快速演变和增加的 DDoS 攻击威胁

随着攻击的针对性、复杂性和频率与日俱增，每一家企业都需要保持警惕。

没有一家企业能逃脱分布式拒绝服务 (DDoS) 攻击的威胁。一心想要发起勒索攻击、黑客行动主义攻击或报复式攻击的网络犯罪分子可能会将任何企业列为攻击目标，发起大规模复杂攻击。正因如此，当今的每一家数字技术主导型企业都需要筑起抵御 DDoS 攻击的全面防线。

互联网上最早出现的攻击类型之一

1999 年 7 月 22 日，114 台遭遇入侵的计算机向明尼苏达大学的一台计算机发出海量数据包，这次泛洪攻击造成该计算机脱机两天。

根据麻省理工学院科技评论提供的信息，这是第一次记录在案的 DDoS 攻击。

黑客行动主义者和其他网络犯罪分子发现，只需要寥寥数行代码即可轻松发动此类攻击，于是在随后的数周至数月内，从 CNN 到亚马逊等主流企业的网站相继因此类攻击而中断。

DDoS 成为任何拥有在线业务的企业的心头大患。

攻击的规模和复杂度都在增加

从 1999 年至今，DDoS 防御技术在不断提升，但犯罪分子的能力也再提升。当今的 DDoS 攻击者可以利用数十种攻击媒介、大量价格低廉的攻击者工具包，以及互联网上大量容易攻破的设备，这一切让他们可以扩大攻击活动的规模。2016 年，攻击者利用遭入侵的安保摄像头 DVR，造成互联网大面积瘫痪。

而自那之后，又有数以亿计毫不设防的物联网设备接入网络。即将到来的 5G 技术革命有望会使此类设备再多出数亿台。试想一下，借助在速度、容量和减少延迟方面都有指数级变化的 5G 技术，攻击会有怎样的强度和规模。

互联网上不设防、无维护的服务器数量也在飞速增加，犯罪分子可以劫持这些服务器，从而实施放大和反射攻击。犯罪分子知道这其中许多服务器的 IP 地址，并且能利用它们来将欺骗请求的数量增加到原有的 50,000 多倍。

全天候紧急 DDoS 缓解和保护服务

如果 Akamai 客户受到 DDoS 攻击威胁，可联系 Akamai 安全运营指挥中心 (SOCC)。

如果您不是 Akamai 客户，但需要紧急保护，请填写我们 **DDoS 热线页面**上的表格，或致电 **+1-877-425-2624** 寻求紧急援助。

没有哪个行业能完全避开 DDoS 攻击的威胁

如今，Akamai 每年抵御数千次 DDoS 攻击。

在某些情况下，攻击动机显而易见。游戏玩家可能会使用 DDoS 攻击来拖慢网速，并获得相对于比赛对手的竞争优势。曾经有大学生利用定向 DDoS 攻击来让一家 ISP 的客户对服务产生不满情绪，并转而选择该 ISP 竞争对手的服务。

但在其他一些情况下，攻击动机要更加复杂或难以捉摸。我们已经观察到有犯罪分子利用 DDoS 攻击将应急响应团队的注意力引向企业的一个部分，并且伺机在另一部分发起隐秘的攻击。

