



僵尸网络已成为政治武器

罗伯·马兰（**Rob Malan**）

Arbor Networks 共同创始人及首席技术官

行政概要

僵尸网络是一种由引擎驱动的恶意因特网行为：DDoS 攻击是利用服务请求来耗尽被攻击网络的系统资源，从而使被攻击网络无法处理合法用户的请求。DDoS 攻击有多种形式，但是能看到的最典型的的就是流量溢出，它可以消耗大量的带宽，却不消耗应用程序资源。DDoS 攻击并不是新鲜事物。在过去十年中，随着僵尸网络的兴起，它得到了迅速的壮大和普遍的应用。僵尸网络为 DDoS 攻击提供了所需的“火力”——带宽和计算机——以及管理攻击所需的基础架构。

DDoS 规模、程度和复杂性都有新发展：2003 年，由 Arbor Networks 客户发现的规模最大的持续 DDoS 攻击为 2.5 Gbps。到了 2007 年，最大的持续攻击之规模已经超过 40 Gbps。让服务商感到更为棘手的是现在出现了一个新的情况，那就是常见的中等规模的“业余”攻击和使用成千万僵尸主机（zombie）进行的多 GB “专业”攻击之间的差别正在逐步扩大。

Arbor Networks 研究能力：Arbor Networks 在服务商的安全领域内发挥着主导作用，全球 90% 的一级服务商和 60% 的二级服务商都是它的客户。Arbor 充分利用这些关系，创建了可以同时进行数据收集和分析的平台，并提供了在全球服务商之间共享这些信息的方法。Arbor 与其全球服务商客户群合作，从 100 多家服务商那里实时收集因特网攻击数据，并与另外 30 多家服务商实时共享全球路由信息。此外，Arbor 还创建了世界上最大的分布式“暗网”监测系统，可以对全球可路由的 IP 地址进行监控。这些可路由的 IP 地址上不应该有任何活动的主机。Arbor Peakflow 和暗网检测系统联合收集的数据表明，只有 Arbor 才能“真正地”对构成互联网核心部分的骨干网内所传输的恶意数据获得全面的了解。由于这样独特的优势，Arbor 在发布有关恶意软件、后门、网上钓鱼和僵尸网络信息方面比起当今任何其他机构都更加领先。

威胁减除策略：为了减少大规模 DDoS 攻击带来的附带损害，服务商常常会阻断前往受攻站点的所有流量，以籍此阻断 DDoS 攻击。使用集成的威胁管理系统（TMS）设备，Arbor Networks 客户可以仅阻断攻击流量，从而保持可用的服务和较高的客户满意度。Peakflow SP TMS 使服务商能够在不中断合法流量的情况下识别和阻断网络和应用层攻击。Peakflow SP TMS 能够提供具有高成本效益的网络和应用层威胁检测、减除和报告功能，从而使服务商可以维护关键 IP 业务。最后，请求其他服务商帮助过滤流量也是非常必要的，因为当攻击规模达到每秒数十 GB 时，任何服务商都无法在处理这种攻击流量的同时还能维持正常的流量。这正是 Arbor Networks 能够在保护服务商的网络中发挥重要作用的地方。

网络战正走向错误的方向：最近几年，具有政治动机的网络攻击制造了不少新闻并成为人们关注的焦点。从 2007 年对爱沙尼亚的攻击到最近由于俄罗斯采取军事行动而引发的对格鲁吉亚基础设施和网络的攻击，都表明了这一点。Arbor Networks 研究发现，此类具有政治动机的攻击都不是国家支持的行为。Arbor Networks 认为，这些攻击是 21 世纪街头示威的一种形式，是那些对某项事业产生同情的人制造的网络中断，并非行政行为。

概述

DDoS 攻击是利用服务请求来耗尽被攻击网络的系统资源，从而使被攻击网络无法处理合法用户的请求。DDoS 攻击有多种形式，能看到的最典型的的就是流量溢出，它可以消耗大量的带宽，却不消耗应用程序资源。DDoS 攻击并不是什么新鲜事物。在过去十年中，随着僵尸网络的兴起，它得到了迅速的壮大和普遍的应用。僵尸网络为 DDoS 攻击提供了所需的“火力”——带宽和计算机——以及管理攻击所需的基础架构。大部分机器代码库都可以提供某种形式的 DDoS 能力。2006 年，我们检测发现，在我们所监控的僵尸网络中，大约一半网络都曾经发起过至少一次 DDoS 攻击。

