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

**TeenPatti Plus（ 101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 | TeenPatti Plus |
| 版本 | 101 |
| 包名 | com.csgame.plus |
| 域名线索 | 28条 |
| URL线索 | 8条 |
| APP图标 |  |
| 分析日期 | 2025年1月15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 | abcd.apk |
| 文件大小 | 35.42MB |
| MD5值 | 3c8bd50cf8b2da662086829afc5ee511 |
| SHA1值 | b0338c84ead806898c996099cfb73d5cb516e6eb |
| SHA256值 | 4ccbbddb1a3cc184b37fd4edd8914dcc6c4076322c676cae9d56972f936b921a |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | TeenPatti Plus |
| 包名 | com.csgame.plus |
| 主活动Activity | com.csgame.plus.PlusActivity |
| 安卓版本名称 | 101 |
| 安卓版本 | 101 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| app.adjust.net.in | IP: 185.151.204.30  所属国家: United States of America  地区: Arizona  城市: Phoenix |
| oss.aliyuncs.com | IP: 118.178.29.5  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| gdpr.tr.adjust.com | IP: 195.244.54.6  所属国家: Turkey  地区: Izmir  城市: Izmir |
| gdpr.adjust.net.in | IP: 178.162.219.36  所属国家: Germany  地区: Hessen  城市: Frankfurt am Main |
| oss-cn-.aliyuncs.comor | 没有服务器地理信息. |
| www.cocos2d-x.org | IP: 50.18.252.155  所属国家: United States of America  地区: California  城市: San Francisco |
| gdpr.us.adjust.com | IP: 185.151.204.70  所属国家: United States of America  地区: Arizona  城市: Phoenix |
| subscription.eu.adjust.com | IP: 185.151.204.60  所属国家: United States of America  地区: Arizona  城市: Phoenix |
| gdpr.adjust.com | IP: 178.162.219.36  所属国家: Germany  地区: Hessen  城市: Frankfurt am Main |
| app.tr.adjust.com | IP: 195.244.54.5  所属国家: Turkey  地区: Izmir  城市: Izmir |
| app.adjust.world | IP: 185.151.204.42  所属国家: United States of America  地区: Arizona  城市: Phoenix |
| subscription.adjust.world | IP: 185.151.204.44  所属国家: United States of America  地区: Arizona  城市: Phoenix |
| docs.cocos.com | IP: 36.102.212.33  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| www.facebook.com | IP: 103.252.115.49  所属国家: Singapore  地区: Singapore  城市: Singapore |
| image.cnamedomain.com | 没有服务器地理信息. |
| subscription.us.adjust.com | IP: 185.151.204.70  所属国家: United States of America  地区: Arizona  城市: Phoenix |
| gdpr.eu.adjust.com | IP: 185.151.204.60  所属国家: United States of America  地区: Arizona  城市: Phoenix |
| subscription.tr.adjust.com | IP: 195.244.54.6  所属国家: Turkey  地区: Izmir  城市: Izmir |
| app.us.adjust.com | IP: 185.151.204.70  所属国家: United States of America  地区: Arizona  城市: Phoenix |
| subscription.adjust.com | IP: 185.151.204.52  所属国家: United States of America  地区: Arizona  城市: Phoenix |
| subscription.adjust.net.in | IP: 185.151.204.34  所属国家: United States of America  地区: Arizona  城市: Phoenix |
| github.com | IP: 20.205.243.166  所属国家: United States of America  地区: Washington  城市: Redmond |
| docs.cocos2d-x.org | IP: 184.169.198.12  所属国家: United States of America  地区: California  城市: San Francisco |
| 127.0.0.1 | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| app.eu.adjust.com | IP: 185.151.204.60  所属国家: United States of America  地区: Arizona  城市: Phoenix |
| gdpr.adjust.world | IP: 178.162.219.36  所属国家: Germany  地区: Hessen  城市: Frankfurt am Main |
| app.adjust.com | IP: 185.151.204.7  所属国家: United States of America  地区: Arizona  城市: Phoenix |
| oss-cn-hangzhou.aliyuncs.com | IP: 118.31.219.248  所属国家: China  地区: Zhejiang  城市: Hangzhou |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://app.adjust.com | com/adjust/sdk/Constants.java |
| https://gdpr.adjust.com | com/adjust/sdk/Constants.java |
| https://subscription.adjust.com | com/adjust/sdk/Constants.java |
| https://github.com/adjust/android\_sdk | com/adjust/sdk/ActivityHandler.java |
| https://app.adjust.world | com/adjust/sdk/network/UrlStrategy.java |
| https://app.eu.adjust.com | com/adjust/sdk/network/UrlStrategy.java |
| https://app.adjust.net.in | com/adjust/sdk/network/UrlStrategy.java |
| https://app.tr.adjust.com | com/adjust/sdk/network/UrlStrategy.java |
| https://app.us.adjust.com | com/adjust/sdk/network/UrlStrategy.java |
| https://gdpr.adjust.world | com/adjust/sdk/network/UrlStrategy.java |
| https://gdpr.eu.adjust.com | com/adjust/sdk/network/UrlStrategy.java |
| https://gdpr.adjust.net.in | com/adjust/sdk/network/UrlStrategy.java |
