MoGua

# APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

Astrow 2.2.8.APK

| | |
|---|---|
| APP名称: | Astrow |
| 包名: | com.amanoeurope.astrow |
| 域名线索: | 1条 |
| URL线索: | 1条 |
| 邮箱线索: | 0条 |
| 分析日期: | 2022年2月2日 17:02 |

## 文件信息

文件名: astrow549654.apk
文件大小: 8.69MB
**MD5值:** d30c9916b97f463b1db4eaa049785fb0
**SHA1值:** 7ab4aa76821ca8e8d9e055f14366d417dd5ee728
**SHA256值:** 5f9cf3e197782a786aac9a69527e29877fbf4fa7f0c3b0c8a2c54aebcf9e8025

# APP 信息

**App名称:** Astrow
包名: com.amanoeurope.astrow
主活动**Activity:** com.amanoeurope.astrow.MainActivity
安卓版本名称: 2.2.8
安卓版本: 100053

# 域名线索

| 域名 | 是否危险域名 | 服务器信息 |
| --- | --- | --- |
| astrow-47183.firebaseio.com | good | **IP:** 35.201.97.85<br>所属国家: United States of America<br>地区: Missouri<br>城市: Kansas City<br>纬度: 39.099731<br>经度: -94.578568<br>查看地图: Google Map |

# URL线索

| URL信息 | Url所在文件 |
| --- | --- |
| https://astrow-47183.firebaseio.com | Android String Resource |

## 数据库线索

| FIREBASE链接地址 | 详细信息 |
| --- | --- |
| https://astrow-47183.firebaseio.com | info<br>App talks to a Firebase Database. |

## 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.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.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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| 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.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 |
| com.google.android.c2dm.permission.RECEIVE | 合法 | C2DM 权限 | 云到设备消息传递的权限 |

# 签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: CN=Amano
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2016-07-21 08:44:24+00:00
Valid To: 3015-11-22 08:44:24+00:00
Issuer: CN=Amano
Serial Number: 0xd1a26fa
Hash Algorithm: sha256
md5: fbb3ae007e55a7bca2ba4c96f42e51dc
sha1: e5d24c0dd667d1fd9b47c2675f81470651ef10ee
sha256: 30ab215d6bd750d55d0a59f6a9a7291fd73d56e4c5ffaadef7f4d1454ae41f20
sha512: 32d1e517078c53fe7134a918a89ff09a75e22d8ac2536f460f0a6eddbf1632df03dedb6e0d5fd3389988078e2a22f071c55048af09d94491d3b2a107a539b6ba
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 41150aa65e9348335e1188feb854b780d7f484b56698aa1bc64e8b012117a1b9

# Exodus威胁情报

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| Google Firebase Analytics | Analytics | https://reports.exodus-privacy.eu.org/trackers/49 |

# 硬编码敏感信息

| 可能的敏感信息 |
| --- |
| "firebase_database_url" : "https://astrow-47183.firebaseio.com" |
| "google_api_key" : "AIzaSyB9dQ5JuUN39hk1kf33BgVSo1HuuavARQs" |
| "google_crash_reporting_api_key" : "AIzaSyB9dQ5JuUN39hk1kf33BgVSo1HuuavARQs" |

# 加壳分析

| 文件列表 | 分析结果 |
| --- | --- |

<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<br>Build.PRODUCT check<br>Build.BOARD check<br>possible Build.SERIAL check</td></tr>
<tr><td>反调试</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>编译器</td><td>r8</td></tr>
</table>
</td></tr>
</table>

---