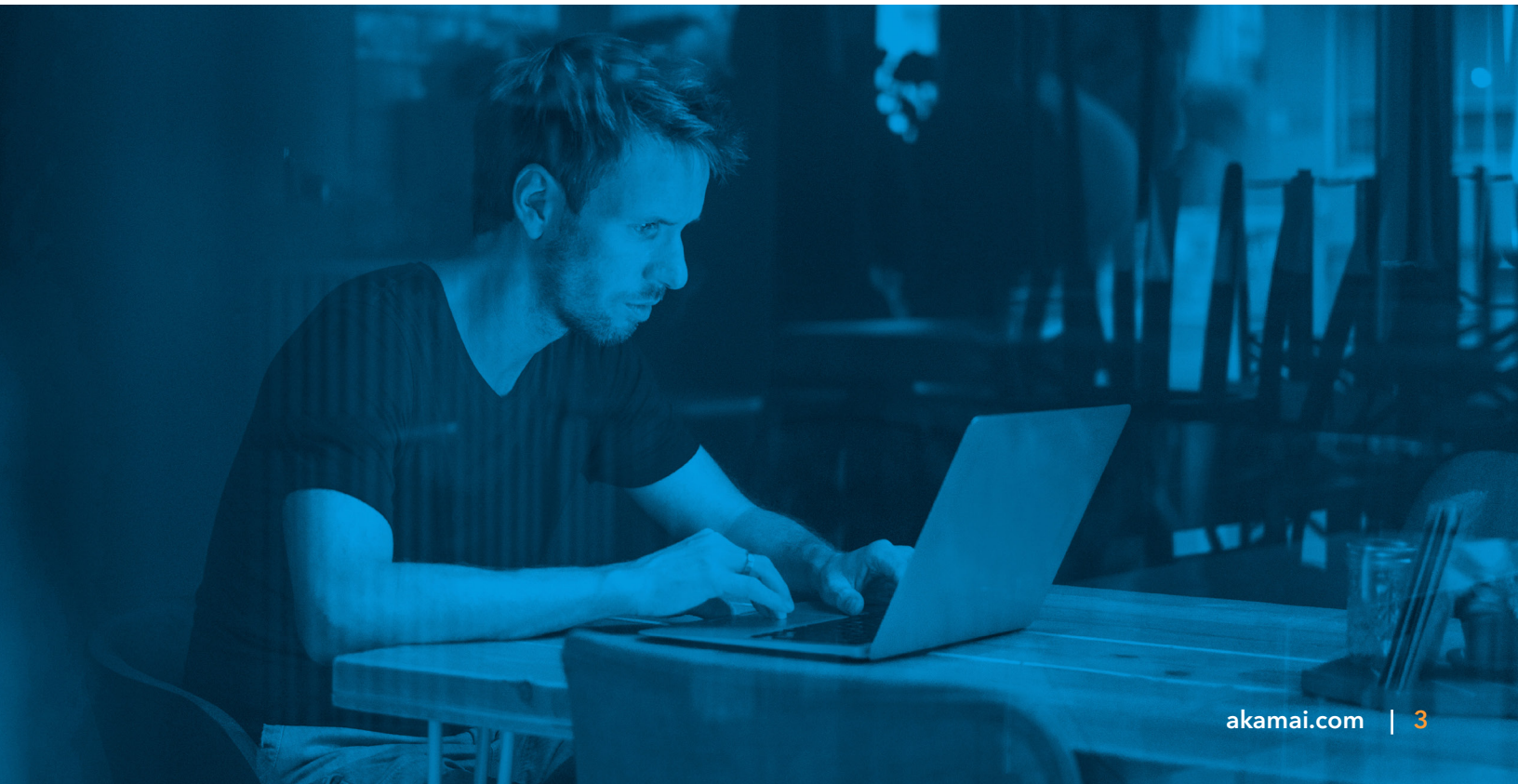
技术不精的恶意攻击者可以通过暗网获得"DDoS 租用"服务。5 分钟攻击的价格从 5 美元起，24 小时攻击的价格则会增加至 400 美元。如果有人对一家公司心怀不满，他们可以花上 200 美元或 300 美元，让一家公司蒙受数百万美元的损失。

2020 年，我们观察到了规模更大、复杂度更高的攻击

2020 年上半年，Akamai 阻止了每秒 Tb 数 (Tbps) 达到 1.44、每秒百万数据包数 (Mpps) 达到 809 的大规模攻击，这是有纪录以来 Mpps 量级最高的攻击。

尽管这些攻击在不到一秒的时间内就得到了缓解，但它们体现出攻击速度更快（按 100 Gbps 衡量）、攻击规模更大的趋势。许多攻击都采用了独特、复杂的攻击媒介组合。他们意图攻破或绕过防御措施，并消耗事件响应资源。

至少需要一定人为缓解措施（而非仅限于自动响应）的攻击也在增加。



史上最大规模的 DDoS 勒索攻击活动

2020 年 8 月，Akamai 安全情报研究团队发出警报，提醒公众注意，各行各业的许多公司都收到了 DDoS 勒索电子邮件。攻击者以运营瘫痪的后果作为要挟，称企业如果不支付比特币赎金，就得面对重大停机和严重经济损失。

