Evaluation Warning: The document was created with Spire.Doc for Python.

**魔域手游（ 10.68.0版本）   
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。  
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | 魔域手游 |
| 版本 | 10.68.0 |
| 包名 | com.westhouse.mysjb.xsj |
| 域名线索 | 5条 |
| URL线索 | 1条 |
| APP图标 |  |
| 分析日期 | 2025年7月17日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | xsj\_omni\_half\_10\_68\_0\_jinshan.apk |
| 文件大小 | 637.03MB |
| MD5值 | b20ef8e33fcd73fc7e7e69f56ded0a53 |
| SHA1值 | d1cb204a1d0275b7b9e03eceeb77a8046709aab9 |
| SHA256值 | 3dd5935b2123104b696896c32b44c586d020fd99370bf6e0052431b9501e32af |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 魔域手游 |
| 包名 | com.westhouse.mysjb.xsj |
| 主活动Activity | com.lh.impl.LoadActivity |
| 安卓版本名称 | 10.68.0 |
| 安卓版本 | 10680 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| a2.xgsdk.seayoo.com | IP: 68.79.27.25  所属国家: China  地区: Ningxia Huizu  城市: Yinchuan |
| www.jufangsoft.com | IP: 120.52.12.83  所属国家: China  地区: Hebei  城市: Langfang |
| xgdata.xgsdk.com | IP: 120.92.147.134  所属国家: China  地区: Beijing  城市: Beijing |
| cnks3.xgsdk.seayoo.comu0027 | 没有服务器地理信息. |
| ta.seayoo.com | IP: 161.189.17.86  所属国家: China  地区: Ningxia Huizu  城市: Yinchuan |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://xgdata.xgsdk.com | 摸瓜V2引擎 |
| https://cnks3.xgsdk.seayoo.com\u0027 | 摸瓜V2引擎 |
| https://ta.seayoo.com | 摸瓜V2引擎 |
| https://www.jufangsoft.com/legal/index.html?g\u003dmysy\u0026id\u003dprivate-policy\u0026channel\u003dwebsite | 摸瓜V2引擎 |
| https://a2.xgsdk.seayoo.com/ | 摸瓜V2引擎 |
| https://www.jufangsoft.com/legal/index.html?g\u003dmysy\u0026id\u003duser-agreement\u0026channel\u003dall | 摸瓜V2引擎 |
| https://a2.xgsdk.seayoo.com/pay-notify/jinshan/15985/v1 | 摸瓜V2引擎 |

### **4.3 邮箱线索**

### **4.4 手机号线索**

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: C=CN, ST=GUANGDONG, L=ZHUHAI, O=SEASUN, OU=XGSDK, CN=15985 签名算法: rsassa\_pkcs1v15 有效期自: 2016-05-16 06:22:29+00:00 有效期至: 2116-04-22 06:22:29+00:00 发行人: C=CN, ST=GUANGDONG, L=ZHUHAI, O=SEASUN, OU=XGSDK, CN=15985 序列号: 0x4fe76ec3 哈希算法: sha256 md5值: 639f51f7a8dec651bdff0cae9500eebe sha1值: e4f0665fe31b8779dfe7ceecfeb7b36505f2f9a1 sha256值: f3bbd042036ee98c4cc72471baaa7587e67595737293fc527d5ce70b0e779cb9 sha512值: 23c4f89e6ad2cd516341fc953b7361c3140f581ed7f080c56ee76fc2b49ce1e2f023f07915972695963bb97b4cfd7f0448bcb38e30ad1b7d9c6d9e0d5b1358f7 公钥算法: rsa 密钥长度: 1024 指纹: 7df4c7397811c993840f41eab1eeb67c950f1e16f9df46dfc89e05cc97b64e13**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "ks\_authentication\_agreement\_tip" : "其他相关政策说明%1$s、%2$s" |
| "ks\_authentication\_agreement\_tip\_link\_word1" : "《网络服务使用协议》" |
| "ks\_authentication\_agreement\_tip\_link\_word2" : "《在线隐私政策》" |
| "ks\_authentication\_tip" : "依照%1$s要求，网络游戏用户需进行实名认证，请先进行实名认证再进入游戏。为确保您身份真实性、向您提供更好的安全保障，您可以向我们提供真实姓名、身份证号码以完成实名认证。" |
| "ks\_authentication\_tip\_link\_word" : "《关于防止未成年人沉迷网络游戏的通知》" |
| "ks\_authentication\_title" : "实名认证" |
| "ks\_do\_find\_pwd" : "完成找回" |
| "ks\_do\_submit\_authentication" : "提交认证" |
| "ks\_find\_pwd" : "密码找回" |
| "ks\_find\_pwd\_goback" : "返回账号登录" |
| "nduni\_my\_str\_bind\_account\_tip\_password" : "密码：" |
| "weibosdk\_demo\_toast\_auth\_canceled" : "取消授权" |
| "weibosdk\_demo\_toast\_auth\_failed" : "授权失败" |
| "weibosdk\_demo\_toast\_auth\_success" : "授权成功" |

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看 |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看 |  |  |

## **9. 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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.WRITE\_MEDIA\_STORAGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.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.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.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.RECORD\_VIDEO | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |
| com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| freemme.permission.msa | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.CHANGE\_NETWORK\_STATE | 正常 | 更改网络连接 | 允许应用程序更改网络连接状态。 |
| 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 |
| freemme.permission.msa.SECURITY\_ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| oplus.permission.settings.LAUNCH\_FOR\_EXPORT | 未知 | Unknown permission | Unknown permission from android reference |
| com.vivo.identifier.permission.OAID\_STATE\_DIALOG | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BLUETOOTH | 正常 | 创建蓝牙连接 | 允许应用程序连接到配对的蓝牙设备 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| com.westhouse.mysjb.xsj.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| org.simalliance.openmobileapi.SMARTCARD | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.NFC | 正常 | 控制近场通信 | 允许应用程序与近场通信 (NFC) 标签,卡和读卡器进行通信 |

## **10. 应用内通信**

**报告由**  [**摸瓜APK反编译平台**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**