b8b79ea166c09e5c9a1a3b10f75ac1c25

Exodus威胁情报

名称	分类	URL链接
Bugly		https://reports.exodus-privacy.eu.org/trackers/190

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.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
possible Build.SERIAL check
Build.TAGS check
SIM operator check
network operator name check
subscriber ID check
emulator file check</td></tr>
<tr><td>编译器</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>
