MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

e支付 0.0.6.APK

APP名称:	e支付
包名:	com.y15062147741.kjz
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 11:39

文件信息

文件名: ezhifu.apk
文件大小: 2.04MB
MD5值: 425ef3bfc70c546f1d2de8d91be9e37d
SHA1值: 759c53fb71f5b38c89ee8e53548e7a5b937d1c65
SHA256值: 2a92bd6d8db79eeae98e648d61d6e4f790633b2200c8a9f13e0bef7c85d331c8

APP 信息

App名称: e支付
包名: com.y15062147741.kjz
主活动**Activity:** com.uzmap.pkg.LauncherUI
安卓版本名称: 0.0.6
安卓版本: 6

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。
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

签名证书

APK is signed
v1 signature: True
v2 signature: False

v3 signature: False
Found 1 unique certificates
Subject: C=(zh), ST=(nanjing), L=(nanjing), O=(15062147741@163.com), OU=(15062147741@163.com), CN=(15062147741@163.com)
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-09-09 03:46:10+00:00
Valid To: 2120-08-16 03:46:10+00:00
Issuer: C=(zh), ST=(nanjing), L=(nanjing), O=(15062147741@163.com), OU=(15062147741@163.com), CN=(15062147741@163.com)
Serial Number: 0x29c207d6
Hash Algorithm: sha256
md5: 0034cda2d62cf1be3a19c6743adf32df
sha1: dea0bce3e536f60b98286c3653d45c20cc4419a8
sha256: 22ed2e27e5eab61864ac67b3303849cc164dcf054f9172d2061ffe2897507089
sha512: 12b22218b1ecafbad286bb68c79cba58c7364eb24c9b8e9bcc2494537c1ef76043d7978ec667eedec9829543865846c3a0ae5604ab0eca0de8ec7161f409e105

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