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

**BigWin 777 slots（ 1.0.1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 | BigWin 777 slots |
| 版本 | 1.0.1 |
| 包名 | com.BigWin777.top |
| 域名线索 | 17条 |
| URL线索 | 12条 |
| APP图标 |  |
| 分析日期 | 2025年1月5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 | BigWin 777 slots.apk |
| 文件大小 | 44.38MB |
| MD5值 | b84b0186a625b1f4f9a7bcb6d083e544 |
| SHA1值 | 53ffec47e37dd982b6d54881e646c5794754acd9 |
| SHA256值 | 80d21ca9ac3a85c944912a69b08314f80713b8060d6173f5c8af7b2a247d24ca |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | BigWin 777 slots |
| 包名 | com.BigWin777.top |
| 主活动Activity | com.wnpdjazslf.cxljhtcvmi.avudfthmln.MDPMUBAZZE |
| 安卓版本名称 | 1.0.1 |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| sattr.s | 没有服务器地理信息. |
| sinapps.s | 没有服务器地理信息. |
| sonelink.s | 没有服务器地理信息. |
| sapp.s | 没有服务器地理信息. |
| sstats.s | 没有服务器地理信息. |
| sadrevenue.s | 没有服务器地理信息. |
| slaunches.s | 没有服务器地理信息. |
| ssdk-services.s | 没有服务器地理信息. |
| simpression.s | 没有服务器地理信息. |
| play.google.com | IP: 142.251.42.238  所属国家: United States of America  地区: California  城市: Mountain View |
| sdlsdk.s | 没有服务器地理信息. |
| smonitorsdk.s | 没有服务器地理信息. |
| svalidate.s | 没有服务器地理信息. |
| sgcdsdk.s | 没有服务器地理信息. |
| sconversions.s | 没有服务器地理信息. |
| ds.alipay.com | IP: 124.239.239.236  所属国家: China  地区: Hebei  城市: Langfang |
| sregister.s | 没有服务器地理信息. |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://ds.alipay.com/?from=mobileweb | com/wnpdjazslf/cxljhtcvmi/avudfthmln/C1463.java |
| https://play.google.com/store/apps/details?id= | com/wnpdjazslf/cxljhtcvmi/avudfthmln/ཙད/C1449.java |

### **4.3 邮箱线索**

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 19222222222 | com/appsflyer/internal/a.java |

