MoGua

# APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成


以诺行车管家 1.2.APK

| | |
|---|---|
| APP名称: | 以诺行车管家 |
| 包名: | com.enoch.erp |
| 域名线索: | 4条 |
| URL线索: | 11条 |
| 邮箱线索: | 0条 |
| 分析日期: | 2022年2月3日 13:04 |

## 文件信息

文件名: yinuoxingcheguanjia.apk
文件大小: 8.64MB
**MD5值:** c5cfd6b3d05d1df98ff66b4af7619ecc
**SHA1值:** f6da7e4ad536a2ccc7024cd7a669fa96e309c824
**SHA256值:** d23ec0472553c9debf13fddd5f75e878fa6452dea5c70ae8dd961208265185de

# APP 信息

**App名称:** 以诺行车管家
包名: com.enoch.erp
主活动**Activity:** com.enoch.erp.modules.splash.SplashActivity
安卓版本名称: 1.2
安卓版本: 12

# 域名线索

| 域名 | 是否危险域名 | 服务器信息 |
| --- | --- | --- |
| enocloud.enoch-car.com | good | **IP:** 47.99.123.54<br>所属国家: China<br>地区: Zhejiang<br>城市: Hangzhou<br>纬度: 30.293650<br>经度: 120.161423<br>查看地图: Google Map |
| schemas.android.com | good | 没有服务器地理信息. |

| 域名 | 是否危险域名 | 服务器信息 |
| --- | --- | --- |
| errlog.umeng.com | good | **IP:** 116.132.223.36<br>所属国家: China<br>地区: Beijing<br>城市: Beijing<br>纬度: 39.907501<br>经度: 116.397232<br>查看地图: Google Map |
| errlogos.umeng.com | good | **IP:** 47.246.110.18<br>所属国家: Hong Kong<br>地区: Hong Kong<br>城市: Hong Kong<br>纬度: 22.285521<br>经度: 114.157692<br>查看地图: Google Map |

## URL线索

| URL信息 | Url所在文件 |
| --- | --- |
| https://errlog.umeng.com/api/crashsdk/logcollect | com/efs/sdk/base/core/f/c.java |
| https://errlogos.umeng.com/api/crashsdk/logcollect | com/efs/sdk/base/core/controller/ControllerCenter.java |
| https://errlog.umeng.com/api/crashsdk/logcollect | com/efs/sdk/base/core/controller/ControllerCenter.java |
| https://enocloud.enoch-car.com/ | com/enoch/erp/http/NetworkManager.java |
| http://schemas.android.com/apk/res/android | com/enoch/erp/view/SlidingTabLayout.java |

| URL信息 | Url所在文件 |
| --- | --- |
| https://errlog.umeng.com/api/crashsdk/logcollect | lib/armeabi-v7a/libcrashsdk.so |
| https://errlogos.umeng.com/api/crashsdk/logcollect | lib/armeabi-v7a/libcrashsdk.so |
| https://errlog.umeng.com | lib/armeabi-v7a/libcrashsdk.so |
| https://errlogos.umeng.com | lib/armeabi-v7a/libcrashsdk.so |
| https://errlog.umeng.com/api/crashsdk/logcollect | lib/x86/libcrashsdk.so |
| https://errlogos.umeng.com/api/crashsdk/logcollect | lib/x86/libcrashsdk.so |
| https://errlog.umeng.com | lib/x86/libcrashsdk.so |
| https://errlogos.umeng.com | lib/x86/libcrashsdk.so |
| https://errlog.umeng.com/api/crashsdk/logcollect | lib/arm64-v8a/libcrashsdk.so |
| https://errlogos.umeng.com/api/crashsdk/logcollect | lib/arm64-v8a/libcrashsdk.so |
| https://errlog.umeng.com | lib/arm64-v8a/libcrashsdk.so |
| https://errlogos.umeng.com | lib/arm64-v8a/libcrashsdk.so |
| https://errlog.umeng.com/api/crashsdk/logcollect | lib/armeabi/libcrashsdk.so |
| https://errlogos.umeng.com/api/crashsdk/logcollect | lib/armeabi/libcrashsdk.so |
| https://errlog.umeng.com | lib/armeabi/libcrashsdk.so |

| URL信息 | Url所在文件 |
| --- | --- |
| https://errlogos.umeng.com | lib/armeabi/libcrashsdk.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.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 |
| 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_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.RECORD_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.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 |

## 签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=310000, ST=浙江, L=杭州, O=杭州以诺行汽车科技股份有限公司, OU=杭州以诺行汽车科技股份有限公司, CN=周山
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-08-03 01:28:44+00:00
Valid To: 2046-07-28 01:28:44+00:00
Issuer: C=310000, ST=浙江, L=杭州, O=杭州以诺行汽车科技股份有限公司, OU=杭州以诺行汽车科技股份有限公司, CN=周山
Serial Number: 0x3974c7af
Hash Algorithm: sha256
md5: ce4211feb3ecfe4d5d1e9bb9e8505f86
sha1: 8107941dd3c21259b4d49dfae0e3a2d92fe7aa42
sha256: 19a3e7feb554f1f6903df7885267ac226f57b071623d239c11400573712660f0
sha512: c5b2d21f0eebf2948b6900bb0af6152d0a9eae144590cc45db34235edf8bb6e5bc85b03087b918f956b35c1ce58263d1b85f3c85838c83acd33371ba05ed7716
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 0de4121160687461e22715e6625eb4873f19c911662dfc6ceaf3bc187b826f9c

# Exodus威胁情报

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| Umeng Analytics | | https://reports.exodus-privacy.eu.org/trackers/119 |

# 硬编码敏感信息

| 可能的敏感信息 |
| --- |
| "one_key_login" : "一键登录" |

# 加壳分析

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>classes2.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<br>Build.MODEL check<br>Build.MANUFACTURER check<br>Build.PRODUCT check<br>Build.HARDWARE check<br>Build.BOARD check<br>possible Build.SERIAL check<br>Build.TAGS check<br>network operator name check</td></tr>
<tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

<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<br>Build.MODEL check<br>Build.MANUFACTURER check</td></tr>
<tr><td>编译器</td><td>r8</td></tr>
</table>
</td></tr>
</table>

---