MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

GXB 2.0.28.APK

APP名称:	GXB
包名:	m.ue5
域名线索:	6条
URL线索:	9条
邮箱线索:	1条
分析日期:	2022年2月2日 11:50

文件信息

文件名: gzhifu.apk
文件大小: 1.78MB
MD5值: d92faebfaeb6a6bf2f1a22642444138c
SHA1值: 7b73a6b67cfe4834a4207a6a4152ae404e122158
SHA256值: d17da39aca376349ae4ef0f32ebbde742b4a3f493785fcee502f42e82eb28b4b

APP 信息

App名称: GXB
包名: m.ue5
主活动**Activity:** com.uzmap.pkg.LauncherUI
安卓版本名称: 2.0.28
安卓版本: 191

域名线索

域名	是否危险域名	服务器信息
r.apicloud.com	good	**IP:** 182.92.145.58 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
d.apicloud.com	good	**IP:** 47.94.176.24 **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
as.apicloud.com	good	没有服务器地理信息.
p.apicloud.com	good	**IP:** 47.93.154.30 **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
a.apicloud.com	good	**IP:** 182.92.145.58 **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
s.apicloud.com	good	没有服务器地理信息.

URL线索

URL信息	Url所在文件
https://a.apicloud.com	compile/Properties.java
https://d.apicloud.com	compile/Properties.java
https://s.apicloud.com	compile/Properties.java
https://p.apicloud.com	compile/Properties.java
https://r.apicloud.com	compile/Properties.java
https://as.apicloud.com	compile/Properties.java

邮箱线索

邮箱地址	所在文件
developer@apicloud.com	com/uzmap/pkg/uzcore/b/d.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
com.huawei.android.launcher.permission.CHANGE_BADGE	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
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_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_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_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.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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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

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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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。

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=(zh), ST=(Beijing), L=(Beijing), O=(woliuwny@outlook.com), OU=(woliuwny@outlook.com), CN=(woliuwny@outlook.com)

Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-08-15 14:50:33+00:00
Valid To: 2120-07-22 14:50:33+00:00
Issuer: C=(zh), ST=(Beijing), L=(Beijing), O=(woliuwny@outlook.com), OU=(woliuwny@outlook.com), CN=(woliuwny@outlook.com)
Serial Number: 0x4171f8e1
Hash Algorithm: sha256
md5: 007da875f9161bc4e18ed3b405d93491
sha1: d207536166fef36cf6e32ea39c126ce149df6ba1
sha256: 86b58226c2b80ce2dc3de0ae7716344fefa5a1c35097179d80391dbd9199cb19
sha512: fba09a842052788b31f82be900368247fd64ceede378be16a0067de813a30f78510db26171449cd2579dbac5ddb9c894ddaa4601e1f95705fa367a87f30db627
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: 9f454148e9a1ff113109d0c4f736ee68695121525863ae39614ead01121e3a30

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
possible Build.SERIAL check</td></tr>
<tr><td>编译器</td><td>dx</td></tr>
</table>
</td></tr>
</table>
