简译版

DDoS 攻击的七个趋势

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	7 Things to Know About Today's DDoS Attacks		
原文作者	Jai Vijayan	**原文发布日期**	2017 年 8 月 30 日
作者简介	Jai Vijayan 是一名经验丰富的技术记者，拥有超过 20 年的 IT 行业新闻经验。https://www.darkreading.com/author-bio.asp?author_id=1912		
原文发布单位	Dark Reading		
原文出处	https://www.darkreading.com/cloud/7-things-to-know-about-todays-ddos-attacks/d/d-id/1329758?image_number=1		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

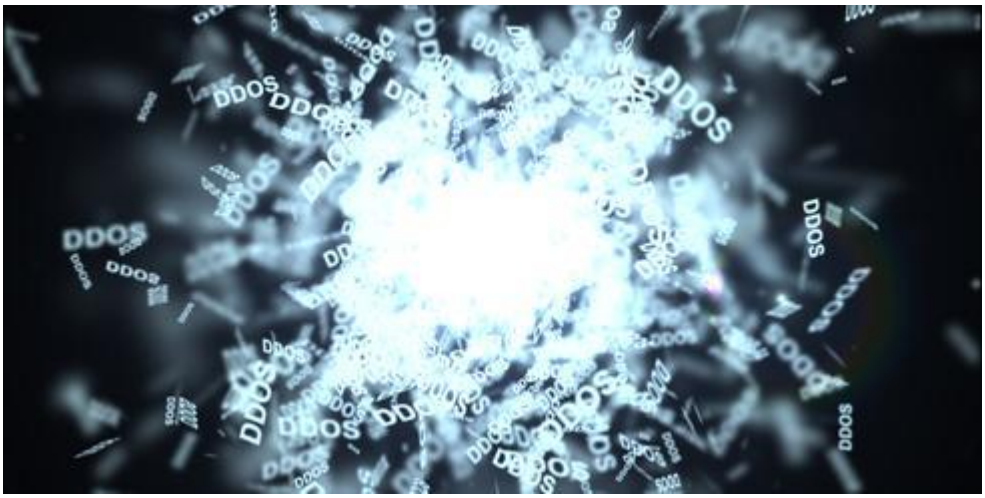
DDoS 攻击的七个趋势

Jai Vijayan

2017 年 8 月 30 日

DDoS 攻击已经不再只是少数行业内的大公司需要担心的事情了，每个企业都面临这种威胁。

不要纠结于数字



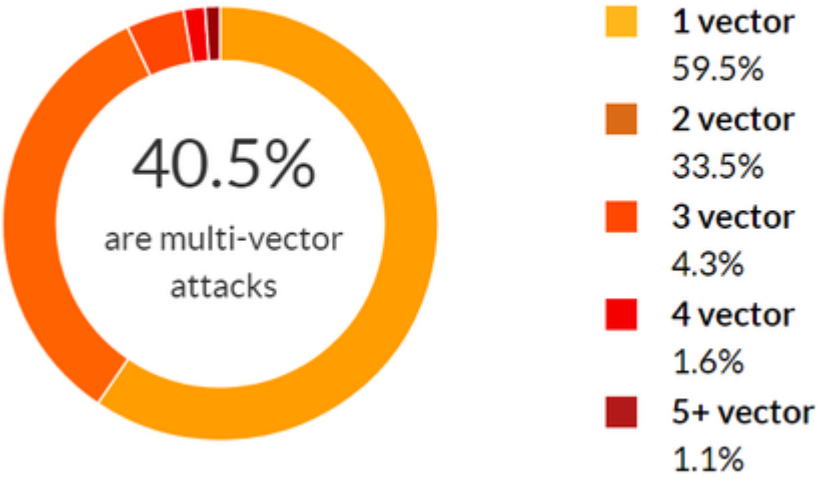
DDoS 攻击的实际数量和平均规模（带宽）每个季度都会以很大的变化，有时甚至以月为单位发生变化。

从 Akamai Technologies《2017 年第二季度互联网/安全状态报告》来看，经过连续三个季度的下降后，2017 年第二季度的 DDoS 攻击比上个季度增长了 28%。同时，第二季度没有看到超过 100Gbps 的 DDoS 攻击。

相比之下，就在上个季度，Verisign 报道称至少有一个攻击达到了 120Gbps，平均攻击规模比上一年高 26%。

数字本身不应该决定缓解策略 :更重要的是了解 DDoS 攻击已成为大多数组织面临的威胁。攻击者比以前更加坚定，拥有更多的资源。DDoS 攻击规模不必是数 Gbps 就能导致网络崩溃。

多向量攻击



结合了容量、应用级和协议级元素的多向量 DDoS 攻击已成为主要威胁。攻击者可以一次使用一个向量来启动这些攻击，或者同时使用所有向量以混淆目标。

据报道称，2016 年多向量 DDoS 攻击增加了 322%；而在 2015 年，UDP、TCP 和 ICMP 是最受欢迎的攻击向量。早在 2016 年第一季度，诸如 Akamai 的公司报告称，多向量 DDoS 攻击占其减灾工作的 60%以上。

