翻墙 | Ghost Assassin：GFW如何识别并封锁翻墙工具

GFW的工作原理（1）

原文

————GFW是如何识别并封锁翻墙工具的

有人看过这篇文章1之后提出了一个问题：共匪是如何知道屁民在翻墙的呢？

这其实要看你使用的是什么翻墙工具，对于不同的翻墙工具，共匪GFW是有着不同的应对策略的。

先从使用人数最多的自由门说起：有人曾经反映自己在公司里用自由门+TOR翻墙，结果公司接到了公安的电话，要求公司加强管理阻止有人翻墙2。共匪公安怎么知道的？

问题在于自由门用户很多，而自由门虽说是通过拥有一个IP库不断变化IP从而躲避封锁（我自己观察自由门网络活动之后的推断），但IP和对应的服务器还是有限的，这样就会经常出现大量不同墙内客户端同时连接到少数几个服务器上的情况，而这是非常可疑的（说明一下为什么可疑：相对于明文流量，GFW对加密流量会特别关照，而自由门为了躲避GFW的关键词过滤自然会加密传输数据，那么也会被GFW特别关照，通向几个服务器的大量流量自然更会被注意），GFW就会试图去追踪那些远程服务器，进而就能发现那根本就不是什么网站服务器，而是用于翻墙的流量中转服务器（只要试着用浏览器连接服务器对应的域名或IP就能发现了）。虽说GFW无法完全封锁这些服务器，但可以通知公安当有人试图与这些服务器建立连接时进行警告（这种卑鄙手法的学名叫社会工程学）。

技术上来说现在还没有什么很好的应对方法（因为IPv4地址实在有限，都快被耗尽了），但如果只是用自由门翻墙浏览，不妨直接把事情闹大，共匪做这种事一向是偷偷摸摸的，一旦看到你试图曝光就会退缩，到时那公安成为替罪羊的可能性很大：）或者在家翻墙，共匪公安管不了你，“因为GFW是不存在的”。

VPN也有着类似的问题，一旦用的人多了就会被GFW重点关注，大部分时候对应VPN远程服务器的域名或IP会直接被拉入GFW黑名单中（别忘了GFW监控着所有流向国际互联网的流量），但其实这种封锁方法效率不高（很多时候需要手动填写黑名单，有人发现GFW封锁VPN总是在白天，那么最大的可能是IP或域名黑名单是人来维护的，今年1月21日墙内发生的大范围断网事件也可以佐证这一点3，共匪党媒说什么“被攻击”，其实是GFW这猪队友被共匪奴才误操作了之后造成了大面积断网）而且严重滞后，所以很长一段时间之内很多人满足于花钱买个付费VPN图个方便省事，而且能用很长时间。

不过2年前共匪十八大之后GFW大幅升级，引入了基于DPI的特征检测和流量分析技术，使得相当多VPN（尤其是OPENVPN）失效。

那么究竟什么是特征检测，什么又是流量分析呢？

先说说特征检测是怎么一回事吧：

不管是VPN还是TOR还是其他翻墙工具，要想成功翻墙都必须与对应的远程服务器建立连接，然后再用对应的协议进行数据处理并传输。

而问题就出在这里：翻墙工具和远程服务器建立连接时，如果表现的很独特，在一大堆流量里很显眼，就会轻易被GFW识别出从而直接阻断连接，而VPN（尤其是OPENVPN）和SSH这方面的问题尤其严重。

做个类比：通往国际互联网的流量是很多车队（数据包），车队在正式出发之前先要派个斥候与目标基地取得联系，确认目标基地正常之后再出发（有翻墙工具的制作者认为不用确认目标服务器的身份，但这么做会把翻墙者置身于危险之中：GFW可以轻易发动中间人攻击，然后翻墙者干了些什么就都被共匪知道了。迄今为止，据我所知只有TOR有严密完善的防止中间人攻击的机制，所以请大家改用TOR，别被共匪查水表）*。

“正常”的加密连接斥候说的是中文，但OPENVPN说的是英文，SSH说的是法文，那么OPENVPN和SSH就变得相当显眼（刚开始的连接建立过程一定是明文的，身份确认完毕之后才会建立加密连接），GFW据此在一开始就切断了联系从而使连接失败，这就是有效的特征检测。

焦点网谈

范玮琪道歉, 9.3阅兵, 天津爆炸事故, 新开罗宣言, 文化部禁曲120首, 被拐女教师, 文登爱国青年事件, 维权律师大抓捕, 股市暴跌, 金山PX示威, 香港政改风波, 昂山素季访华, 六四26周年, “东方之星”船难, 复旦校庆抄袭丑闻, 屠夫吴淦, 更多»

编辑推荐

陈希我｜我该怎样当教师?

