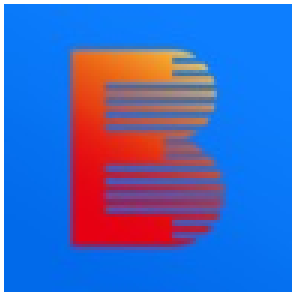
MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成



新业务在线 2.0.09.APK

APP名称:	新业务在线
包名:	com.zgbd.yfgd
域名线索:	26条
URL线索:	31条
邮箱线索:	0条
分析日期:	2022年2月3日 12:46

文件信息

文件名: xywzx577984.apk
文件大小: 3.48MB
MD5值: cbfe6ebc3b48335060a0d90417e74aa5
SHA1值: 633d5e1297b855f2df68504a368c471c48988dc9
SHA256值: a0a80034e6b08364f2a545e396a0bf3d55e3c38282dbf92455002d64c3733ac9

APP 信息

App名称: 新业务在线
包名: com.zgbd.yfgd
主活动**Activity:** com.zgbd.yfgd.home.MainActivity
安卓版本名称: 2.0.09
安卓版本: 35

域名线索

域名	是否危险域名	服务器信息
seed.pgyer.com	good	**IP:** 121.37.246.9 **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

域名	是否危险域名	服务器信息
console.ctayun.com	good	**IP:** 120.25.247.178 **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
www.vocsystem.cn	good	**IP:** 119.23.57.45 **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
schemas.android.com	good	没有服务器地理信息.
canc.cebenvironment.com.cn	good	**IP:** 121.43.154.28 **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
restsdk.amap.com	good	**IP:** 106.11.43.113 **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

域名	是否危险域名	服务器信息
apilocate.amap.com	good	**IP:** 59.82.31.183 **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
d-gt.getui.com	good	没有服务器地理信息.
dualstack-a.apilocate.amap.com	good	**IP:** 106.11.40.50 **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
sdk.open.phone.igexin.com	good	**IP:** 124.160.127.196 **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
lbs.amap.com	good	**IP:** 59.82.60.46 **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

域名	是否危险域名	服务器信息
119.23.57.45	good	**IP:** 119.23.57.45 **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
www.pgyer.com	good	**IP:** 203.107.44.30 **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
file.ctayun.com	good	**IP:** 120.25.247.178 **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
dualstack-arestapi.amap.com	good	**IP:** 39.98.22.142 **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

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
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
abroad.apilocate.amap.com	good	**IP:** 59.82.39.53 **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
cgicol.amap.com	good	**IP:** 59.82.60.45 **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
ns.adobe.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
c-hzgt2.getui.com	good	**IP:** 183.131.7.106 **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
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
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
yf.vocsystem.cn	good	**IP:** 120.78.217.251 **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

域名	是否危险域名	服务器信息
collecter.pgyer.com	good	**IP:** 42.194.227.90 **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
lfsx.vip	good	**IP:** 125.37.206.224 **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

URL线索

URL信息	Url所在文件
http://xml.apache.org/xslt}indent-amount	com/blankj/utilcode/util/c.java
http://cgicol.amap.com/collection/collectData?src=baseCol&ver=v74&	com/loc/cc.java
http://restsdk.amap.com	com/loc/s.java
http://dualstack-arestapi.amap.com/v3/geocode/regeo	com/loc/ef.java
http://restsdk.amap.com/v3/geocode/regeo	com/loc/ef.java

URL信息	Url所在文件
https://restsdk.amap.com/v3/iasdkauth	com/loc/l.java
https://dualstack-arestapi.amap.com/v3/iasdkauth	com/loc/l.java
http://apilocate.amap.com/mobile/binary	com/loc/ek.java
http://dualstack-a.apilocate.amap.com/mobile/binary	com/loc/ek.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/ek.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/ed.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/eo.java
http://restsdk.amap.com/v3/place/text?	com/loc/a.java
http://restsdk.amap.com/v3/config/district?	com/loc/a.java
http://restsdk.amap.com/v3/place/around?	com/loc/a.java
http://debugtbs.qq.com	com/tencent/smtt/sdk/WebView.java
http://debugx5.qq.com	com/tencent/smtt/sdk/WebView.java
http://debugtbs.qq.com?10000	com/tencent/smtt/sdk/WebView.java
http://mdc.html5.qq.com/d/directdown.jsp?channel_id=11047	com/tencent/smtt/sdk/b/a/a.java
http://mdc.html5.qq.com/d/directdown.jsp?channel_id=11041	com/tencent/smtt/sdk/b/a/a.java