其中一部分 DDoS 攻击似乎具有政治动机，被攻击者都是被认为对攻击者一方的某些人犯下了错误的对象。去年，爱沙尼亚政府和国家基础设施就受到了长达几个星期的 DDoS 攻击。这些攻击正好发生在爱沙尼亚发生反对俄罗斯的街头示威期间。同样的情况也发生在最近俄罗斯和格鲁吉亚发生的网络战中。在这些案例中，我们发现，大部分的 DDoS 攻击背后都有僵尸网络的支持和人工在协调，某些组织的俄语论坛就对这些攻击进行了支持。但是，我们从未发现有任何证据证明所谓俄罗斯政府部门对这些攻击进行支持的说法。

我们最近看到的其他具有政治动机的 DDoS 攻击包括在 2008 年冬季选举前奏中针对俄罗斯政治家 Gary Kasparov 及其政党的攻击。在这起攻击事件中，网站被迫短暂关闭，使其用户无法使用。然而，这样做好像并不能对政党本身产生任何损害，也就是说，这些攻击更像是暴乱和示威，而不是抢劫和掠夺。

政治性的 DDoS 事件不只是针对俄罗斯和欧洲的网络。我们监控的大部分攻击来自美国，而且大部分攻击对象也是美国。从美国具有大量的地址空间来看，这也是合理的。过去，我们发现过与印度和巴基斯坦冲突有关的 DDoS 攻击，而最近，我们也发现过针对伊朗某些目标的 DDoS 攻击。

事实上，我们认为最近的政治性 DDoS 攻击是 21 世纪街头示威的一种形式，是那些对某项事业产生同情的人制造的网络中断，并非行政行为。

僵尸网络和 DDoS 攻击的这些新情况对网络服务商会产生各种实质性的后果。

Arbor Networks 是如何获取数据的

我们使用两种方法来监控 DDoS 攻击。第一种方法是利用我们的 ATLAS（Arbor 威胁级别分析系统）系统，该系统可以检测骨干网流量，将全球 DDoS 统计数据聚合在一起。

ATLAS 的创新之处在于，它能够使用一个可以提供分析和行动信息的平台将全球因特网攻击信息汇聚起来。然后，ATLAS 再使全球各服务商共享这些信息。只有借助于这种全面的透视能力、信息和协作，服务商才能打击僵尸网络、DDoS 攻击和其他恶意因特网行为带来的灾难。

Arbor Networks 在服务商的安全领域内发挥着主导作用，全球 90% 的一级服务商和 60% 的二级服务商都是它的客户。Arbor 充分利用这些关系，创建了可以同时进行数据收集和分析的平台，并提供了在全球服务商之间共享这些信息的方法。

Arbor 与其全球服务商客户群进行合作，从 100 多家服务商那里实时收集因特网攻击数据，并与另外 30 多家服务商实时共享全球路由信息。此外，Arbor 还创建了世界上最大的分布式“暗网”监测系统，可以对全球可路由的 IP 地址进行监控。这些可路由的 IP 地址上不应该有任何活动的主机。

Arbor Peakflow 和暗网检测系统联合收集的数据表明，只有 Arbor 才能“真正地”对构成互联网核心部分的骨干网内所传输的恶意数据获得全面的了解。由于这样独特的优势，Arbor 在发布有关恶意软件、后门、网上钓鱼和僵尸网络信息方面比起当今任何其他机构都更加领先。

我们收集数据的第二种方法是通过对僵尸网络进行主动监控、对发送到僵尸程序的命令进行监测，并从中提取攻击信息。虽然这两种方法都不完整，但都是广泛了解 DDoS 行为不可或缺的手段。从监测中我们还发现，这两种方法可以阻断某些攻击的连接，也就是说我们将永远无法跟踪观察因特网上的所有 DDoS 攻击命令。

