MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

肇东交警 00.01.0001.APK

APP名称:	肇东交警
包名:	com.zuolan.zhaodong
域名线索:	5条
URL线索:	3条
邮箱线索:	0条
分析日期:	2022年1月26日 20:26

文件信息

文件名: zhaodonjiaoj.apk
文件大小: 3.84MB
MD5值: f0f92225d8f824a49c9468dc3a3abb31
SHA1值: ecd7f1ca7866c5fdfafafb276371fe123459c89a
SHA256值: c9b5aae08b3a3d8fe3a09a63ba5a51508371c29813bd127c487efe66e191b15e

APP 信息

App名称: 肇东交警
包名: com.zuolan.zhaodong
主活动**Activity:** org.zywx.wbpalmstar.engine.LoadingActivity
安卓版本名称: 00.01.0001
安卓版本: 103

域名线索

域名	是否危险域名	服务器信息
storeb.appcan.cn	good	**IP:** 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000 查看地图: Google Map

域名	是否危险域名	服务器信息
newdc.appcan.cn	good	**IP:** 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000 查看地图: Google Map
newpush.appcan.cn	good	**IP:** 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000 查看地图: Google Map
rqd.uu.qq.com	good	**IP:** 182.254.88.185 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
android.bugly.qq.com	good	**IP:** 109.244.244.35 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

URL线索

URL信息	Url所在文件
http://android.bugly.qq.com/rqd/async	com/tencent/bugly/lejiagu/crashreport/common/strategy/StrategyBean.java
http://rqd.uu.qq.com/rqd/sync	com/tencent/bugly/lejiagu/crashreport/common/strategy/StrategyBean.java
http://android.bugly.qq.com/rqd/async	com/tencent/bugly/legu/crashreport/common/strategy/StrategyBean.java
http://rqd.uu.qq.com/rqd/sync	com/tencent/bugly/legu/crashreport/common/strategy/StrategyBean.java
http://newdc.appcan.cn/	Android String Resource
http://newpush.appcan.cn/	Android String Resource
http://storeb.appcan.cn/	Android String Resource

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

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.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.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.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
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.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

签名证书

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=cn
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2018-02-26 07:35:03+00:00
Valid To: 2043-02-20 07:35:03+00:00

Issuer: C=cn
Serial Number: 0x22b05e8
Hash Algorithm: sha256
md5: 5e5220b40e78e5d858c0e5115bfb99e0
sha1: a43c2c4b7eec9b2ab6b83319472453af08876a32
sha256: dabfd7cea5daa0f4f850fa5baeec3ede38ce58df32789672b3d7a8285869ed01
sha512: 0db122d09c8f1f6904c578e28228efa06be0c87011436bc546c27c2f75f36d833dbeeab1748d9d530affd2f8ef52207a299df816c4228936be58e44cf5ab7ba8

Exodus威胁情报

名称	分类	URL链接
Bugly		https://reports.exodus-privacy.eu.org/trackers/190

硬编码敏感信息

可能的敏感信息
"appkey" : "c60ba1ea-6092-65cb-6421-d3cbb9d80f84"

应用内通信

活动(ACTIVITY)	通信(INTENT)
org.zywx.wbpalmstar.engine.EBrowserActivity	Schemes: appcanscheme://,

加壳分析

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>APK包</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>打包</td><td>Mobile Tencent Protect</td></tr>
</table>
</td></tr>
<tr><td>lib/armeabi/mix.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>编译器</td><td>dx</td></tr>
</table>
</td></tr>
<tr><td>lib/armeabi/mixz.dex!classes.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>编译器</td><td>dx</td></tr>
</table>
</td></tr>
</table>

文件列表	分析结果
classes.dex	壳列表 / 详细情况 打包: Mobile Tencent Protect 反虚拟机: Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.TAGS check subscriber ID check 编译器: dexlib 2.x

---