URL信息	Url所在文件
http://mdc.html5.qq.com/mh?channel_id=50079&u=	com/tencent/smtt/sdk/a/a.java
https://sdk.open.phone.igexin.com/api.php	com/igexin/push/a.java
http://c-hzgt2.getui.com/api.php	com/igexin/push/a.java
https://d-gt.getui.com/api.htm	com/igexin/push/a.java
http://bi.	com/igexin/push/config/b.java
http://config.	com/igexin/push/config/b.java
http://bi.	com/igexin/push/config/g.java
http://config.	com/igexin/push/config/g.java
http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/查看错误码说明	com/amap/api/location/AMapLocation.java
https://seed.pgyer.com/vJOlUDPI	com/pgyer/pgyersdk/PgyerSDKManager.java
https://seed.pgyer.com/ENoD6m4t	com/pgyer/pgyersdk/PgyerSDKManager.java
https://www.pgyer.com/apiv2/app/check	com/pgyer/pgyersdk/p010o0O0O/Ooo.java
https://collecter.pgyer.com/	com/pgyer/pgyersdk/p010o0O0O/Ooo.java
http://collecter.pgyer.com/	com/pgyer/pgyersdk/p009oO/Oo0.java
http://ns.adobe.com/xap/1.0/	t0/a.java

URL信息	Url所在文件
http://www.vocsystem.cn	x4/k.java
http://lfsx.vip/h5/hybrid/html/map.html	x4/a.java
http://119.23.57.45:8009/yfep/#	o4/a.java
http://canc.cebenvironment.com.cn/dist/#	o4/a.java
https://canc.cebenvironment.com.cn/h5/index.html#	o4/a.java
http://www.vocsystem.cn	o4/a.java
https://canc.cebenvironment.com.cn	o4/a.java
https://www.pgyer.com/apiv2/app/builds	o4/a.java
http://file.ctayun.com/cheta/console/page/hw/guide/guide0.png	o4/a.java
http://file.ctayun.com/cheta/console/page/hw/guide/guide1.png	o4/a.java
http://file.ctayun.com/cheta/console/page/hw/guide/guide2.png	o4/a.java
http://file.ctayun.com/cheta/console/page/hw/guide/guide3.png	o4/a.java
http://console.ctayun.com/system	o4/a.java
http://yf.vocsystem.cn:11010	o4/a.java
http://schemas.android.com/apk/res/android	b0/i.java

URL信息	Url所在文件
http://file.ctayun.com/cheta/console/page/demo/privacyAgreement_gd.html	Android String Resource

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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息
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.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.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
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.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.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.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.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	正常		应用程序必须持有的权限才能使用Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
android.permission.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
android.permission.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕
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_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference
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.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.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.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.ACCESS_BACKGROUND_LOCATION	危险	后台访问位置	允许应用程序在后台访问位置
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.ACCESS_LOCATION_EXTRA_COMMANDS	正常	访问额外的位置提供程序命令	访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作
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。

向手机申请的权限	是否危险	类型	详细情况
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
getui.permission.GetuiService.com.zgbd.yfgd	未知	Unknown permission	Unknown permission from android reference
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=key0, ST=key0, L=key0, O=key0, OU=key0, CN=key0
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-06-14 14:53:29+00:00
Valid To: 2046-06-08 14:53:29+00:00
Issuer: C=key0, ST=key0, L=key0, O=key0, OU=key0, CN=key0
Serial Number: 0x4762caeb
Hash Algorithm: sha256
md5: 4bd9c03a7f152ed619757327ba602d8f
sha1: eda83ebb02c1304d063a2832d3a59329188d3461
sha256: 0955876428b2afee3cc00de5e38de82998d475bcadca16a7acca566d06f78c8d
sha512: 678a451276abbfff1f6367aa1b7c56b180c6453a2dedbc33635093d5e39e73b53ffbf6560113bbfe81dddf3c7fe5d0ede0f70445fe8138b5bf591badd71f0210
PublicKey Algorithm: rsa
Bit Size: 2048

Fingerprint: b4137d15b6879e8268e1ba904640404803321ed30bdbdf6c7a8e6fa53b7e519e

Exodus威胁情报

名称	分类	URL链接
AutoNavi / Amap	Location	https://reports.exodus-privacy.eu.org/trackers/361

硬编码敏感信息

可能的敏感信息
"PGYER_API_KEY" : "04c402ba3338b252c2798b10d05f5a14"
"PGYER_FRONTJS_KEY" : "e6789c4530e0741dabfcdaa507b5d0d9"
"amapkey" : "32280dba6ad6dcd92b76166bee8f0464"
"pgyappkey" : "c291acab351a1f04389a633bc95a673e"

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
device ID check
subscriber ID check</td></tr>
<tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr>
<tr><td>模糊器</td><td>unreadable field names
unreadable method names</td></tr>
</table>
</td></tr>
</table>