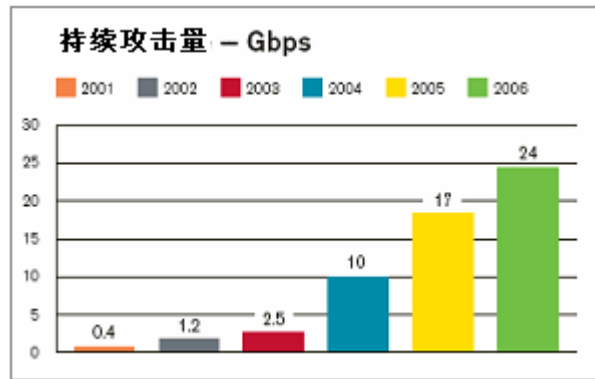
对 DDoS 攻击意图的估计通常是推测性的，而且往往是根据受攻击对象的外部资料来进行。DDoS 攻击的动机往往是对受攻击者的某些行为的报复或愤怒，有时还包括勒索或惩罚性攻击。过去几年，我们对全球成千上万种此类攻击进行了跟踪，发现任何网络都无法免受来自“业务端”的这种攻击。垃圾信息发送者或在线网络钓鱼团队可能会对研究人员发起攻击，以阻止他们的工作。但是我们更常见的是针对宽带用户或小型电子商务网站发起的各种小规模攻击。更大规模和更复杂的攻击往往会涉及到对主要在线商业机构的某种勒索。某些攻击已导致商业机构破产，因为后者无法处理其客户需求或支付带宽费用。当然，最近我们还看到，具有政治动机的攻击有很大增加。

僵尸网络对服务商网络的影响

作为我们的《全球构架安全报告》的一部分，Arbor Networks 每年都要对其全球客户群进行调查。调查结果清楚表明，僵尸网络及其在 DDoS 攻击中作为引擎使用是当今因特网服务商（ISP）网络面临的一个最大的威胁。

DDoS 攻击越来越专业化：虽然自 2000 年以来，中等规模的 DDoS 攻击一直困扰着互联网，但是根据调查反馈者的报告，普通中等规模的“业余”攻击和使用成千万僵尸主机（zombie）进行的多 GB “专业”攻击之间的差别正在逐步扩大。接受调查的大部分服务商都报告说，僵尸军团的攻击无论在复杂性还是在协调性上都有了很大发展。

攻击发展速度超过 ISP 网络发展速度：过去几年，大部分一级和二级服务商都已完成了对骨干网络基础构架的大量投资——把链路从 OC12/48（2 Gbps）升级到 OC192（10 Gbps）。但是，接受调查的服务提供商报告说，曾经遇到超过 24 Gbps 的持续攻击速率，此数字超过最近升级的链路容量的两倍。



我们很快将会发布 2008 年的调查结果，今天我想与各位分享一个数据。在今年的报告中，有好几家服务商报告说，他们曾经遭受超过 40 Gbps 的持续 DDoS 攻击。总之，DDoS 攻击在继续变得越来越复杂，规模也变得越来越大。

缺少执法助长网络攻击：如果您在街上示威，就有可能真正触犯法律。但是如果您在因特网上进行示威，触犯法律的机率会变得很小，法律对您会很有利。

在我们的报告中，几乎没有服务商向执法机构举报这些攻击。不进行举报的原因很多。其中指出的一些原因包括：

- 客户隐私/要求
- 缺乏取证分析的详细信息
- 攻击太多无暇应对
- 对报告是否有用心存疑虑

全世界大多数国家的执法都是努力制止街头犯罪，却不管网络犯罪，这是一个事实。那些干坏事的人很清楚这一点，所以他们不断地把他们的行为转向因特网所代表的安全空间。

DDoS 减除策略

DDoS 攻击永远无法被阻断，这是由因特网的性质所决定的。即使没有僵尸网络和各种复杂的工具，任何人都可以鼓励其他人去访问某一网站，从而有效地发生请求溢出，破坏网站的稳定性。我们无数次看到过使用“点杠效应（Slashdot effect）”进行攻击的例子。同样是在爱沙尼亚和韩国，就发生过烦躁民众向攻击对象发送大量请求，导致服务被迫中断的情况。然而，我们可以对攻击进行管理，对基础构架的配置进行更改，避免其在此类攻击中被滥用。

就象 20 世纪 90 年代采取的协同行动，通过更改默认的路由器设置来阻断“Smurf”攻击一样，开放的递归式 DNS 服务器会对因特网的基础构架造成威胁，因为它们可以用来进行 DNS 放大攻击。发现并配置好这些设施是一个重大的挑战。在这方面几乎还没有取得任何进展。

如果流量发生明显的变化，则可以在入侵点对其进行大规模的拦截，这样对正常流量的中断最小；例如，在上游路由器处对所有 ICMP 回显请求进行过滤可以阻断 Ping 泛洪攻击。即使攻击者向被攻击对象发送随机数据包，具有这种特征的“异常”流量也能够被安全拦截，从而减少带宽的使用。

