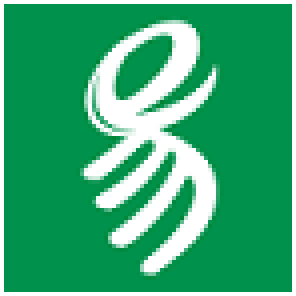
MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成



包裹自提 3.0.0.5.APK

APP名称:	包裹自提
包名:	com.gotop.yjdtzt
域名线索:	8条
URL线索:	12条
邮箱线索:	0条
分析日期:	2022年2月2日 17:02

文件信息

文件名: baoguoziti.apk
文件大小: 2.07MB
MD5值: 5225728390b995d177e8673060a95369
SHA1值: e56f662f807127e5b51cdb372c500593701448de
SHA256值: e16b8d258bed5f7d7ad2a0c8f07e7d3f3e54669bdc3c6c444ed8ecd7f758b6f8

APP 信息

App名称: 包裹自提
包名: com.gotop.yjdtzt
主活动**Activity:** com.gotop.yjdtzt.LoadingActivity
安卓版本名称: 3.0.0.5
安卓版本: 3005

域名线索

域名	是否危险域名	服务器信息
xmlpull.org	good	**IP:** 74.50.61.58 **所属国家:** United States of America **地区:** Texas **城市:** Dallas **纬度:** 32.814899 **经度:** -96.879204 **查看地图:** Google Map

域名	是否危险域名	服务器信息
211.156.200.95	good	**IP:** 211.156.200.95 **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.openmobilealliance.org	good	**IP:** 172.67.75.102 **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
www.w3.org	good	**IP:** 128.30.52.100 **所属国家:** United States of America **地区:** Massachusetts **城市:** Cambridge **纬度:** 42.365078 **经度:** -71.104523 **查看地图:** Google Map
service.search.gnzq.com	good	**IP:** 18.166.248.208 **所属国家:** Hong Kong **地区:** Hong Kong **城市:** Hong Kong **纬度:** 22.285521 **经度:** 114.157692 **查看地图:** Google Map

域名	是否危险域名	服务器信息
www.wireless-village.org	good	**IP:** 172.67.131.214 **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
schemas.xmlsoap.org	good	**IP:** 104.105.231.47 **所属国家:** United States of America **地区:** Georgia **城市:** Atlanta **纬度:** 33.749001 **经度:** -84.387978 **查看地图:** Google Map
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

URL线索

URL信息	Url所在文件
http://211.156.200.95:8081/attach.do?method=apkrenovatemodernized	com/gotop/yjdtzt/yyztlib/main/Activity/YyztMainActivity.java

URL信息	Url所在文件
http://service.search.gnzq.com/	com/gotop/yjdtzt/yyztlib/common/utils/SoapSend1.java
http://211.156.200.95:8082/gnzqService/service/	com/gotop/yjdtzt/yyztlib/common/utils/SoapSend1.java
http://xmlpull.org/v1/doc/properties.html#xmldecl-standalone	org/kxml2/kdom/Document.java
http://www.w3.org/XML/1998/namespace	org/kxml2/wap/WbxmlParser.java
http://www.w3.org/2000/xmlns/	org/kxml2/wap/WbxmlParser.java
http://www.	org/kxml2/wap/wml/Wml.java
https://www.	org/kxml2/wap/wml/Wml.java
http://www.wireless-village.org/CSP	org/kxml2/wap/wv/WV.java
http://www.wireless-village.org/PA	org/kxml2/wap/wv/WV.java
http://www.wireless-village.org/TRC	org/kxml2/wap/wv/WV.java
http://www.openmobilealliance.org/DTD/WV-CSP	org/kxml2/wap/wv/WV.java
http://www.openmobilealliance.org/DTD/WV-PA	org/kxml2/wap/wv/WV.java
http://www.openmobilealliance.org/DTD/WV-TRC	org/kxml2/wap/wv/WV.java
www.wireless-village.org	org/kxml2/wap/wv/WV.java
http://xmlpull.org/v1/doc/features.html#indent-output	org/kxml2/io/KXmlSerializer.java

URL信息	Url所在文件
http://www.w3.org/XML/1998/namespace	org/kxml2/io/KXmlSerializer.java
http://xmlpull.org/v1/doc/	org/kxml2/io/KXmlParser.java
http://www.w3.org/XML/1998/namespace	org/kxml2/io/KXmlParser.java
http://www.w3.org/2000/xmlns/	org/kxml2/io/KXmlParser.java
http://schemas.xmlsoap.org/soap/encoding/	org/ksoap2/SoapEnvelope.java
http://www.w3.org/2003/05/soap-encoding	org/ksoap2/SoapEnvelope.java
http://schemas.xmlsoap.org/soap/envelope/	org/ksoap2/SoapEnvelope.java
http://www.w3.org/2003/05/soap-envelope	org/ksoap2/SoapEnvelope.java
http://www.w3.org/2001/XMLSchema	org/ksoap2/SoapEnvelope.java
http://www.w3.org/1999/XMLSchema	org/ksoap2/SoapEnvelope.java
http://www.w3.org/2001/XMLSchema-instance	org/ksoap2/SoapEnvelope.java
http://www.w3.org/1999/XMLSchema-instance	org/ksoap2/SoapEnvelope.java
http://xml.apache.org/xml-soap	org/ksoap2/serialization/MarshalHashtable.java
http://xmlpull.org/v1/doc/features.html#process-docdecl	org/xmlpull/v1/XmlPullParser.java
http://xmlpull.org/v1/doc/features.html#process-namespaces	org/xmlpull/v1/XmlPullParser.java

URL信息	Url所在文件
http://xmlpull.org/v1/doc/features.html#report-namespace-prefixes	org/xmlpull/v1/XmlPullParser.java
http://xmlpull.org/v1/doc/features.html#validation	org/xmlpull/v1/XmlPullParser.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.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.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_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.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.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.RESTART_PACKAGES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
android.permission.INTERNET	正常	互联网接入	允许应用程序创建网络套接字

向手机申请的权限	是否危险	类型	详细情况
android.permission.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备
android.permission.BLUETOOTH_ADMIN	正常	蓝牙管理	允许应用程序发现和配对蓝牙设备。
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_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
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.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.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_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.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.KILL_BACKGROUND_PROCESSES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: CN=1
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2014-07-24 01:30:28+00:00
Valid To: 3013-11-24 01:30:28+00:00
Issuer: CN=1
Serial Number: 0x53d061b4
Hash Algorithm: sha1
md5: b6c0a9c61b874c029dd5ef34d9f00a66
sha1: 29df47892f0d107ac4d413c1409f8cee8c6187ef
sha256: ad4baa0dd37b775972b19d53978a8572011dd67342662046a6f651d8a0be1483
sha512: c88ae6a6e8435e8580f815962697041f979d44d8e80090b7a57c94b8502e22397b8b1d4ba8f2767f24a6a0eda1c111ee01a8e3276cbac08f012793c92dcdbb6a
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: 38aa58bee55e64d99836c2de916be9d2b6c9696931bdfa641e1a48c3b660b0ce

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>编译器</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>
