MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

百龄药多多 1.2.APK

APP名称:	百龄药多多
包名:	com.gdjztw.yaoqi.gxblt
域名线索:	14条
URL线索:	17条
邮箱线索:	2条
分析日期:	2022年1月25日 21:39

文件信息

文件名: blydd.apk
文件大小: 6.8MB
MD5值: 8982ed633c7e044314c5b557a08383b4
SHA1值: f9a53b4488ec712ce1e36b01cfb7155b24895e41
SHA256值: cd7247d577a9e0042971ae56b36b1d4e8aa0093773330c3b80ed0222e5523147

APP 信息

App名称: 百龄药多多
包名: com.gdjztw.yaoqi.gxblt
主活动**Activity:** com.gdjztw.yaodian.yuanzhilindayaofang.MainActivity
安卓版本名称: 1.2
安卓版本: 1

域名线索

域名	是否危险域名	服务器信息
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
ibsbjstar.ccb.com.cn	good	**IP:** 114.251.28.2 **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
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
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.

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
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
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

域名	是否危险域名	服务器信息
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
m.gxbltyy.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
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.gxbltyy.com	com/gdjztw/yaodian/yuanzhilindayaofang/b.java
http://m.gxbltyy.com/privacy	com/gdjztw/yaodian/yuanzhilindayaofang/e.java
http://m.gxbltyy.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
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

URL信息	Url所在文件
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
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

邮箱线索

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

向手机申请的权限	是否危险	类型	详细情况
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
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: 2021-03-12 03:16:58+00:00
Valid To: 2046-03-06 03:16:58+00:00
Issuer: CN=gdjztw.com
Serial Number: 0x71c8b7fc
Hash Algorithm: sha256
md5: 606079c3bbfba69f2c6b689d03761a95
sha1: 0dc15e0dcc8f364a48f35c7ffeb976ca536dbad9

sha256: 1baf0c8cc438fdff4e21c01de0c7401a9e6180100f58f3eb59b3e8a7a8f0be1f
sha512: 37207fafaa1767e1f7dd9bd2e2e5d4b50fbfd3c4957e204bab8683b5aedda036ce884a1df27b84e6747436bb76486a7b7876b1a6c86f1e218aa3fccd674af986
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 3d2eb4f3e51d44bc7039d608bb06f946f0b46a49211f0b202338868a16f7609b

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