MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

百洋医药网 1.0.11.APK

APP名称:	百洋医药网

包名:	com.baiyang
域名线索:	14条
URL线索:	33条
邮箱线索:	1条
分析日期:	2022年1月25日 21:39

文件信息

文件名: byyyw521258.apk
文件大小: 8.47MB
MD5值: f28881b86e9917dd7a68cc24d34ea611
SHA1值: 642abef71f664460dddfb871ff4f397813b11ec5
SHA256值: 06c57602e88d5918d69ea973eef7426a84c46d36b92a4cefd1a8e42ba8ce620e

APP 信息

App名称: 百洋医药网
包名: com.baiyang
主活动Activity: com.baiyang.ui.activity.SplashActivity
安卓版本名称: 1.0.11

安卓版本: 11

域名线索

域名	是否危险域名	服务器信息
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
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
schemas.android.com	good	没有服务器地理信息.
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
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
byyy.baheal.com	good	**IP:** 139.9.142.116 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
t15.baidu.com	good	**IP:** 218.68.136.36 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142220 经度: 117.176666 查看地图: Google Map
www.baidu.com	good	**IP:** 110.242.68.4 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
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

域名	是否危险域名	服务器信息
xml.apache.org	good	**IP:** 151.101.2.132 **所属国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.775700 **经度:** -122.395203 **查看地图:** Google Map
open.weixin.qq.com	good	**IP:** 175.24.219.72 **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
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
gimg2.baidu.com	good	**IP:** 123.125.132.36 **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
www.baidu.com	com/blankj/utilcode/util/NetworkUtils.java
http://xml.apache.org/xslt}indent-amount	com/blankj/utilcode/util/LogUtils.java

URL信息	Url所在文件
https://api.weixin.qq.com/sns/oauth2/access_token?appid=wx882600ef8416ba45&secret=460fd90fffd416004fe16e2a2df657d5&code=	com/baiyang/ui/activity/LoginViewModel.java
http://t15.baidu.com/it/u=3768986255,1243616948&fm=224&app=112&f=JPEG?w=500&h=313&s=192357305B224A0B02DD7CCA0300E0B0	com/baiyang/ui/activity/shopping/ShoppingDetailActivity$shearXian$1.java
http://www.qq.com	com/baiyang/ui/activity/shopping/ShoppingDetailActivity.java
http://www.qq.com	com/baiyang/ui/activity/cuxiao/CuXiaoViewModel.java
http://www.qq.com	com/baiyang/ui/activity/cuxiao/CuXiaoDetailActivity.java
https://gimg2.baidu.com/image_search/src=http%3A%2F%2Fc-ssl.duitang.com%2Fuploads%2Fitem%2F202005%2F27%2F20200527142027_aogqb.thumb.1000_0.jpg&refer=http%3A%2F%2Fc-ssl.duitang.com&app=2002&size=f9999,10000&q=a80&n=0&g=0n&fmt=jpeg?sec=1635218687&t=6a3329b9ffb6cf66de521581b496de92	com/baiyang/ui/fragment/mine/MineViewModel.java
https://api.weixin.qq.com/sns/oauth2/access_token?appid=wx2898c265fe56689c&secret=ec54141c1184679094af78fe353597d7&code=	com/baiyang/wxapi/WXEntryActivity.java
https://api.weixin.qq.com/sns/userinfo?access_token=	com/baiyang/wxapi/WXEntryActivity.java
https://byyy.baheal.com/	com/baiyang/data/source/http/RetrofitClient.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/c.java
https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async	com/tencent/bugly/crashreport/common/strategy/c.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
http://schemas.android.com/apk/res/android	com/afollestad/materialdialogs/prefs/PrefUtil.java
http://www.baidu.com	me/goldze/mvvmhabit/http/NetworkUtil.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Flowable.java

URL信息	Url所在文件
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

邮箱线索

邮箱地址	所在文件
this@webactivity.window	com/baiyang/ui/activity/web/WebActivity.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_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_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.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

向手机申请的权限	是否危险	类型	详细情况
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.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.ANSWER_PHONE_CALLS	危险		允许应用接听来电。

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=by, ST=by, L=by, O=by, OU=by, CN=by
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-10-20 02:25:09+00:00
Valid To: 2046-10-14 02:25:09+00:00
Issuer: C=by, ST=by, L=by, O=by, OU=by, CN=by
Serial Number: 0xdf09e0d
Hash Algorithm: sha256
md5: c19ed6035e9f98320ea332b97eaf2a07
sha1: bbd659c7dbb0dc4703beece31cdd87a0ba256dd1
sha256: 0d4b4e385ccc43120747f1375adb17ca8da86c382788e3c655013fcd67b67a0e
sha512: d241818da13a61c9a99b07ad7b3692ca27bca80c315aa40363978bc43f5124a52fb4649be193406c1221827c0b45db2a83631d0e2e82ef7aa80ec83a59c0a735
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 249d96c95501dd47334e23a6173328fc5a9e9eaae48738e6e0f0d0596b361c6f

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

<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.BRAND check
Build.DEVICE check
Build.PRODUCT check
possible Build.SERIAL check
possible VM 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>反虚拟机</td><td>Build.MANUFACTURER check
Build.TAGS check
emulator file check</td></tr>
<tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

报告由 摸瓜平台 自动生成，并非包含所有检测结果，有疑问请联系管理员。

查诈骗APP | 查木马APP | 违法APP分析 | APK代码分析