MoGua

# 熊盒子 5.0.APK 分析报告

| | |
|---|---|
| APP名称: | 熊盒子 |
| 包名: | www.xoicn.cn |
| 域名线索: | 1条 |
| URL线索: | 1条 |
| 邮箱线索: | 0条 |
| 分析日期: | 2022年9月26日 |
| 分析平台: | 摸瓜反编译平台 |

# 文件信息

文件名: 熊盒子 5.0.apk
文件大小: 10.25MB
**MD5值:** 032fe2b19bfd76a7573f2e0785177296
**SHA1值:** 53189a0384ac96b6f178c45333e99f339b8f5623
**SHA256值:** 8a9131816c9516712aec725c6024260f78676e6d20556bb3b6a125567f0d5315

# APP 信息

**App名称:** 熊盒子
包名: www.xoicn.cn
主活动**Activity:** com.xoicn.appbear.MainActivity
安卓版本名称: 5.0
安卓版本: 5

# 域名线索

| 域名 | 服务器信息 |
| --- | --- |
| www.xoicn.cn | **IP:** 103.45.65.78<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 |

# URL线索

| URL信息 | Url所在文件 |
| --- | --- |
| www.xoicn.cn; | www/xoicn/cn/R.java |

## 邮箱线索

## 手机线索

## 签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=CN, ST=, L=, O=, OU=, CN=
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-02-14 18:30:34+00:00
Valid To: 2044-02-08 18:30:34+00:00
Issuer: C=CN, ST=, L=, O=, OU=, CN=
Serial Number: 0x62f48b15
Hash Algorithm: sha1
md5: 6ce4e77494ae776348e5172dbc02e253
sha1: d6ee7b1102a2491b79e7624efed6f0b4713689a3
sha256: a16be632b3d73cb9e3368fdc1550d90613a758b40c3c569f165b2c8c7f1bc106
sha512: f64e1df6dc18b7e0f2ffd7a573528563071b63e8d24d6af9bf3e6bfed5eb077d52a0975b0c3670cda8082250df511c3512b24023ac495b948f9905d0cce87079
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: b30846f842f50771e9928b227acc72b8502dd32aa466cf1b77fc0947f53c06ad

# 硬编码敏感信息

# 加壳分析

| 加壳类型 | 所属文件 |
| --- | --- |
| 360 | libjiagu.so |
| 360 | libjiagu_x86.so |

# 第三方SDK

# 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_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_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 |

| 向手机申请的权限 | 是否危险 | 类型 | 详细情况 |
| --- | --- | --- | --- |
| 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.GET_INTENT_SENDER_INTENT | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.WRITE_MEDIA_STORAGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ACCESS_KEYGUARD_SECURE_STORAGE | 未知 | Unknown permission | Unknown permission from android reference |
| 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.READ_PRIVILEGED_PHONE_STATE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.MODIFY_AUDIO_SETTINGS | 正常 | 更改您的音频设置 | 允许应用程序修改全局音频设置,例如音量和路由 |
| 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 |

| 向手机申请的权限 | 是否危险 | 类型 | 详细情况 |
| --- | --- | --- | --- |
| 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 |

# 应用内通信