| https://gdpr.tr.adjust.com | com/adjust/sdk/network/UrlStrategy.java |
| https://gdpr.us.adjust.com | com/adjust/sdk/network/UrlStrategy.java |
| https://subscription.adjust.world | com/adjust/sdk/network/UrlStrategy.java |
| https://subscription.eu.adjust.com | com/adjust/sdk/network/UrlStrategy.java |
| https://subscription.adjust.net.in | com/adjust/sdk/network/UrlStrategy.java |
| https://subscription.tr.adjust.com | com/adjust/sdk/network/UrlStrategy.java |
| https://subscription.us.adjust.com | com/adjust/sdk/network/UrlStrategy.java |
| http://www.facebook.com/xvpn2017 | com/csgame/plus/PlusActivity.java |
| https://ip. | com/alibaba/sdk/android/oss/OSSImpl.java |
| http://oss-cn-\*\*\*\*.aliyuncs.com',or | com/alibaba/sdk/android/oss/OSSImpl.java |
| http://image.cnamedomain.com'! | com/alibaba/sdk/android/oss/OSSImpl.java |
| http://oss-cn-hangzhou.aliyuncs.com | com/alibaba/sdk/android/oss/common/OSSConstants.java |
| http://oss.aliyuncs.com | com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java |
| http://127.0.0.1 | com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java |
| http://oss-cn-\*\*\*\*.aliyuncs.com',or | com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java |
| http://image.cnamedomain.com'! | com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java |
| https://docs.cocos.com/creator/manual/zh/scripting/class.html | Mogua Engine V2 |
| http://docs.cocos2d-x.org/creator/manual/en/scripting/class.html | Mogua Engine V2 |
| https://docs.cocos.com/creator/manual/zh/scripting/reference/attributes.html | Mogua Engine V2 |
| http://docs.cocos2d-x.org/creator/manual/en/scripting/reference/attributes.html | Mogua Engine V2 |
| https://docs.cocos.com/creator/manual/zh/scripting/life-cycle-callbacks.html | Mogua Engine V2 |
| https://www.cocos2d-x.org/docs/creator/manual/en/scripting/life-cycle-callbacks.html | Mogua Engine V2 |

### **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=tt4tt5y, ST=try545, L=tret34t5, O=rrt43r43t, OU=ewrfwef34, CN=fer332fre 签名算法: rsassa\_pkcs1v15 有效期自: 2023-01-04 03:48:09+00:00 有效期至: 2047-12-29 03:48:09+00:00 发行人: C=tt4tt5y, ST=try545, L=tret34t5, O=rrt43r43t, OU=ewrfwef34, CN=fer332fre 序列号: 0x159a385d 哈希算法: sha256 md5值: d332fb01818d0691bfe576e4ce9e1a58 sha1值: 59752ff36b28581fe05ef396a3a167416141c164 sha256值: c59b41e4f026927dbf43e7e150651e0666d66a61ff04b406873642f5ec518d0c sha512值: 1239808aff0d8a31852440d64e73f8d3c282b7e9f078e3d35e30bd772ca7f7efd3671f7480b843339488d6a1f599c66875483463c51182c2435f2995a0ccdde7 公钥算法: rsa 密钥长度: 2048 指纹: 6a11f03e22fa1369f29e1780d1f6d9570c527ce8d522b28dbbece03a8e6acda1**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "com\_facebook\_device\_auth\_instructions" : "Visit <b>facebook.com/device</b> and enter the code shown above." |
| "com\_facebook\_device\_auth\_instructions" : "Gå til <b>facebook.com/device</b> og indtast koden, som er vist ovenfor." |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b>にアクセスして、上のコードを入力してください。" |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> 'ਤੇ ਵਿਜਿਟ ਕਰੋ ਅਤੇ ਉੱਪਰ ਦਿੱਤੇ ਕੋਡ ਨੂੰ ਦਾਖ਼ਲ ਕਰੋ।" |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> ஐப் பார்வையிட்டு, மேலே காட்டப்பட்ட குறியீட்டை உள்ளிடவும்." |
| "com\_facebook\_device\_auth\_instructions" : "Gå til <b>facebook.com/device</b> og skriv inn koden som vises over." |
| "com\_facebook\_device\_auth\_instructions" : "Kunjungi <b>facebook.com/device</b> dan masukkan kode yang ditampilkan di atas." |
| "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 ఎగువన చూపిన కోడ్‌ను నమోదు చేయండి." |
| "com\_facebook\_device\_auth\_instructions" : "Besoek <b>facebook.com/device</b> en voer die kode wat hierbo gewys word, in." |
| "com\_facebook\_device\_auth\_instructions" : "ไปที่ <b>facebook.com/device</b> แล้วป้อนรหัสที่ปรากฏด้านล่าง" |
| "com\_facebook\_device\_auth\_instructions" : "Siirry osoitteeseen <b>facebook.com/device</b> ja anna oheinen koodi." |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> पर विज़िट करें और ऊपर दिखाया गया कोड डालें." |
| "com\_facebook\_device\_auth\_instructions" : "Truy cập <b>facebook.com/device</b> và nhập mã được hiển thị bên trên." |
| "com\_facebook\_device\_auth\_instructions" : "Navštívte stránku <b>facebook.com/device</b> a zadajte kód zobrazený vyššie." |
