

APP线索分析报告

报告由模瓜APP分析平台(mogua.co) 生成



♣ 工友驿站 0.0.21.APK

APP名称: 工友驿站

包名: ylu.we56332

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 20:01

文件名: gongyouyizhan.apk

文件大小: 2.61MB

MD5值: 436b354185c033efe9763c2fc770c5e7

SHA1值: 93cbdd09c25a0b7ca993927c77e175b0830fb7d8

SHA256值: 9b630cb933d17a43c293fc6d681c37234da3be7fcd758a158e90cc34d5dad56b

i APP 信息

App名称: 工友驿站 包名: ylu.we56332

主活动**Activity:** com.uzmap.pkg.LauncherUI

安卓版本名称: 0.0.21

安卓版本: 21

0 域名线索

域名	是否危险域名	服务器信息
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
as.apicloud.com	good	没有服务器地理信息.

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
s.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
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



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。
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



APK is signed v1 signature: True v2 signature: True v3 signature: False

Found 1 unique certificates

Subject: C=(zh), ST=(Beijing), L=(Beijing), O=(mweoy357@126.com), OU=(1), CN=(1)

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2020-09-20 13:03:58+00:00 Valid To: 2120-08-27 13:03:58+00:00

Issuer: C=(zh), ST=(Beijing), L=(Beijing), O=(mweoy357@126.com), OU=(1), CN=(1)

Serial Number: 0x52a255b0 Hash Algorithm: sha256

md5: b8f6869f4ef7d55975383e1e8ef58b31

sha1: 56a35c4a96b2ea7866eeefde8122253dbcf8b391

sha256: d4a1cd0136941b3e82a01c1ce50fa1ab187ae4451c0e649fb97878f1aff83f0c

sha512: 4acc13ae8fb0621bc226d14c400c62530d74c186d2ec6f29bb7328932a72dcc30f2ea022b805fb6984cc3ff2d17a9ca42581057634042ee824c7d5f4d7bbeb0e

PublicKey Algorithm: rsa

Bit Size: 1024

Fingerprint: 039fec74c5814451480f3880174a6fdfd5f6a716359c23f3c30bcccfd45ffdf5



活动(ACTIVITY)	通信(INTENT)
com.uzmap.pkg.EntranceActivity	Schemes: gongyouyizhan://,

命加壳分析

文件列表	分析结果
------	------

壳孩	売列表 详细情况	
反虚 classes.dex	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check possible Build.SERIAL check	
编译	a译器 dx	

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