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

**RAYBET（ 3.1.55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 | RAYBET |
| 版本 | 3.1.55 |
| 包名 | com.yartech.yarclient |
| 域名线索 | 12条 |
| URL线索 | 15条 |
| APP图标 |  |
| 分析日期 | 2025年7月3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 | com.yartech....1.apk |
| 文件大小 | 122.08MB |
| MD5值 | fbcd7d2a02cdc4fdea78dbce1190efa1 |
| SHA1值 | edce407299562c40ad999dbb4e38c3a3ee50e4f1 |
| SHA256值 | b57de1ba09235d68dbf0fcaa5024c93ab9d1aef561f133c702728e741d9d321f |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | RAYBET |
| 包名 | com.yartech.yarclient |
| 主活动Activity | com.yartech.yarclient.MainActivity |
| 安卓版本名称 | 3.1.55 |
| 安卓版本 | 351 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| developer.mozilla.org | IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| developer.android.com | IP: 142.250.73.78 所属国家: United States of America 地区: California 城市: Mountain View  |
| 39.97.233.230 | IP: 39.97.233.230 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| watchfree.ylkkl.com | 没有服务器地理信息.  |
| www.example.com | IP: 23.46.155.166 所属国家: Japan 地区: Osaka 城市: Osaka  |
| raytech-android.firebaseio.com | IP: 35.190.39.113 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| static.geetest.com | IP: 221.204.209.227 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| journeyapps.com | IP: 13.35.37.37 所属国家: Taiwan (Province of China) 地区: Taipei 城市: Taipei  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| api.geetest.com | IP: 103.143.17.142 所属国家: China 地区: Hebei 城市: Shijiazhuang  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.geetest.com | IP: 60.28.220.193 所属国家: China 地区: Tianjin 城市: Tianjin  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://static.geetest.com/static/appweb/app3-index.html  | com/geetest/sdk/O00000o0.java  |
| https://static.geetest.com/static/appweb/app3-index.html  | com/geetest/sdk/O00000o0.java  |
| https://api.geetest.com/get.php?gt=  | com/geetest/sdk/O00O0Oo.java  |
| https://api.geetest.com/gettype.php?gt=  | com/geetest/sdk/O00000o.java  |
| http://www.geetest.com/first\_page  | com/geetest/sdk/GT3GeetestButton.java  |
| http://static.geetest.com/static/appweb/app3-index.html  | com/geetest/sdk/Bind/O00000Oo.java  |
| https://static.geetest.com/static/appweb/app3-index.html  | com/geetest/sdk/Bind/O00000Oo.java  |
| https://api.geetest.com/gettype.php?gt=  | com/geetest/sdk/Bind/O00000o0.java  |
| http://39.97.233.230/  | com/kefu/chat/api/apiUtils/KFBaseUrl.java  |
| https://github.com/pichillilorenzo/flutter\_inappwebview  | com/pichillilorenzo/flutter\_inappwebview/InAppWebView/FlutterWebView.java  |
| https://github.com/flutter/flutter/wiki/Upgrading-pre-1.12-Android-projects\n\n\n  | com/pichillilorenzo/flutter\_inappwebview/InAppWebView/FlutterWebView.java  |
| http://www.example.com  | com/pichillilorenzo/flutter\_inappwebview/ChromeCustomTabs/CustomTabsHelper.java  |
| https://developer.android.com/guide/topics/permissions/overview  | io/flutter/plugin/platform/PlatformPlugin.java  |
| https://github.com/flutter/flutter/issues/2897).It  | io/flutter/plugin/platform/PlatformViewsController.java  |
| https://github.com/flutter/flutter/wiki/Upgrading-pre-1.12-Android-projects  | io/flutter/view/FlutterView.java  |
| https://raytech-android.firebaseio.com  | 摸瓜V1引擎  |
| https://journeyapps.com/  | 摸瓜V1引擎  |
| https://github.com/journeyapps/zxing-android-embedded  | 摸瓜V1引擎  |
| https://watchfree.ylkkl.com/stream/yyzb\_571123\_sg\_ff/playlist.m3u8  | 摸瓜V2引擎  |
| https://github.com/richtr/NoSleep.js/issues/15  | 摸瓜V2引擎  |
| https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released)  | 摸瓜V2引擎  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| appro@openssl.org  | lib/arm64-v8a/libflutter.so  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 13300000359  | 摸瓜V2引擎  |
| 13300000359  | 摸瓜V2引擎  |

## **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: CN=RayTech 签名算法: rsassa\_pkcs1v15 有效期自: 2019-02-12 06:06:18+00:00 有效期至: 2044-02-06 06:06:18+00:00 发行人: CN=RayTech 序列号: 0x5e3f46b9 哈希算法: sha256 md5值: 9e9cca398ef3aab5ab12d3d876aa0a0d sha1值: 462cee33b80ab53f145beb0ca12ae7c13c020a05 sha256值: 4a6a8a350e016418c49bbde494659dd0f35718f37112db75463de66916a32a01 sha512值: 8e26280f40a8148e008663e0ed69d800ab71ee9a1af60c0da749f21991a1180127575d098dca207ce65b437b7f0c71172c193d50d196fc5de450df3857918ace 公钥算法: rsa 密钥长度: 2048 指纹: 92cbd5dcd36c29e36a83f8b418ecf2f5edca3b1a2b791be4ae1e66e2b8260174**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "com.google.firebase.crashlytics.mapping\_file\_id" : "00000000000000000000000000000000"  |
| "firebase\_database\_url" : "https://raytech-android.firebaseio.com"  |
| "google\_api\_key" : "AIzaSyBd2mp7lHffrAuHLWdJ8ZxMpH7L8VJBReg"  |
| "google\_crash\_reporting\_api\_key" : "AIzaSyBd2mp7lHffrAuHLWdJ8ZxMpH7L8VJBReg"  |
| "kf\_ding\_cai\_sessionoff" : "会话结束，无法反馈"  |
| "library\_zxingandroidembedded\_author" : "JourneyApps"  |
| "library\_zxingandroidembedded\_authorWebsite" : "https://journeyapps.com/"  |
| "kf\_ding\_cai\_sessionoff" : "Conversation ended, you can't send feedback"  |
| "kf\_ding\_cai\_sessionoff" : "สนทนาจบลงแล้ว ไม่สามารถเสนอแนะได้"  |
| "kf\_ding\_cai\_sessionoff" : "Hội thoại kết thúc, không thể phản hồi"  |

## **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.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.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.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.USE\_FINGERPRINT | 正常 | allow use of指纹 | 该常量在 API 级别 28 中已被弃用。应用程序应改为请求 USE\_BIOMETRIC |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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.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.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.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 |
| com.google.android.providers.gsf.permission.READ\_GSERVICES | 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 |
| android.permission.USE\_BIOMETRIC | 正常 |  | 允许应用使用设备支持的生物识别模式。 |
| 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 |
| com.google.android.apps.photos.permission.GOOGLE\_PHOTOS | 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.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.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 |

## **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。**