分布式拒绝（DDoS）攻击又来了思科认证 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/644/2021_2022__E5_88_86_E5_B8_83_E5_BC_8F_E6_c101_644437.htm DdoS攻击的目标基本都是相同的，包括私营公司和政府网站。攻击的动机通常是勒索或者扰乱竞争对手公司的正常运行或者攻击不受欢迎的政府。但是这种攻击的凶猛程度和深度正如滚雪球般迅速扩大，这在很大程度上要归功于僵尸网络的扩散以及该攻击的目标从ISP连接转移到寻找服务器中的看似合法的请求。 位于马萨诸塞州的Akamai技术公司的首席安全官Andy Ellis表示，现在的很多DdoS攻击都是僵尸网络间接发起的，僵尸网络范围非常庞大，以至于那些控制僵尸网络的公司可能会丢失很久以前他们控制的感染计算机的追踪记录。 Ellis是从一个制高点来分析这个问题的。很多人几乎没有意识到自己在使用Akamai服务，该公司运行着上千台服务器的全球平台，很多客户都依赖他们的服务器来进行网上业务。目前，该公司每天需要为很多国际知名公司(如奥迪、NBC、富士通、美国国防部以及纳斯达克等)处理数百亿条网络通信信息，最重要的是，几乎没有任何一家Akamai负责的公司受到过DdoS攻击。“ 我们发现有很多攻击者利用被人遗忘的恶意软件来攻击被感染的计算机， ”Ellis表示，例如过时的蠕虫攻击，包括Blaster、Mydoom和code red等。“ 现在这些恶意软件被用来控制僵尸网络内的计算机，而僵尸网络本身则被作为武器来利用。 ”去年，Akamai最近还发现了最大的DDoS攻击，Ellis表示“ 超过每秒120千兆字节的巨大攻击 ”，如果你处在接受如此巨大攻击的接收端，那绝对是非常危险。 去年7

月4日周末发生的大规模攻击就是很好的例子，在那次攻击中，18万台被劫持的计算机形成的僵尸网络对美国政府网站造成重创，也给美国和韩国的业务带来恶劣影响。攻击从星期六开始，首先攻击了美国联邦贸易委员会(FTC)和美国运输部(DOT)网站。美国Bancorp，美国第六大商业银行，也受到了攻击。攻击者还攻击了Google、yahoo和Amazon网站。对Google的攻击并没有持续很久，考虑到Google的内容占整个互联网流量的5%，如果对其发起更持续的攻击可能会对整个互联网造成巨大影响。 Prolexic技术公司的首席技术官Paul Sop从他的角度分析了僵尸网络对于DdoS攻击的影响，他们公司有30名程序员花了所有时间来研究这个问题。“ 我们构建了一个IP信誉数据库，能够对攻击我们客户的非假冒IP地址进行追踪，现在已经追踪到大约400万受感染计算机， ”他表示，“ 令人惊讶的是僵尸网络的数据之大，以及能够很容易建立新的僵尸网络。 ”他们发现layer-7对HTTP、HTTPS和DNS服务的攻击越来越多，这些攻击并没有攻击用户的ISP连接，相反，他们攻击的是服务器，这样更难移识别和阻止，特别是当个体僵尸行为变得不那么明显以及伪装成合法用户流量。 他的团队观察到的大多数攻击都是针对企业实体间的恶意竞争引发的攻击。“ 在某些高风险市场(如网上赌博)，这在亚洲是非常受欢迎的，存在非常激烈的竞争，也存在不少DdoS攻击， ”他表示，“ 处于政治原因的攻击也开始变得越来越多，我们保护着很多大大小小的新闻和媒体网站。通常是某条新闻让外国攻击者感到不快，不过有时候，有些攻击可能是国家政府秘密资助的，或者说，国家批准的。 ”在最新发表的关于僵尸网络产生DdoS攻击的报告中，Prolexic

指出，攻击者能够迅速调整他们的僵尸网络，让攻击流量看起来非常像合法流量，日常流量。“ 通常那些巨大流量都标志着攻击的开始，而现在流量则是慢慢的形成僵尸，然后在任意时间间隔内每个僵尸会变换攻击风格，这让我们很难分辨真正用户和僵尸网络，”报告指出。