研究人士说："这些攻击很难防御，并且通常非常有效，因此颇受欢迎。"

事实上，Verisign 在今年第一季度发现的最大 DDoS 攻击是多向量攻击，峰值带宽为 120Gbps，每秒大约传输 9000 万个数据包。该攻击主要由 TCP SYN 和 TCP RST 流量洪泛攻

击组成，持续了两周，并在 15 小时的时间内持续发送 60Gbps 的流量。

据称 Arbor 最新的全球基础设施安全报告指出，67%的受访者报告了多向量 DDoS 攻击，比去年高 56%。

网络层/容量耗尽攻击仍然是最常见的

Imperva 研究团队负责人 Avishay Zawoznik 说，网络层攻击（也称容量耗尽 DDoS 攻击）仍然是最常见的攻击类型。

这些攻击的特点是高带宽或每秒数据包数量，以受害者网络管道的带宽容量或受害者网络设备的路由容量为目标。Zawoznik 说，容量耗尽攻击的常见例子包括 SYN、ACK、UDP 和 ICMP 洪泛攻击。

他说："在过去的几个月中，我们最常看到的 DDoS 攻击是 TCP 攻击、NTP 放大攻击和多向量攻击。" 显然，攻击带宽、每秒数据包数量或每秒请求数量越大，容量耗尽攻击导致的伤害就越大。

Akamai 上个季度帮助客户处理了 4051 个 DDoS 攻击，其中 99%是容量耗尽攻击。80%以上针对游戏行业的公司。埃及 IP 地址数量最多，占全球总数的 38%。

应用级 DDoS 攻击正在增加

虽然网络层 DDoS 攻击仍然很常见，但应用级攻击正在迅速增加。

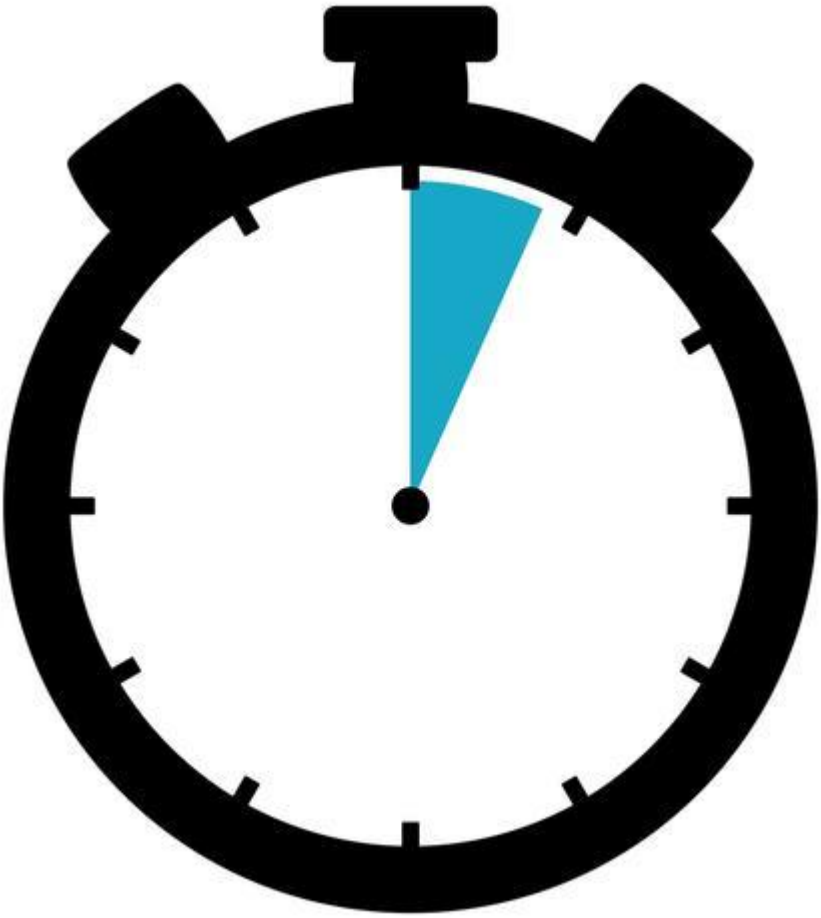
应用级 DDoS 攻击使用一系列看似合法的请求来轰炸业务应用程序，直到应用程序无法响应。与容量耗尽攻击相反，应用程序攻击的流量低得多，并以每秒请求量（RPS）进行测量。典型的攻击针对的是 HTTP 和 DNS 服务，现在越来越多地针对 HTTPS 服务。

