MEMCACHED 反射攻击：
DDoS 的新纪元

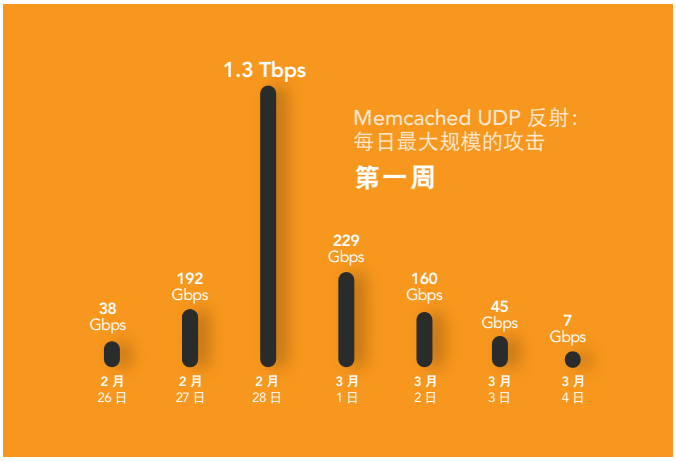
当攻击者发现并采用新的大规模 DDoS 反射和放大方法之后，DDoS 攻击的规模在 2018 年初增加了一倍，这种方法有可能使其攻击资源增加 50 万倍。称为 *Memcached UDP 反射*的攻击向量使用免费暴露在互联网上的资源 — 不需要恶意软件或僵尸网络。

2018 年 2 月 28 日，针对 Akamai 客户发起了迄今为止记录的最大规模 DDoS 攻击，其中 Memcached 反射 DDoS 流量达到了创纪录的每秒 1.3 Tb (Tbps)。与 Mirai 物联网 (IoT) 僵尸网络发起的上一次创纪录的 DDoS 攻击规模相比，此次攻击的规模是其两倍多。

Akamai 的 Prolexic DDoS 防护服务在收到客户的网络流量后立即抵御了巨大的 DDoS 攻击，过滤掉了来自 Memcached（一种开源数据缓存工具）使用的默认端口的所有流量。清洁流量将从位于欧洲、美国和亚洲的 Akamai DDoS 净化中心返回到客户网络，因此不会进一步对客户的运营造成影响。

Memcached 通常用于缩短磁盘和数据库的查询响应时间，现已被使用反射 DDoS 技术的攻击者转变成了互联网武器。仅在大规模攻击的前两天才观察到由 Memcached 反射造成的第一次 DDoS 攻击。在发生 1.3 Tbps 攻击时，Akamai 已经实施了自动化抵御措施来及时防范针对我们客户的 Memcached 攻击。

在第一周内，针对身处多个行业的 Akamai 客户发起了 19 次 Memcached 反射 DDoS 攻击。



令人惊讶的 500,000 放大倍数和数据包速率

Memcached 反射具有令人惊讶的放大因子：一次 210 字节的请求会触发一次直接针对目标的 100 MB 响应。按照设计，Memcached 数据将以高速率进行传送：Akamai 测得此次攻击期间的速率为每秒 1.27 亿个数据包 (Mpps)。

在不受保护的互联网服务器上（默认情况下已启用 UDP 通信协议），Memcached 会将其数据发送给任何询问者，包括具有欺诈性的 IP 地址。超过 1,000 个 ASN 上的成千上万台服务器参与了 1.3 Tbps 的攻击，每个攻击平均传送了将近 1 Gbps 的攻击流量。研究人员估计，互联网上有超过 90,000 台 Memcached 服务器，目前有超过 50,000 台容易作为反射器被攻击者利用。

预计将出现更多的 Memcached DDoS 攻击和赎金 DDoS

随着安全社区注意到其他反射 DDoS 攻击向量的持续流行，依靠远程系统管理员来修补、重新配置或移除易受攻击的服务器不太可能带来立竿见影的效果。Memcached DDoS 攻击将在可预见的未来出现。

对于 Memcached 之类的反射 DDoS 攻击，攻击者不需要恶意软件即可感染和控制僵尸网络中的爬虫程序。即使是不熟练的攻击者也能发起攻击。Akamai 发现客户会为识别易受攻击的 Memcached 服务器而增加扫描次数。更多攻击者会滥用更多的 Memcached 服务器来生成各种规模的 DDoS 攻击。此外，Memcached 有效负载正被用于提供勒索消息；Akamai 建议不要支付任何赎金。

