MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

纸有你 0.0.4.APK

APP名称:	纸有你
包名:	com.advertdh.pageTeacher
域名线索:	7条
URL线索:	19条
邮箱线索:	1条
分析日期:	2022年2月3日 13:20

文件信息

文件名: zhiyouni.apk
文件大小: 2.46MB
MD5值: aee663098f47d34b344685927439a567
SHA1值: 576ff4d2452416ddf2d1da3bab4aef1f6d7621f8
SHA256值: 0cf3c9af6aa5364b961bd9cc5f5979de095d82bc74cbe7221aaf8f89f8be1a0e

APP 信息

App名称: 纸有你
包名: com.advertdh.pageTeacher
主活动**Activity:** com.uzmap.pkg.LauncherUI
安卓版本名称: 0.0.4
安卓版本: 4

域名线索

域名	是否危险域名	服务器信息
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

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
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.
as.apicloud.com	good	没有服务器地理信息.
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
schemas.android.com	good	没有服务器地理信息.

URL信息	Url所在文件
http://schemas.android.com/apk/res/android	com/apicloud/third/gif/GifTextureView.java
http://schemas.android.com/apk/res/android	com/apicloud/third/gif/GifTextView.java
http://schemas.android.com/apk/res/android	com/apicloud/third/gif/GifViewUtils.java
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_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.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.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=(18605559916@163.com), OU=(18605559916@163.com), CN=(b18605559916)
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-08-12 03:08:26+00:00
Valid To: 2121-07-19 03:08:26+00:00
Issuer: C=(zh), ST=(Beijing), L=(Beijing), O=(18605559916@163.com), OU=(18605559916@163.com), CN=(b18605559916)
Serial Number: 0x38586673
Hash Algorithm: sha256
md5: f845920729e90f98358ff986670b2e9b
sha1: a108865a7d7832a9b0bbc3dfd50f04225fc7be26
sha256: 7a4b79b6a8cb45157440a06804cb2d6e2626b751756b1f71bde4c14f3500b0ae
sha512: cb848d6bbaff5ec1b30f5a35df44a55cc39cd744406e149b80013aec9edde468cb686d80742d8ffb31746f0cfed72f35718978c0035a558f759ab7be2f1b4c15
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: 3176ab49f7cf32ee02bd787079ebba521f7280924995cde114949609c2d3e3e6

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</td></tr>
<tr><td>编译器</td><td>r8</td></tr>
</table>
</td></tr>
</table>
