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

**TubeVPN（ 3.3.2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 | TubeVPN |
| 版本 | 3.3.2 |
| 包名 | com.tubevpn.client |
| 域名线索 | 4条 |
| URL线索 | 1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 | TubeVPN 3.3.2 com.tubevpn.client.apk |
| 文件大小 | 19.74MB |
| MD5值 | 4dd27ee6b2214d383f57f183ba55f8ea |
| SHA1值 | 5e0d6a15c707ddef7629759c1454487496b79594 |
| SHA256值 | 35a514ef3f52c4a406ea86fdec0f1958dd26740a5f0a88ea403db4850a511028 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | TubeVPN |
| 包名 | com.tubevpn.client |
| 主活动Activity | com.github.shadowsocks.test |
| 安卓版本名称 | 3.3.2 |
| 安卓版本 | 30 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| stripe.com | IP: 198.137.150.141 所属国家: United States of America 地区: New York 城市: New York City  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| tubevpn-feaac.firebaseio.com | IP: 35.201.97.85 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| mikepenz.com | IP: 104.21.27.65 所属国家: United States of America 地区: California 城市: San Francisco  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://stripe.com/au-becs-dd-service-agreement/legal>Direct  | Mogua Engine V1  |
| https://tubevpn-feaac.firebaseio.com  | Mogua Engine V1  |
| http://mikepenz.com/  | Mogua Engine V1  |
| https://github.com/mikepenz/Android-Iconics  | Mogua Engine V1  |
| https://github.com/mikepenz/FastAdapter  | Mogua Engine V1  |
| https://github.com/mikepenz/MaterialDrawer  | Mogua Engine V1  |
| https://github.com/mikepenz/Materialize  | Mogua Engine V1  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| name@site.ru  | Mogua Engine V1  |
| ambrop7@gmail.com  | lib/arm64-v8a/libtun2socks.so  |
| ambrop7@gmail.com  | lib/armeabi-v7a/libtun2socks.so  |
| p.a.rombouts@home.nl tmoestl@gmx.net  | lib/x86/libpdnsd.so  |
| ambrop7@gmail.com  | lib/x86/libtun2socks.so  |
| p.a.rombouts@home.nl tmoestl@gmx.net  | lib/x86\_64/libpdnsd.so  |
| ambrop7@gmail.com  | lib/x86\_64/libtun2socks.so  |

### **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: True 找到 1 个唯一证书 主题: C=CN, ST=ciyrmc, L=ciyrmc, O=ciyrmc, OU=ciyrmc, CN=ciyrmc 签名算法: rsassa\_pkcs1v15 有效期自: 2022-10-04 08:19:08+00:00 有效期至: 2047-09-28 08:19:08+00:00 发行人: C=CN, ST=ciyrmc, L=ciyrmc, O=ciyrmc, OU=ciyrmc, CN=ciyrmc 序列号: 0x5650d30e 哈希算法: sha256 md5值: 7fb53041953d0ac0dc8e5f3527c48329 sha1值: b0a51a00abbab1a23a8a96b50aff4d9b18abe448 sha256值: c5adcae0b4a5066b1981c3069f5136eec162ab05a4c17138de09e1b0b98bb032 sha512值: 02dcec85225eb85c8ba1f4277f1bf572a53099ed4223fa3cdf750ef37fc6e1402a82aa2942ebdfe2cded4ae3f8eb101b2c42fc8eb53a4572b446229dc3b7a021 公钥算法: rsa 密钥长度: 2048 指纹: 3b896592c7c8f00fb66002137e638703f068edb392eedb2ed2f9d378f5a18172**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "firebase\_database\_url" : "https://tubevpn-feaac.firebaseio.com"  |
| "frontproxy\_password" : "Password"  |
| "frontproxy\_username" : "Username"  |
| "google\_api\_key" : "AIzaSyC5tClnSAO0ImMZ6kiGLGT0JwJjwSp4AAo"  |
| "google\_crash\_reporting\_api\_key" : "AIzaSyC5tClnSAO0ImMZ6kiGLGT0JwJjwSp4AAo"  |
| "library\_AndroidIconics\_author" : "Mike Penz"  |
| "library\_AndroidIconics\_authorWebsite" : "http://mikepenz.com/"  |
| "library\_fastadapter\_author" : "Mike Penz"  |
| "library\_fastadapter\_authorWebsite" : "http://mikepenz.com/"  |
| "library\_materialdrawer\_author" : "Mike Penz"  |
| "library\_materialdrawer\_authorWebsite" : "http://mikepenz.com/"  |
| "library\_materialize\_author" : "Mike Penz"  |
| "library\_materialize\_authorWebsite" : "http://mikepenz.com/"  |
| "onetime\_auth" : "One-time Authentication"  |
| "onetime\_auth\_summary" : "Enable one-time authentication"  |
| "password" : "Change Password"  |
| "sitekey" : "Password"  |
| "stripe\_failure\_reason\_authentication" : "We are unable to authenticate your payment method. Please choose a different payment method and try again."  |
| "frontproxy\_password" : "パスワード"  |
| "frontproxy\_username" : "ユーザー名"  |
| "onetime\_auth" : "ワンタイム認証"  |
| "onetime\_auth\_summary" : "ワンタイム認証を使用する"  |
| "sitekey" : "パスワード"  |
| "frontproxy\_password" : "пароль"  |
| "frontproxy\_username" : "имя пользователя"  |
| "onetime\_auth" : "Единоразовая Аутентификация"  |
| "onetime\_auth\_summary" : "Включить единоразовую аутентификацию"  |
| "sitekey" : "Пароль"  |
| "frontproxy\_password" : "密码"  |
| "frontproxy\_username" : "用户名"  |
| "onetime\_auth" : "一次性认证"  |
| "onetime\_auth\_summary" : "启用一次性认证"  |
| "password" : "修改密码"  |
| "sitekey" : "密码"  |
| "frontproxy\_password" : "密碼"  |
| "frontproxy\_username" : "用戶名"  |
| "onetime\_auth" : "單次驗證"  |
| "onetime\_auth\_summary" : "啟用單次驗證"  |
| "sitekey" : "密碼"  |
| "password" : "Change Password"  |

## **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.QUERY\_ALL\_PACKAGES | 正常 |  | 允许查询设备上的任何普通应用程序,无论清单声明如何 |
| android.permission.FORCE\_STOP\_PACKAGES | 合法 | 强制停止其他应用程序 | 允许一个应用程序强行停止其他应用程序 |
| 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.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 |
| 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 |
| 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.REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS | 正常 |  | 应用程序必须持有的权限才能使用 Settings.ACTION\_REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS。 |
| 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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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.MOUNT\_UNMOUNT\_FILESYSTEM | 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 |
| 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.DOWNLOAD\_WITHOUT\_NOTIFICATION | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.KILL\_BACKGROUND\_PROCESSES | 正常 | 杀死后台进程 | 允许应用程序杀死其他应用程序的后台进程,即使内存不低 |
| android.permission.RESTART\_PACKAGES | 正常 | 杀死后台进程 | 允许应用程序杀死其他应用程序的后台进程,即使内存不低 |
| 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 |
| com.google.android.c2dm.permission.RECEIVE | 合法 | C2DM 权限 | 云到设备消息传递的权限 |
| 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.github.shadowsocks.ProfileManagerActivity | **Schemes**: ss://, ssr://,  |

**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。**