DDoS 勒索反击战清单

随着分布式拒绝服务 (DDoS) 攻击数量的增加，您准备好进行反击了吗？企业若是缺乏适当的 DDoS 缓解策略就只有两种选择 - 要么支付赎金，要么承受意外停机的风险。遵循以下步骤操作，帮助企业最大限度降低遭受以勒索为目标的 DDoS 攻击的风险。

1. 不要助纣为虐（无论是哪种方式）

Akamai 建议您不要支付赎金；谁也不能保证攻击者是否还会继续威胁，支付赎金也不代表就能阻止 DDoS 攻击。攻击者正在尝试利用人们"对未知的恐惧"来迅速赚钱，然后他们会转向下一个目标。

2. 借力缓解专家

确认关键业务资产和后端基础架构是否受到保护。如果您没有适当的 DDoS 缓解措施，请与基于云的服务提供商联系（联系 Akamai 的 DDoS 热线），他们将快速启动紧急服务来帮助您降低风险。20 多年来，我们的全球 SOCC 专家已经成功抵御各种 DDoS 攻击。

3. 打响 DDoS 攻击反击战

有了合适的缓解技术合作伙伴和安全控制措施，攻击者就会没有可乘之机。Akamai 的零秒 SLA 几乎主动缓解了所有与此系列攻击活动相关的 DDoS 攻击，只有一小部分攻击需要我们的全球 SOCC 来主动缓解。实际上，在 2020 年我们缓解的所有攻击中，大约 70% 的攻击都是通过 Prolexic 的零秒 SLA 完全阻止的。

4. 改变您的安全态势

只要经历过一次攻击，就能明白 DDoS 防御是当今威胁形势下的必备武器。评估您的风险承受能力，以确定应采用按需缓解措施还是不间断的云端缓解措施，才能更好地保护您的联网资产。

5. 重新查阅您的 DDoS 手册

如果您还没有准备好，请召集您的 IT、运营、安全和客户服务人员，确保做好充分准备，了解在发生攻击时应采取哪些措施。Akamai 与每位客户一起创建自定义防御行动手册，并执行各种桌面攻击演习，以确保适当的人员、流程和程序准备就绪，以优化事件响应。

DDoS 勒索反击战清单

为了保持当今关键业务资产的正常运行，无论企业规模大小，都需要借助高质量的缓解控制措施、平台规模和专业知识，以阻止 DDoS 攻击活动的进行。访问 akamai.com/ddos-briefing，申请您的自定义 DDoS 威胁简报，并获取有助于保障业务安全的深刻见解。

Akamai

Akamai 为全球的大型企业提供安全的数字化体验。Akamai 的智能边缘平台涵盖了从企业到云端的一切，从而确保客户及其公司获得快速、智能且安全的体验。全球优秀品牌依靠 Akamai 敏捷的解决方案扩展其多云架构的功能，从而获得竞争优势。Akamai 使决策、应用程序和体验更贴近用户，帮助用户远离攻击和威胁。Akamai 一系列的边缘安全、Web 和移动性能、企业访问和视频交付解决方案均由优质客户服务、分析和全天候监控提供支持。如需了解全球顶级品牌信赖 Akamai 的原因，请访问 www.akamai.com 或 blogs.akamai.com，或者扫描下方二维码，关注我们的微信公众号。您可以访问 www.akamai.com/locations 查找全球联系信息。发布时间：2020 年 10 月。

扫码关注，获取最新CDN前沿资讯