DDoS 攻击使本地网络管道陷入瘫痪

除了已做好充分准备的基于云的 DDoS 防御和内容交付网络 (CDN) 提供商（如 Akamai）和最大的 ISP 以外，很少有组织能通过可用的网络容量在面对更大的 DDoS 攻击（当然不是这种规模的攻击）时保持运营。进入数据中心和边缘路由设备的网络管道将首当其冲，这让现场 DDoS 抵御变得无计可施。

DDoS 防御规划的重要性

遭受这一创纪录的 DDoS 攻击的 Akamai 客户事先做了充分准备，结果为了抵御攻击，在经历停机后不到 10 分钟就将流量路由到了 Akamai。客户提前使用了 Prolexic DDoS 防护服务，制定并实施了 DDoS 行动手册，因此相关人员知道该做什么以及给谁打电话。监控网络流量，在发现异常情况后，相关人员在短短的五分钟时间内就将所有网络流量路由到了 Akamai。

为什么选择 Akamai：为获得 DDoS 恢复能力而构建

Akamai 通过我们的 CDN、Prolexic 网络和分布式 Fast DNS 基础设施来保护我们的客户免遭 DDoS 攻击。我们加大投资，不断改进这些平台的 DDoS 恢复能力。

在最高级别上，Akamai 的容量规划模型可承受我们能够证实的最大 DDoS 攻击，并用该流量乘以一个比例因子，从而提供充足的余量来应对攻击规模的增大。因此，我们能够成功抵御包括本次攻击在内的最大、最错综复杂的 DDoS 攻击，即使它们的规模增加一倍也能抵御。

我们的对抗性恢复能力团队不断评估新威胁和事件，以便发现 Akamai 系统中潜在的断裂点，并与工程团队一起实施自动抵御措施，共同提升各个领域的恢复能力。

内容交付网络中的 DDoS 恢复能力

除容量之外，我们还构建我们的 CDN，从而实现在不利条件下的可用性和恢复能力，而不只是防御 DDoS 攻击。借助在全球部署的 220,000 多台服务器，Akamai CDN 能够对个别服务器的状态加以调整，并自动路由用户流量，以便避开中断和拥塞。每台服务器都具有 DDoS 抵御功能，包括速率控制、黑名单和地域拦截。

Prolexic 网络中的 DDoS 恢复能力

Prolexic 网络是世界上最强大的 DDoS 净化服务之一。它由七个全球净化中心组成，有超过 3.5 Tbps 的容量，并有 150 个安全专家组成的团队，每个月可抵御数千次 DDoS 攻击。每个净化中心都有多个 1 级运营商连接和超过 500 个对等体的公共对等互联，可在 OSI 协议栈的多个层面上开展高性能流量分析和主动抵御。我们不断增加 DDoS 防护能力。

Fast DNS 基础设施中的 DDoS 恢复能力

Akamai 提供权威的 DNS 服务，即 Fast DNS，旨在实现高可用性、速度和 DDoS 恢复能力。我们随后将域名服务器分配至 20 多个隔离的 DNS 云中的客户，以最大程度降低针对任何 Akamai 客户的 DDoS 攻击可能对其他客户造成的影响。域名服务器群集和其他控制措施可以最大程度降低本地化 DDoS 攻击的影响。

结论

近 20 年来，Akamai 致力于抵御 DDoS 攻击，即使在承受最大 DDoS 攻击的时候，也做到了对客户的保护，并且保持基础设施可用性。Akamai 持续调查和报告新威胁，并且我们还会持续改进我们的规程和平台，做到始终领先于恶意图谋。我们将利用自身为所有客户提供保护的丰富经验，提高我们的保护能力。我们承诺为 Akamai 客户提供业界最稳健的平台。

审查您自己的 DDoS 恢复能力

如果您希望 Akamai 帮助审查您的基础设施的恢复能力，请联系我们的**专业服务机构**，以获得由我们安全架构师提供的咨询服务。

请访问 **https://www.akamai.com/memcached** 了解更多信息。

Akamai