MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

德平堂药业 1.0.APK

APP名称:	德平堂药业
包名:	com.gdjztw.yaoqi.gddptyy
域名线索:	19条
URL线索:	21条
邮箱线索:	2条
分析日期:	2022年1月22日 17:43

文件信息

文件名: dptyy567158.apk
文件大小: 7.31MB
MD5值: 45695154988d266deec175ce88cd5dcb
SHA1值: bf373f4361bab2fb8ad55da500cc3dab19480c78
SHA256值: 671de18923a62c90725ea435b82a1c331ccbe517c045a1bd4c03608e6a922ca7

APP 信息

App名称: 德平堂药业
包名: com.gdjztw.yaoqi.gddptyy
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
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

域名	是否危险域名	服务器信息
m.gddptyy.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
mobile.unionpay.com	good	没有服务器地理信息.
android.bugly.qq.com	good	**IP:** 109.244.244.35 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
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
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

域名	是否危险域名	服务器信息
log.tbs.qq.com	good	IP: 109.244.244.32 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
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
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
ibsbjstar.ccb.com.cn	good	IP: 124.127.108.66 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

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
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
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
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
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
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
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
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

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.gddptyy.com	com/gdjztw/yaodian/yuanzhilindayaofang/b.java
http://m.gddptyy.com/privacy	com/gdjztw/yaodian/yuanzhilindayaofang/e.java
http://m.gddptyy.com/userAgreement	com/gdjztw/yaodian/yuanzhilindayaofang/e.java
https://ibsbjstar.ccb.com.cn/	com/ccb/ccbnetpay/a.java

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

URL信息	Url所在文件
https://log.tbs.qq.com/ajax?c=pu&v=2&k=	com/tencent/smtt/utils/n.java
https://log.tbs.qq.com/ajax?c=pu&tk=	com/tencent/smtt/utils/n.java
https://log.tbs.qq.com/ajax?c=dl&k=	com/tencent/smtt/utils/n.java
https://cfg.imtt.qq.com/tbs?v=2&mk=	com/tencent/smtt/utils/n.java
https://log.tbs.qq.com/ajax?c=ul&v=2&k=	com/tencent/smtt/utils/n.java
https://mqqad.html5.qq.com/adjs	com/tencent/smtt/utils/n.java
https://log.tbs.qq.com/ajax?c=ucfu&k=	com/tencent/smtt/utils/n.java
https://tbsrecovery.imtt.qq.com/getconfig	com/tencent/smtt/utils/n.java
https://soft.tbs.imtt.qq.com/17421/tbs_res_imtt_tbs_DebugPlugin_DebugPlugin.tbs	com/tencent/smtt/utils/d.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

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
android.permission.READ_SETTINGS	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.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
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
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

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: 2021-12-20 02:25:51+00:00
Valid To: 2046-12-14 02:25:51+00:00
Issuer: CN=gdjztw.com
Serial Number: 0x38efc55d
Hash Algorithm: sha256
md5: 2bd867fed5005431d284f6edeb0566c4
sha1: 223cee8143c9bafa6e630711cc4086e160403f08
sha256: f7ed94464358cecdc87520117067e31bde67ab65a3f24908fd46ccba2716656e
sha512: 96490f9e2b2225bc28d9a8f1c25ef1cdd9cd9f660c9baca3558e7f6cfeeeefd0c72142a1fdf222587ef8072782c91cf7bba2f45f2a495748e034f362d612a966
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 420f653cd05c908244e6000780de016bb2582817da4e25365fedd939fc9672b5

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
classes.dex	壳列表 / 详细情况 反虚拟机：Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.BOARD check possible Build.SERIAL check Build.TAGS check SIM operator check network operator name check subscriber ID check emulator file check 编译器：unknown (please file detection issue!)