仅仅几周后，美国联邦调查局就发布报告称，全球各地有成千上万的组织收到了类似的勒索电子邮件。攻击者会集体向一个行业的企业发起威胁，然后转向另一个行业，再转向另一个行业。组织严密的攻击者常常会回过头去威胁以前的目标。

防御越出色，受到攻击的几率就越小

网络犯罪分子与其他类型的犯罪分子没什么不同。他们会先"踩点"，寻找薄弱环节。在 DDoS 攻击中，攻击者会首先窥视目标受害者的 DNS、Web 应用程序和面向互联网的数据中心资产。

如果网络犯罪分子通过侦查发现了容易攻破的资源、站点或服务，那么他们可能会实施攻击。如果他们发现防御做得很好，那么他们就会另寻他处。

事实上，在紧急求助于 Prolexic 新客户中，他们在将流量路由到该平台之前已经受到了攻击，而一旦 Prolexic 的防御措施实施到位，绝大多数客户都不会再次受到攻击。对于网络犯罪分子来说，如果潜在攻击对象采用的是 Prolexico 防御产品，那么他们可能会认为不值得浪费时间，因为还有许多其他唾手可得的目标可供选择。

全面 DDoS 防御的运作机制

Akamai 通过由专用边缘、分布式 DNS 和云端净化抵御解决方案构成的透明网格，提供深度 DDoS 防御能力，网络总容量超过 175 Tbps。这些专门构建的云旨在增强 DDoS 安全态势，同时缩小攻击面。这种端到端的 DDoS 防护旨在提高抵御措施的质量并减少误报，同时提高抵御规模最大、复杂度最高的攻击的韧性。

此外，该解决方案还可以进行调优，以满足您的 Web 应用程序和基于互联网的服务的特定要求。

边缘防御

Akamai 将全球分布式 Intelligent Edge Platform 设计成一个反向代理，只接受通过 80 和 443 端口传输的流量。该平台可立即在边缘消除所有网络层 DDoS 攻击，并提供零秒 SLA。

针对应用层事件，包括通过 API 发起的攻击，Kona Site Defender 可以吸收攻击，同时支持合法用户正常访问。

DNS 防御

Akamai 的权威 DNS 服务 Edge DNS 也会在边缘处过滤流量。不同于其他 DNS 解决方案，Akamai Edge DNS 的架构经过专门设计，旨在保证用户在面对 DDoS 攻击时的可用性和韧性。Edge DNS 还有着卓越的性能，提供多个层面上的架构冗余，包括名称服务器、入网点、网络，甚至是分段式 IP Anycast 云。

云端净化防御

Prolexic 通过 20 个全球净化中心和 8.2 Tbps 的专用 DDoS 防御容量，保护整个数据中心和混合基础架构抵御 DDoS 攻击，并且覆盖所有端口和协议。这样的能力旨在保持面向互联网的资产的可用性，而这正是任何信息安全计划的基石。

作为一项完全托管式服务，Prolexic 可以建立主动和被动安全模式。该服务整合了自动防御机制以及 Akamai 全球 SOCC 网络的专家协助式抵御服务。Prolexic 还通过主动防御控制提供**行业卓越**的零秒缓解 SLA。

Prolexic 如何阻止创纪录的攻击

2020 年 6 月的 809 Mpps 攻击是互联网上有史以来规模最大（按每秒数据包数 (PPS) 衡量）的攻击。不同于更常见的每秒发出数比特流量的攻击（尝试造成入站互联网管道不堪重负），PPS 攻击旨在耗尽数据中心或云端的网络资源。

这次可怕的攻击涉及到大量的攻击源 IP 地址。其中超过 96% 的 IP 地址从未在以往的攻击中观测到。攻击的升级速度也非常惊人，在短短两分钟内，攻击速度就从 418 Gbps 猛增到 809 Mpps。

幸运的是，目标企业是一家 Prolexic 客户，有零秒 SLA 作为坚实后盾。Akamai SOCC 与该客户合作，了解了其正常运行时期的流量基准概况，并制定了控制措施和安全策略来即时阻止 DDoS 攻击。

立即预约定制威胁简报会

访问 akamai.com/ddos-briefing