## **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=(1), ST=(1), L=(1), O=(1), OU=(1), CN=(1) 签名算法: rsassa\_pkcs1v15 有效期自: 2023-06-07 02:08:01+00:00 有效期至: 2121-12-30 02:08:01+00:00 发行人: C=(1), ST=(1), L=(1), O=(1), OU=(1), CN=(1) 序列号: 0x3211a1cd 哈希算法: sha256 md5值: aa6c5395ca796399a148b9aa0c85cd39 sha1值: 9a615fd5366f51358c216e9bfea47bd0d29c3bc7 sha256值: 68c21cd75dfd98d18b3b6063388be6bcb9610f5a4da9b5d0af8311b3c93d99e7 sha512值: 03e8324df474ecb715ba4afd5368daf8f8d7246a027ef3116aab321f2b74d262afe3f5212f3f79373dc23139ad1a728bb0c32070a7940c8f89962b4fddc1079c 公钥算法: rsa 密钥长度: 2048 指纹: 332f9340fee0f5f9cf36fe20a28cd12cf2cc1ffeb2fdea0e8526c94217d50523**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "PASSWORD" : "Password" |
| "USERNAME" : "Username" |
| "com\_facebook\_device\_auth\_instructions" : "Visit <b>facebook.com/device</b> and enter the code shown above." |
| "PASSWORD" : "Adgangskode" |
| "USERNAME" : "Brugernavn" |
| "com\_facebook\_device\_auth\_instructions" : "Besøg <b>facebook.com/device</b>, og indtast koden ovenfor." |
| "PASSWORD" : "パスワード" |
| "USERNAME" : "ユーザー名" |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b>にアクセスして、上記のコードを入力してください。" |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> 'ਤੇ ਜਾਓ ਅਤੇ ਉੱਤੇ ਦਿੱਤਾ ਕੋਡ ਪਾਓ।" |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b>என்ற இணைப்பிற்குச் சென்று, மேலே காட்டப்படும் குறியீட்டை உள்ளிடவும்." |
| "com\_facebook\_device\_auth\_instructions" : "Gå til <b>facebook.com/device</b>, og skriv inn koden som vises ovenfor." |
| "com\_facebook\_device\_auth\_instructions" : "Kunjungi <b>facebook.com/device</b> dan masukkan kode yang ditampilkan di atas." |
| "PASSWORD" : "Passwort" |
| "USERNAME" : "Nutzername" |
| "com\_facebook\_device\_auth\_instructions" : "Gehe zu <b>facebook.com/device</b> und gib den oben angezeigten Code ein." |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b>ని సందర్శించి పైన చూపిన కోడ్‌ను నమోదు చేయండి." |
| "com\_facebook\_device\_auth\_instructions" : "Besoek <b>facebook.com/device</b> en voer die kode in wat hierbo gewys word." |
| "com\_facebook\_device\_auth\_instructions" : "ไปที่ <b>facebook.com/device</b> แล้วป้อนรหัสที่แสดงด้านบน" |
| "PASSWORD" : "密码" |
| "USERNAME" : "用户名" |
| "com\_facebook\_device\_auth\_instructions" : "Siirry osoitteeseen <b>facebook.com/device</b> ja anna yllä oleva koodi." |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> पर जाएँ और ऊपर दिया गया कोड डालें." |
| "PASSWORD" : "Mật khẩu" |
| "USERNAME" : "Tên đăng nhập" |
| "com\_facebook\_device\_auth\_instructions" : "Truy cập <b>facebook.com/device</b> và nhập mã hiển thị bên dưới." |
| "com\_facebook\_device\_auth\_instructions" : "Prejdite na stránku <b>facebook.com/device</b> a zadajte kód, ktorý je zobrazený vyššie." |
| "com\_facebook\_device\_auth\_instructions" : "Πηγαίνετε στο <b>facebook.com/device</b> και πληκτρολογήστε τον κωδικό που φαίνεται παραπάνω." |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> സന്ദർശിച്ച് മുകളിൽ കാണിച്ചിരിക്കുന്ന കോഡ് നൽകുക." |
| "PASSWORD" : "Wachtwoord" |
| "USERNAME" : "Gebruikersnaam" |
| "com\_facebook\_device\_auth\_instructions" : "Ga naar <b>facebook.com/device</b> en voer de bovenstaande code in." |
| "com\_facebook\_device\_auth\_instructions" : "Odwiedź stronę <b>facebook.com/device</b> i wprowadź kod wyświetlony powyżej." |
| "com\_facebook\_device\_auth\_instructions" : "Bisitahin ang <b>facebook.com/device</b> at ilagay ang code na ipinapakita sa itaas." |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> -এ যান এবং উপরে দেখানো কোডটি লিখুন৷" |
| "com\_facebook\_device\_auth\_instructions" : "Buka <b>facebook.com/device</b> dan masukkan kode yang ditunjukkan di atas." |
| "com\_facebook\_device\_auth\_instructions" : "Visit <b>facebook.com/device</b> ಮತ್ತು ಮೇಲೆ ತೋರಿಸಿರುವ ಕೋಡ್ ಅನ್ನು ನಮೂದಿಸಿ." |
| "PASSWORD" : "암호" |
| "USERNAME" : "사용자 이름" |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b>를 방문하여 위 코드를 입력하세요." |
| "com\_facebook\_device\_auth\_instructions" : "Vizitează <b>facebook.com/device</b> şi introdu codul afişat mai sus." |
| "com\_facebook\_device\_auth\_instructions" : "يمكنك زيارة <b>facebook.com/device</b> وإدخال الرمز المعروض أعلاه." |
| "PASSWORD" : "Mot de passe" |
| "USERNAME" : "Nom d'utilisateur" |
| "com\_facebook\_device\_auth\_instructions" : "Consultez <b>facebook.com/device</b> et entrez le code affiché ci-dessous." |
| "com\_facebook\_device\_auth\_instructions" : "Posjetite stranicu <b>facebook.com/device</b> i unesite gore prikazani kôd." |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> येथे जा आणि वर दाखवलेला कोड प्रविष्ट करा." |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> adresini ziyaret et ve yukarıda gösterilen kodu gir." |
| "com\_facebook\_device\_auth\_instructions" : "Tento kód zadejte na webu <b>facebook.com/device</b>." |
| "PASSWORD" : "Contraseña" |
| "USERNAME" : "Nombre de usuario" |
| "com\_facebook\_device\_auth\_instructions" : "Visita <b>facebook.com/device</b> e ingresa el código que aparece más arriba." |
| "com\_facebook\_device\_auth\_instructions" : "Lawati <b>facebook.com/device</b> dan masukkan kod yang ditunjukkan di atas." |
| "PASSWORD" : "Parola d'ordine" |
| "USERNAME" : "Nome utente" |
| "com\_facebook\_device\_auth\_instructions" : "Consulta <b>facebook.com/device</b> e inserisci il codice mostrato sopra." |
| "PASSWORD" : "Senha" |
| "USERNAME" : "Nome de usuário" |
| "com\_facebook\_device\_auth\_instructions" : "Acesse <b>facebook.com/device</b> e insira o código mostrado acima." |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b>ની મુલાકાત લો અને ઉપર બતાવેલો કોડ લખો." |
| "com\_facebook\_device\_auth\_instructions" : "Nyisd meg a <b>facebook.com/device</b> oldalt, és add meg a fent látható kódot." |
| "PASSWORD" : "пароль" |
| "USERNAME" : "имя пользователя" |
| "com\_facebook\_device\_auth\_instructions" : "Перейдите на <b>facebook.com/device</b> и введите код, указанный выше." |
| "PASSWORD" : "Lösenord" |
| "USERNAME" : "Användarnamn" |
| "com\_facebook\_device\_auth\_instructions" : "Besök <b>facebook.com/device</b> och ange koden som visas ovan." |
| "com\_facebook\_device\_auth\_instructions" : "יש לבקר ב-<b>facebook.com/device</b> ולהזין את הקוד המוצג למעלה." |
| "com\_facebook\_device\_auth\_instructions" : "Consultez <b>facebook.com/device</b> et entrez le code affiché ci-dessus." |
| "com\_facebook\_device\_auth\_instructions" : "前往<b> facebook.com/device </b>並輸入上方顯示的代碼。" |
| "com\_facebook\_device\_auth\_instructions" : "访问<b>facebook.com/device</b>并输入上方显示的验证码。" |
| "com\_facebook\_device\_auth\_instructions" : "Visita <b>facebook.com/device</b> e introduce el código que aparece más arriba." |
| "com\_facebook\_device\_auth\_instructions" : "Acede a <b>facebook.com/device</b> e insere o código mostrado acima." |
| "PASSWORD" : "密碼" |
| "USERNAME" : "用戶名" |
| "com\_facebook\_device\_auth\_instructions" : "前往<b> facebook.com/device </b>並輸入上方顯示的代碼。" |