张千帆：如何评价“中国模式”与印度民主？

自由亚洲｜鲍彤：习主席访美绕不开两个门槛

墙外楼｜中国经济好不了，放弃搬砖吧！

析世鉴｜殷海光：我对国共的看法

太阳报｜当官不发财？中共官场涌动下海潮

李悔之｜心头滴血的数据

万维网｜泼在习近平阅兵式上的冷水

大象公会｜斯大林到底应不应该勃起

江金泽：有钱也不许逃

数字时代安卓客户端

ANDROID APP ON Google play

数字时代iOS客户端

新闻关键词

媒体札记, 大月饼, 左手礼, 法西斯, 信力健, 抗战历史真相, 抗战老兵, 连爷爷, 抗日神剧, 为长者续命, 蛤丝, 为国接盘, 自干五, 网络上甘岭, 共青团, 曾庆红, 郭文贵, 陈检罗, 穹顶之下, 更多»

数字时代谷加账号

这里补充说明一下：我曾经说过如果共匪对shadowsocks进行了特征检测，那么不管使用什么加密方式远程服务器都会很快被封，依据就是上面说的：最开始的连接建立过程一定是明文的（如果全是密文，那么连送到哪儿都不知道，还建立连接呢。而且最开始客户端和服务端要协商传输方式再建立相应的加密连接，如果是密文，就变成了先有鸡还是先有蛋的问题了。是有一些加密方式号称从一开始就是强加密的，其实根本就只是加密了内容而没有加密数据包头部，而头部会泄露客户端的很多信息，例如HTTP Headers），GFW若是从一开始的连接过程入手，那么shadowsocks就和OPENVPN一个下场了（这也恰恰是shadowsocks的高明之处：在普通的socks代理之上加入自定义加密系统，而不是像OPENVPN那样有着极为独特的身份验证和加密连接建立协议，这样GFW就很难进行特征检测，具体我会在分析各翻墙手段安全性时进行说明），而且特征检测效果不受加密方式影响。

那流量分析呢？

还是用车队做类比："正常"的流量车队是小轿车，但特别的流量（例如TOR流量）是大卡车，小轿车队与大卡车队在车辆上（数据包结构，长度）与车队中每辆车的间距（数据包发送时的时间间隔）都不一样，这样GFW就能轻易的在小轿车流中找出大卡车队再进行阻断。同样，ISP也能通过流量分析知道你在翻墙（ISP本身就是GFW的组成之一）

还有就是暴力破解不可靠的VPN加密，得知你在翻墙以及翻墙之后干了什么4，VPN协议本身就很特别，ISP很轻松就能知道你在使用VPN。

总结：GFW通过追踪远程服务器（尤其是被很多人使用的远程服务器）和特征检测还有流量分析知道屁民们在翻墙，如果是墙内的VPN服务，那都不用GFW费力气了，流氓公司直接就把你给卖了。

系列下一篇我想具体聊聊GFW在DNS上下的功夫。

最后照例附上科普文链接集合https://plus.google.com/u/0/109790703964908675921/about

参考资料：

1，https://pao-pao.net/article/286
2，http://www.rfa.org/cantonese/firewall_features/firewall_yahoo-07132012120813.html?encoding=simplified
3，https://pao-pao.net/article/27
4，VPN翻墙，不安全的加密，不要相信墙内公司 https://plus.google.com/109790703964908675921/posts/AXgoJutf5sz

源地址：https://plus.google.com/109790703964908675921/posts/Qs4mjSQEuh7

翻墙技术博客订阅地址及社交帐号

2015年1月26日 下午 9:07

作者: 图样 图森破

分类: 科学上网

标签: GFW, u7ffbu5899

相关文章

2015.09.08 翻墙 | 中国继续开展对 VPN 服务的打击行动
2015.09.07 翻墙 | 道高一尺 墙高一丈：互联网封锁是如何升级的
2015.09.06 端传媒 | 道高一尺 墙高一丈：互联网封锁是如何升级的
2015.09.06 翻墙 | 淘宝禁售"国母同款"红裙
2015.09.06 翻墙 | 自由门翻墙推出7.55版
2015.09.02 翻墙 | "对抗专制、捍卫自由"的 N 种技术力量
2015.09.02 【麻辣总局】谷歌新旧Logo对比图（中国版）
2015.08.31 翻墙 | 从9月1日起中国手机实名制更严格
2015.08.31 翻墙 | 网传北京市公安局海淀分局下架翻墙软件通知
2015.08.31 翻墙 | 公安部整治网络谣言 查处197人关停账号165个
2015.08.26 GWI | 超九千万中国网民使用VPN访问国外社交网站
2015.08.26 翻墙 | VPN服务受到防火长城的进一步打击
2015.08.25 翻墙 | GoAgent开发者删除项目 GitHub再次受到DDoS攻击
2015.08.25 翻墙 | 慕容雪村：十四个梯子和一个春天

友情链接

天安门母亲, TankMan, 新公民运动, Weiboscope, 喷嚏图卦, 奇闻录, 公民行動影音紀錄資料庫, 相声四格, 蟹农场 Hexie Farm, 五柳村, 博谈网, 编程随想, 非新闻, HikingGFW, 香港独立媒体

2015.08.22 巴丢草 | 墙头打灰机
2015.08.22 纽约时报 | 慕容雪村：十四个梯子和一个春天
2015.08.21 翻墙 | Lantern 2.0版本推出 更加稳定 支持一键翻墙
2015.08.21 翻墙 | 翻墙站点红杏因“服务器故障”暂停新用户注册
2015.08.21 翻墙 | 翻墙站点vpnso同因“不可抗力”暂停网站服务
2015.08.21 GFW Blog | shadowsocks重要领导者被喝茶 放弃项目维护