MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

弹个猪 1.0.0.APK

APP名称:	弹个猪
包名:	com.pigs_app
域名线索:	6条
URL线索:	6条
邮箱线索:	0条
分析日期:	2022年2月2日 13:18

文件信息

文件名: tangezhu.apk
文件大小: 7.85MB
MD5值: 207a10b81010e622886bc383a0a40b7e
SHA1值: 1627396d796e8abdf72e238bacdd6bda44db4d00
SHA256值: 6c396f0aa17f922a1eb55ec50247b8ca662cbb210f804a5b65a791de2cab1b0b

APP 信息

App名称: 弹个猪
包名: com.pigs_app
主活动**Activity:** com.pigs_app.MainActivity
安卓版本名称: 1.0.0
安卓版本: 1

域名线索

域名	是否危险域名	服务器信息
tsis.jpush.cn	good	**IP:** 103.230.236.38 所属国家: China 地区: Fujian 城市: Xiamen 纬度: 24.479790 经度: 118.081871 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
pingma.qq.com	good	**IP:** 119.45.78.184 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
mta.qq.com	good	**IP:** 111.161.14.94 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
mta.oa.com	good	**IP:** 193.123.33.15 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam 纬度: 52.374031 经度: 4.889690 查看地图: Google Map
182.92.20.189	good	**IP:** 182.92.20.189 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线索

URL信息	Url所在文件
http://mta.qq.com/	com/tencent/wxop/stat/e.java
http://mta.oa.com/	com/tencent/wxop/stat/e.java
http://pingma.qq.com:80/mstat/report	com/tencent/wxop/stat/c.java
https://tsis.jpush.cn	cn/jiguang/c/a.java
http://182.92.20.189:9099/	cn/jiguang/a/a/c/i.java
http://ns.adobe.com/xap/1.0/	lib/armeabi-v7a/libimagepipeline.so

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
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

向手机申请的权限	是否危险	类型	详细情况
com.pigs_app.permission.JPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
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.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.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.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
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。
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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
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

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.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.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_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.CHANGE_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。
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

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=cn, ST=bj, L=bj, O=firewing, OU=friewing, CN=jj

Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-02-27 02:45:31+00:00
Valid To: 2046-07-15 02:45:31+00:00
Issuer: C=cn, ST=bj, L=bj, O=firewing, OU=friewing, CN=jj
Serial Number: 0x6e1189d3
Hash Algorithm: sha256
md5: c5bb89a13834cd0a2939b05fa4e8ace9
sha1: 2dd7f2d6c1255cb311ba569cd56fec79259130ef
sha256: a4dd95cb03e190aa57becaa9f8ccc8f270f499e4a3c743d7b45040efb6737870
sha512: f086e3264214001400928b8ceec7eb2749ced9e9dced91249fc294c9e74144604bb918836e3047f30d7317abc85d8319acc53a5b427c9849b9de9e68ef4629f7
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 50a4df99d8361539a9e159a411150a0b1a3cfb022ee2de1538efea27b2ecf7c2

Exodus威胁情报

名称	分类	URL链接
JiGuang Aurora Mobile JPush	Analytics	https://reports.exodus-privacy.eu.org/trackers/343
Tencent Stats	Analytics	https://reports.exodus-privacy.eu.org/trackers/116

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.pigs_app.MainActivity	Schemes: pigs_app://,

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.MANUFACTURER check
Build.BOARD check
possible Build.SERIAL 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>
</table>
</td></tr>
</table>
