NOKIA 上海贝尔

阻止 DDoS 很容易，但仅阻止 DDoS 很困难

DDoS 攻击可以影响任何规模的组织，甚至是拥有非常庞大的安全运营团队的超大型组织，几周前 Microsoft 365 的服务中断就揭示了这一点。

然而，在这种情况下，问题并不在于 DDoS 攻击流量本身 -- 据报道，根据诺基亚 Deepfield 应急响应团队的数据，这次 TCP SYN flood 只是 2024 年我们客户网络中第四大最常见的攻击媒介。相反，对攻击的响应造成的问题比攻击本身更多：DDoS 缓解措施确实阻止了恶意流量，但也阻止了很大一部分合法客户流量。因此，缓解过程删除了大量的“正常”流量以及违规的 DDoS 流量，从而在此过程中影响了服务和用户。

看看我们都能从这次故障中学到什么。

在评估特定 DDoS 防护解决方案的有效性时，必须查看我们（正确）阻止了多少 DDoS 攻击流量，同时衡量缓解措施对合法（或“良好”）流量的影响。缓解措施的真正效果在于尽可能接近 0% 的假阴性率（不将任何 DDoS 流量作为好的流量传递）和 0% 的误报（不阻止被识别为 DDoS 的良好流量，从而避免大规模的“计算机说不”问题）。这实际上是同一个刀片的两个边缘：这些指标中的任何一个都很容易得到 0%，但要让它们都正确（或尽可能接近零）要困难得多。

在过去 20 年中，使用传统方法和传统 DDoS 防护解决方案的组织可接受的误报率为 5%到 10%。随着 DDoS 流量的增长以及 DDoS 攻击的频率和复杂性的增加，这将转化为在大规模 DDoS 攻击得到缓解时随时消除数 TB 的合法客户流量。

那么，我们如何使用诺基亚基于 Deepfield Defender 的 DDoS 防护解决方案来降低这两个指标（漏报和误报）呢？这里 AI/ML 派上了大用场。在过去的几年里，我们一直在利用监督学习技术来持续衡量我们的 Deepfield Secure Genome® 模型（由我们的 Deepfield Defender 客户使用）与全球最大的真实 DDoS 攻击样本集合之一的有效性，该样本由全球 DDoS 威胁联盟（GDTA） 的合作客户提供。

让我们考虑一个例子，其中诺基亚的应急响应团队创建了一个新的缓解规则来解决新的攻击媒介。这个新规则被添加到我们的测试版规则集中，然后针对 GDTA 攻击样本的大部分子集运行，更重要的是，针对实际的“和平时期”流量样本运行。新规则只有在提高缓解覆盖率并且不会增加这些“和平时期“样本的合法流量的误报率时，才会添加到实时客户部署中。

我们通过测试模拟攻击，并测量这些不同样本中假阴性和假阳性的百分比来确认情况确实如此。然后，我们可以在客户的网络（Deepfield 实例）中部署新模型，以便使用他们自己的流量在本地运行推理，并且知道它只会帮助阻止 DDoS。

毫无疑问，阻止 DDoS 流量至关重要。但是，衡量 DDoS 防护效率的真正标准在于在不影响合法用户的情况下缓解不良流量，这是我们致力于应对的挑战。