MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

欢喜岛屿 1.0.0.APK

APP名称:	欢喜岛屿
包名:	com.zhaiteng.shenteng
域名线索:	8条
URL线索:	8条
邮箱线索:	0条
分析日期:	2022年1月28日 23:59

文件信息

文件名: huanxidaoyu.apk
文件大小: 5.98MB
MD5值: f5ce8816e173661e730c4ac19b24ce46
SHA1值: 82862a3f70cefe3f22e0621dcd4e8cd85b8a07da
SHA256值: 39a315f5c66226a4c23d88250f5dcd77b7a4fdda7e1ef720ccd85d1e60759bd3

APP 信息

App名称: 欢喜岛屿
包名: com.zhaiteng.shenteng
主活动**Activity:** com.wb.cardsocial.activity.WelcomeActivity
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
www.talkingdata.net	good	**IP:** 116.196.122.26 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

域名	是否危险域名	服务器信息
i.tddmp.com	good	**IP:** 116.196.71.30 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
me.xdrig.com	good	**IP:** 116.198.14.129 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
av1.xdrig.com	good	**IP:** 116.198.14.55 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
youyu-qinqin.oss-cn-shenzhen.aliyuncs.com	good	**IP:** 113.96.63.209 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298 查看地图: Google Map

域名	是否危险域名	服务器信息
cloud.xdrig.com	good	**IP:** 116.198.14.43 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
www.baidu.com	good	**IP:** 110.242.68.4 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280 查看地图: Google Map
langu-ugirl.oss-cn-shenzhen.aliyuncs.com	good	**IP:** 120.77.166.77 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
https://youyu-qinqin.oss-cn-shenzhen.aliyuncs.com/icon/1607417392308-200-81-1.jpg	com/k/base/Constants.java

URL信息	Url所在文件
https://langu-ugirl.oss-cn-shenzhen.aliyuncs.com/icon/1607417392476-200-81-1.jpg	com/k/base/Constants.java
https://av1.xdrig.com/u/a/v1	com/tendcloud/tenddata/aa.java
https://cloud.xdrig.com/configcloud/rest/sdk/match	com/tendcloud/tenddata/aa.java
http://i.tddmp.com/a/	com/tendcloud/tenddata/eq.java
https://me.xdrig.com	com/tendcloud/tenddata/e.java
www.talkingdata.net	com/tendcloud/tenddata/bj.java
https://www.baidu.com	com/up/update/Net.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
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.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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径

向手机申请的权限	是否危险	类型	详细情况
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

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=com.zhaiteng.shenteng, ST=com.zhaiteng.shenteng, L=com.zhaiteng.shenteng, O=com.zhaiteng.shenteng, OU=com.zhaiteng.shenteng, CN=com.zhaiteng.shenteng
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-12-08 08:50:34+00:00
Valid To: 2045-12-02 08:50:34+00:00
Issuer: C=com.zhaiteng.shenteng, ST=com.zhaiteng.shenteng, L=com.zhaiteng.shenteng, O=com.zhaiteng.shenteng, OU=com.zhaiteng.shenteng, CN=com.zhaiteng.shenteng
Serial Number: 0x3e496a6
Hash Algorithm: sha256
md5: be6f7df419abd38d0f4730ac47805a11
sha1: f7a8cc355be786b9eaf6d5d451623dd34153d345
sha256: 86c3e3d9fdbab583a73bdaacb61624e776ea0acf661a6094293088422c44fe10
sha512: 420a7827d43d08008e8ef290d6405bfe0234b6f490acdbafc141f48bbb04621ca74133a5614b85ebb8d469551c92cad402f5cedc48130dd63f6b45a121318e60
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: aa395b30206c7ff3e3747e322db6861bac85d020d0b7651aea7cd6e82af7a7f4

Exodus威胁情报

名称	分类	URL链接
TalkingData	Analytics, Advertisement	https://reports.exodus-privacy.eu.org/trackers/293

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
SIM operator check
network operator name check</td></tr>
<tr><td>编译器</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>