Imperva《2017 年第一季度全球威胁全景报告》显示，网络层 DDoS 攻击连续四个季度下降，而应用层攻击每周达到近 1100 次。

最大规模的攻击达到 17600 RPS，高于 Imperva 在 2016 年处理的最大的应用层攻击。“这些攻击旨在消耗服务器、web 服务器和数据库等的计算资源。” Zawoznik 说。他说，典型的攻击包括针对目标应用程序的 HTTP GET，POST 和 PUSH 请求洪泛。

据称，DNS 攻击占去年所有报告的应用层攻击的 81%，超越 HTTP 成为最受欢迎的攻击类型。

大多数 DDoS 攻击小而简短



事实是，绝大多数 DDoS 攻击（即使是容量耗尽攻击）都涉及相对较低的流量。

事实上，在 2017 年第一季度 Corero Network Security 为其客户处理的 DDoS 攻击中，80%规模不到 1Gbps。

从 2016 年第四季度到 2017 年第一季度，98%的攻击都低于 10Gbps。在 2017 年第一季度 Corero 为客户处理的 DDoS 攻击中，71%不超过 10 分钟。

在大多数情况下，这种攻击不足以瘫痪网站，但是也会导致严重的安全问题。

小型 DDoS 攻击经常用于窃取数据并掩盖数据泄露。Corero 表示，许多情况下，威胁源使用这些攻击来映射受害者的网络，安装恶意软件，作为勒索攻击的前身。虽说小型 DDoS 攻击可能不会导致网络瘫痪，但是会导致服务质量降级和拥塞问题。

DDoS 攻击更加持久

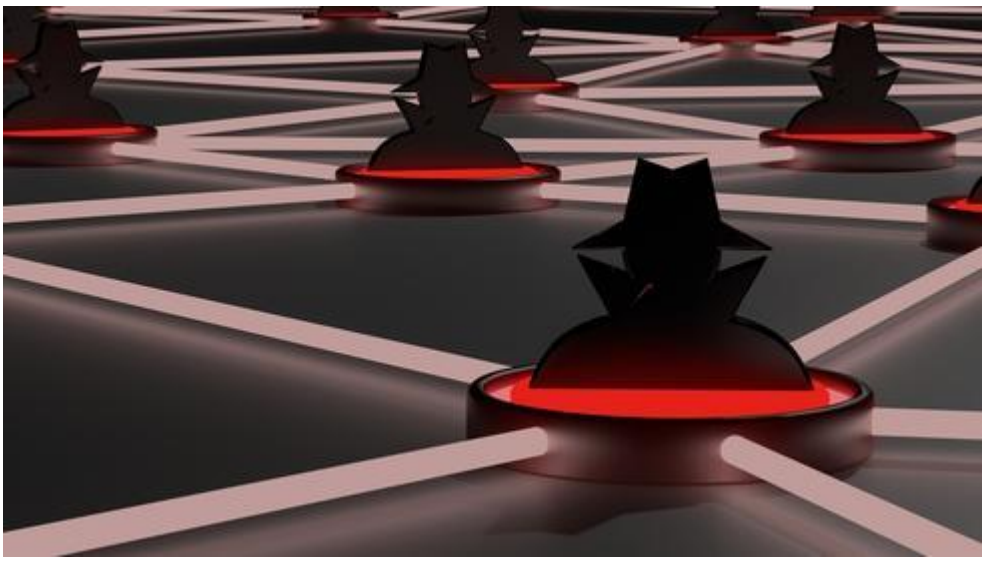
目前有很多执行 DDoS 攻击的工具，导致威胁源能够持续攻击受害者。

例如，Akamai 报告说，在 2017 年第二季度，受害者平均遭受了 32 次 DDoS 攻击。一家游戏公司每天平均遭受 6 次攻击，共遭受了 558 次攻击。Corero 表示，其客户今年第一季度每月平均遭受 124 次 DDoS 攻击，比 2016 年第四季度增加了 9%。

相关报告中说："在宏观层面上，DDoS 攻击越来越短，但也更加复杂和持久。"

公司遇到的所有攻击中，超过 90%不超过 30 分钟。近 75%的 Imperva 客户多次受到攻击，说明威胁源的持续性增加。19%被攻击了 10 次以上。

IoT 和移动僵尸网络驱动的 DDoS 攻击正在崛起



近年来，存在漏洞的移动和物联网设备大量扩散，为攻击者提供了创建大规模僵尸网络来执行 DDoS 攻击的机会。

Marai 是这类僵尸网络的代表，不过其它僵尸网络也在崛起。最近的例子是 WireX，该僵尸网络由受感染的 Android 设备构建，针对多个行业的目标执行应用层 DDoS 攻击。本月，多个安全厂商的研究人员对该僵尸网络进行了分析。其中最大的攻击涉及分布在 100 个国家的超过 7 万个感染节点。

相关报告中指出："大规模僵尸网络驱动的 DDoS 攻击变得越来越普遍。它们已经足够强大，能够破坏本该安全的公司网络。"