大规模DDos攻击趋势的调查和基于云的缓解

作者：FuiFui Wong Cheng Xiang Tan

同济大学，中国上海，计算机科学与技术专业

摘要

分布式拒绝服务攻击如今已经被宽带互联网介入扩大为千兆位数量；同时，实施在小或大规模网络和服务中的更有力的僵尸网络、常见的DDos缓解策略和解决办法都不再有效。我们的调查提供了一个运用超过300Gbps如今最大规模的DNS响应攻击Spamhaus.org的深度研究。我们回顾并研究了当前最广泛的由黑客发起的DDos攻击类型。最后，我们两人一起提出了有效的基于云的DDos缓解和保护技术，并讨论了大型商业云端DDoS服务提供商。

关键字

Dos，DDDos，DNS响应或放大攻击，SYN泛洪，UDP泛洪，ICMP泛洪，HTTP泛洪攻击

1. 介绍

在2013年4月，Seamhaus.org遭遇了记录以来最大规模的分布式拒绝服务攻击，大概的规模超过了300Gbps。CloudFlare采用基于云的DDoS保护解决方案致力于缓解这种攻击。根据Prolexic的《Q1 2013 Global DDoS Attack》报告，如今多于10%的大型DDos攻击超过了60Gbps，多余75%的攻击是针对基础设施的（第三四层），限制带宽容量和路由基础设施，剩下的攻击是针对应用层的。

在一次DDos攻击中，攻击者试图暂时的中止或延迟一个网页的服务，使之对用户不可用。Akamai的2012年第四季度互联网状况报告中陈述了2012年总数768次DDos攻击。超过三分之一（269或35%）的攻击针对商业领域的公司，164（22%）次的攻击针对媒体或者娱乐公司，155次（20%）的攻击针对包含金融服务的企业公司，110次（14%）的攻击针对高科技公司，70次（9%）的攻击针对公共部门机构。这些攻击对这些目标公司在资金，客户满意度和声誉等方面造成了不同程度的损失。

这篇论文目的是提供一个对当前最广泛应用的大量DDos攻击类型完整的更新并讨论多种有效的基于云的DDos缓解策略和保护技术。在论文的第二个部分，我们首先详细研究Spamhaus当前最大规模的DDoS攻击。然后我们在第三部分讨论当前最广泛应用的针对基础设施（第三四层）和应用层的攻击类型。第四部分讨论了多种有效的基于云的DDos缓解策略和保护技术，最后，我们在第五部分提出了自己的结论。

1. 对Spamhaus历史的DDos攻击

在2013年3月18，Spamhaus的一个在线提供反垃圾邮件过滤服务的网站Seamhaus.org，被超过100Gbps的大量DDos攻击了，这次攻击非常巨大，互联网连接饱和，用户无法进入该网站。这次攻击被分类为第三层攻击，并且很难用软件来解决，因为接入的请求远远大于路由器能处理的通信数量，导致路由器饱和。那时，攻击者的身份也是未知的。

这些第三层攻击来源非常广并且是分布式的，信息来源发送流量以淹没目标互联网位置。一群一起工作的个人，一个盗用PC形成的僵尸网络，一个盗用客户端形成的僵尸网络，配置错误的DNS解析器，甚至是一个弱口令的家用网络路由器都可能成为攻击阻塞通信的来源。

像IP过滤这样的DDoS防御机制将不再有效，因为针对第三层攻击是通过发送包含欺骗信息和来源IP的随机数据包启动的，接受到的回应都会被忽略。CloudFlare是一家提供基于云的DDoS保护解决方案的公司，由Spamhaus聘请来减轻攻击，该网站在几小时内就完成了工作。

* 1. 针对Spamhaus网站75Gbps的DDoS攻击的生成

自从2012年开始，DNS反射攻击已成为第3层DDoS攻击的主要来源，Spamhaus最大的攻击流量就来自于DNS反射。

Spamhaus的攻击者首先从开放的解析器请求指向ripe.net的DNS区域文件，分配给Spamhaus的CloudFlare IPs在其DNS请求中被攻击者欺骗。DNS区域文件通过打开解析器来响应，由于36字节的响应被放大到3000字节，导致这些解析器生成了大约75 Gbps的攻击流量。

3000个不同的DNS解析器都参与到了Spamhaus的攻击之中。每一个开放的DNS解析器发送2.5Mbps的DNS区域文件，大部分解析器都允许这样的操作。然后，攻击者仅使用DNS放大并控制僵尸网络或服务器群集来生成750

Mbps DNS区域文件。

* 1. 针对Spamhaus网站75Gbps的DDoS攻击的减轻

CloudFlare使用Anycast来减轻对Spamhaus的75Gbps攻击。Anycast将对Spamhaus的攻击分散到CloudFlare的23个全球数据中心。每个数据中心都使用与Spamhaus相同的IP地址，这导致流量无法定位到某一个地点。这种方法 把多对一的攻击转换为多对多的攻击，这样就不能在网络中的某一个单独节点造成瓶颈。在攻击被分散后，在抵达Spamhaus服务器之前，针对第三层的攻击就被每一个CloudFlare的数据中心停止了。

1. 当前大规模DDoS攻击类型的上升趋势