| "com\_facebook\_device\_auth\_instructions" : "Πηγαίνετε στη διεύθυνση <b>facebook.com/device</b> και εισαγάγετε τον παραπάνω κωδικό." |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> സന്ദർശിച്ച് മുകളിൽ കാണിച്ചിരിക്കുന്ന കോഡ് നൽകുക." |
| "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 powyższy kod." |
| "com\_facebook\_device\_auth\_instructions" : "Puntahan ang <b>facebook.com/device</b> at ilagay ang code na ipinapakita sa itaas." |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> দেখুন এবং উপরে দেখানো কোডটিকে প্রবেশ করান৷" |
| "com\_facebook\_device\_auth\_instructions" : "Kunjungi <b>facebook.com/device</b> dan masukkan kode yang ditampilkan di bawah ini." |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> ಗೆ ಭೇಟಿ ನೀಡಿ ಮತ್ತು ಮೇಲೆ ತೋರಿಸಿದ ಕೋಡ್ ಅನ್ನು ನಮೂದಿಸಿ." |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b>에 방문하여 위 코드를 입력하세요." |
| "com\_facebook\_device\_auth\_instructions" : "Vizitează <b>facebook.com/device</b> şi introdu codul de mai sus." |
| "com\_facebook\_device\_auth\_instructions" : "تفضل بزيارة <b>facebook.com/device</b> وإدخال الرمز الموضح أعلاه." |
| "com\_facebook\_device\_auth\_instructions" : "Consultez <b>facebook.com/device</b> et entrez le code affiché ci-dessus." |
| "com\_facebook\_device\_auth\_instructions" : "Posjetitw <b>facebook.com/device</b> i unesite gore prikazani kôd." |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> भेट द्या आणि वरील कोड प्रविष्ट करा." |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> adresine git ve yukarıda gösterilen kodu gir." |
| "com\_facebook\_device\_auth\_instructions" : "Přejděte na <b>facebook.com/device</b> a zadejte nahoře uvedený kód." |
| "com\_facebook\_device\_auth\_instructions" : "Ve a <b>facebook.com/device</b> e ingresa el código que se muestra arriba." |
| "com\_facebook\_device\_auth\_instructions" : "Lawati <b>facebook.com/device</b> dan masukkan kod yang ditunjukkan di atas." |
| "com\_facebook\_device\_auth\_instructions" : "Visita <b>facebook.com/device</b> e inserisci il codice mostrato qui sotto." |
| "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&gt ની મુલકાત લો; અને ઉપર આપેલો કોડ દાખલ કરો." |
| "com\_facebook\_device\_auth\_instructions" : "Keresd fel a <b>facebook.com/device</b> címet, és írd be a fent megjelenített kódot." |
| "com\_facebook\_device\_auth\_instructions" : "Откройте <b>facebook.com/device</b> и введите код, показанный выше." |
| "com\_facebook\_device\_auth\_instructions" : "Gå till <b>facebook.com/device</b> och skriv in koden som visas ovan." |
| "com\_facebook\_device\_auth\_instructions" : "יש לבקר בכתובת facebook.com/device</b&gt ולהזין את הקוד המוצג למעלה" |
| "com\_facebook\_device\_auth\_instructions" : "Accédez à <b>facebook.com/device</b> et entrez le code affiché ci-dessus." |
| "com\_facebook\_device\_auth\_instructions" : "前往<b>facebook.com/device</b&gt，並輸入上方顯示的代碼。" |
| "com\_facebook\_device\_auth\_instructions" : "请访问<b>facebook.com/device</b>并输入以上验证码。" |
| "com\_facebook\_device\_auth\_instructions" : "Visita <b>facebook.com/device</b> e introduce el código que se muestra más arriba." |
| "com\_facebook\_device\_auth\_instructions" : "Visita <b>facebook.com/device</b> e insere o código apresentado abaixo." |
| "com\_facebook\_device\_auth\_instructions" : "前往<b>facebook.com/device</b&gt，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 |
| --- | --- | --- | --- |
| com.android.vending.BILLING | 未知 | Unknown permission | Unknown permission from android reference |
| 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。 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.READ\_PRIVILEGED\_PHONE\_STATE | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |
| com.google.android.finsky.permission.BIND\_GET\_INSTALL\_REFERRER\_SERVICE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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.RECEIVE\_BOOT\_COMPLETED | 正常 | 开机时自动启动 | 允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.facebook.CustomTabActivity | **Schemes**: @string/fb\_login\_protocol\_scheme://, fbconnect://,  **Hosts:** cct.com.csgame.plus, |

**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。**