## **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.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.ACCESS\_LOCATION\_EXTRA\_COMMANDS | 正常 | 访问额外的位置提供程序命令 | 访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作 |
| android.permission.GET\_TASKS | 危险 | 检索正在运行的应用程序 | 允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.WRITE\_SETTINGS | 危险 | 修改全局系统设置 | 允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。 |
| com.android.launcher.permission.INSTALL\_SHORTCUT | 未知 | Unknown permission | Unknown permission from android reference |
| com.android.launcher.permission.UNINSTALL\_SHORTCUT | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BROADCAST\_STICKY | 正常 | 发送粘性广播 | 允许应用程序发送粘性广播,在广播结束后保留。恶意应用程序会导致手机使用过多内存,从而使手机运行缓慢或不稳定 |
| 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.GET\_PACKAGE\_SIZE | 正常 | 测量应用程序存储空间 | 允许应用程序找出任何包使用的空间 |
| com.huawei.android.launcher.permission.CHANGE\_BADGE | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章。 |
| 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.MOUNT\_UNMOUNT\_FILESYSTEMS | 危险 | 装载和卸载文件系统 | 允许应用程序为可移动存储安装和卸载文件系统 |
| 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.INTERACT\_ACROSS\_USERS\_FULL | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.gms.permission.AD\_ID | 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.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 |
| com.android.vending.BILLING | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.finsky.permission.BIND\_GET\_INSTALL\_REFERRER\_SERVICE | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.wnpdjazslf.cxljhtcvmi.avudfthmln.MDPMUBAZZE | **Schemes**: bigwin777://,  **Hosts:** mainactivity, |
| com.facebook.CustomTabActivity | **Schemes**: @string/fb\_login\_protocol\_scheme://, fbconnect://,  **Hosts:** cct.com.BigWin777.top, |

**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。**