除非端点能够对 Akamai 等大型分布式主机的基础构架进行访问，否则很难在 DNS 层面上采取行动来挫败 DDoS 攻击。为此，它们可以把攻击流量分散到多个高度互连的节点上，从而针对攻击者筑起一道防护栏。除非把 DNS 条目完全下载到本地，否则 DNS 条目的短存活时间（TTL）值对挫败攻击并没有帮助，因为攻击者总可以利用被攻击对象的 IP 地址作为目标。

对付大型 DDoS 攻击最成功的策略是采用多向量方法。如果可以识别泛洪源 IP 地址，则可以在源地址端把它们关闭，或者如果无法联系服务商，则可以使用路由方法在通向网络途中阻断其流量（通过在路由器上执行“单播反向路径转发”[Unicast Reverse Path Forwarding]来实现）。根据攻击的不同类型，也可以采用 SYN 代理等其他防护技术。此外，还可以使用高速线路过滤设备来中断额外流量或将其规模缩小到可接受的水平。

Arbor Networks 应用智能和威胁减除

使用 10 Gbps Arbor Peakflow SP 威胁管理系统（TMS）设备的 Peakflow SP 是第一个能够广泛集成网络级智能和运营商级威胁管理的平台。Arbor Peakflow SP TMS 是一种针对多服务融合式网络的应用智能设备。它可以增强全网事态感知能力，并通过将高水平的威胁识别能力与数据包级分析相结合，可更为迅速地采取措施。它可以补充和完善 Peakflow SP 的其它清洗技术，包括指纹共享、边界网关协议（BGP）黑洞路由选择、BGP 流规范和对第三方产品的支持。

为了减少大规模 DDoS 攻击带来的附带损害，服务商常常会阻断前往受攻站点的所有流量，以藉此阻断 DDoS 攻击。使用集成 TMS 设备，Arbor Networks 可以仅阻断攻击流量，从而保持可用的服务和较高的客户满意度。Peakflow SP TMS 使服务商能够在不中断合法流量的情况下识别和阻断网络和应用层攻击。Peakflow SP TMS 能够提供具有高成本效益的网络和应用层威胁检测、减除和报告功能，从而使服务商可以维护关键 IP 业务。

Arbor 的领导作用促进服务商之间的交流

大规模的 DDoS 攻击不仅会影响既定的受攻击对象，而且会影响到可能正在使用同一共享网络服务的其他用户。Arbor Networks 在建立“指纹共享联盟”等自动进程上发挥了重要作用。“指纹共享联盟”是跨公司、大陆和海洋的一个打击网络攻击活动的全球电信公司联盟。Arbor Networks 向 Peakflow SP 添加了指纹共享功能，允许各公司在不泄露任何竞争性信息的情况下自动共享攻击指纹。

Peakflow SP 通过网络中的设备收集数据来完成这一功能，然后把数据相互关联起来，以利于服务商为网络创建基线和检测异常偏差，并把偏差标记为异常。随后，系统将决定异常情况是合法的瞬时拥塞（例如在线事件发生期间）还是恶意攻击。网络管理员随即决定是否对其进行减除或保留。

如果确认是恶意攻击，Peakflow SP 就会产生指纹，服务商可以通过选择对等体自动安全地对其进行共享。网络管理员可以完全控制谁能够接收共享指纹，且网络无需相邻。指纹接收者在接收到发送过来的指纹时，可以选择接受或拒绝共享请求。

结论

近年来，僵尸网络已成为推动恶意因特网行为发展的主要动力。僵尸网络已变得越来越复杂，规模也變得越来越大。同时，它们已被应用于垃圾邮件、网络钓鱼和 ID 窃取等不断扩大的各种方法中。最近，僵尸网络还被用于发起 DDoS 攻击，成为政治示威的一种形式。虽然，我们还没有看到国家支持的网络攻击，但是大多数政府认为两个政府之间的此类因特网冲突是不可避免的。

鉴于此，解决僵尸网络问题是服务商面临的第一安全要务。

无论是通过“指纹共享联盟”内的创新和协作，还是通过我们对 ATLAS 的研究能力及我们的安全专家团队，Arbor Networks 都将继续发挥关键作用，帮助服务商确保其网络的安全性、可用性和盈利性。