Akamai

网络安全大师：

打造防御第 7 层 DDoS 攻击的终极秘籍

目录

前言

即便是技能高超的安全专业人士，在面对当今的分布式拒绝服务 (DDoS) 攻击时，也很难找到合适的防御措施。所以对于更为复杂的第 7 层 DDoS 攻击，可能会更加力不从心。这种情况下，一种行之有效的解决办法是提供一套分步式操作说明，介绍如何使用不同的方法来应对不同的威胁。换言之，制作一份第 7 层 DDoS 攻击防御指导手册。

不同攻击者会采用不同的方法来准备发起 DDoS 攻击。第 3 层和第 4 层的攻击更偏向于实力比拼。谁会有更大的网络容量，攻击者还是防御者？第 7 层攻击则不同，这种攻击针对的是开放系统互连 (OSI) 模型的应用层，而应用层负责直接与软件应用程序交互。攻击的目标是通过占用容量、内存分配或者侵入这些系统处理请求途径中的弱点，彻底耗尽 Web 服务器、数据库或应用程序的资源。

因此，在抵御第 7 层 DDoS 攻击时会面临特殊的挑战，因为此类请求通常显示为合法的流量，想要筛选掉恶意请求但不影响合法用户，就会变得非常困难。此外，由于攻击可以利用自动化技术和云资源，这使得攻击者可以更轻易地快速发动大规模攻击。

在本文中，我们探讨了抵御第 7 层 DDoS 攻击时面临的难题，并详细介绍了攻击者采用的方案（包括所用的工具和技术）、应对这些攻击的检测和抵御策略，以及事件后分析与恢复建议。

Akamai 在内容分发、网络安全和分布式云平台领域拥有成熟的经验，同时在全球设有 4,200 多个接入点，所以我们对当今的 DDoS 攻击形势有着独到的见解。应用层 DDoS 攻击日趋复杂，涉及的层面也多种多样，因此必须要有深刻的见解，并采取全面的防御策略。本文将满足您的这些需求。

不论您是身处一线的安全专业人士，想要寻求有关应对特定威胁或漏洞的帮助，还是作为 CISO 希望改善安全状况，这份指导手册都可以为您带来打造安全屏障的成功秘籍。

第 7 层 DDoS 攻击的常见目标和示例

第 7 层 DDoS 攻击针对的是 OSI 模型的顶层，也就是应用层。这些攻击的目标是侵入 Web 应用程序处理请求的途径，以此来耗尽目标资源。第 7 层 DDoS 攻击的常见目标包括：

Web 服务器：攻击者将 Web 服务器作为目标，干扰向合法用户分发内容。这可能会导致网站加载速度缓慢，甚至可能完全无法访问。

Web 应用程序：依赖于数据库或后端服务的应用程序非常容易遭受第 7 层 DDoS 攻击，因为这些攻击会侵入应用程序在解析请求、处理请求或管理会话时的弱点。

应用程序编程接口 (API)：在现代化的 Web 服务和移动应用程序中，API 是非常关键的组成部分。攻击者会针对 API 发起攻击，干扰不同软件服务之间的交互，进而影响到依靠这些 API 的应用程序的功能。

DNS 服务：虽然 DNS 攻击还可能发生在其他层，但第 7 层攻击会涉及到利用恶意请求来轰炸 DNS 服务，从而干扰域名解析，导致大面积出现可访问性问题。DNS over HTTP/TLS 的采用日趋普遍，会导致此类攻击的增长。

电子邮件服务器：针对电子邮件服务器的攻击会干扰通信，同时影响到传入和传出电子邮件。

支付网关和金融服务：对于攻击者而言，这些都是相当有利可图的目标，他们通过干扰交易来造成金融运营的混乱。

Akamai 的互联网现状 (SOTI) 报告和安全见解会定期分析第 7 层 DDoS 攻击的发展形势，并重点介绍多元化的攻击媒介以及高风险行业。

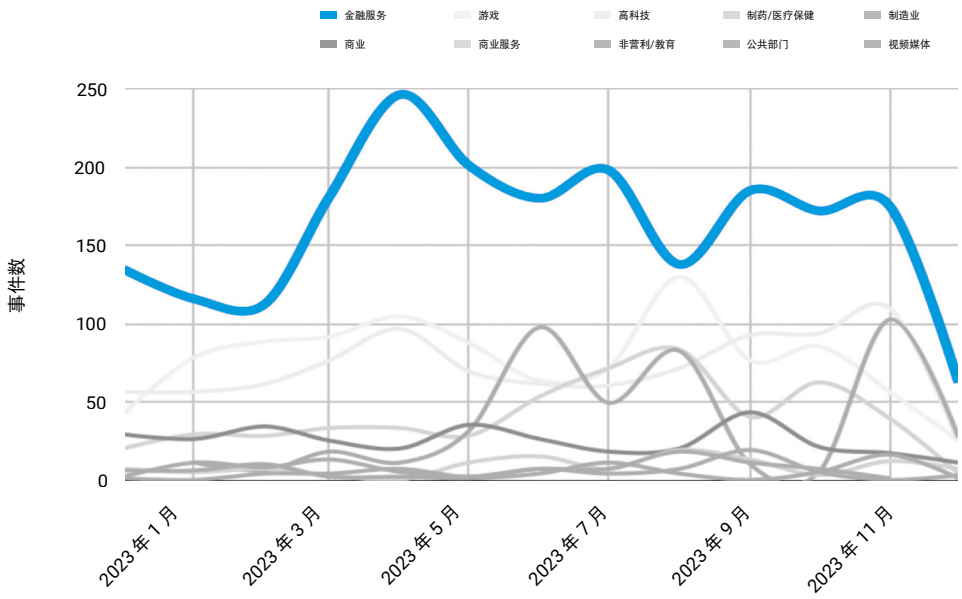
攻击媒介

- Web 应用程序和 API 攻击：一般情况下，攻击者针对的是网站入口点，包括通常由于其内容或配置而不进行缓存的 API 端点。一些常见的攻击目标路径包括“/”、“/home”、“/en-us”、“/pricing/”等。
- 常见的攻击媒介包括：
  - 针对主页的 HTTP GET/POST 泛洪
  - 针对随机路径和查询字符串的 HTTPS GET 泛洪
  - 慢速读取攻击
  - 大文件上传泛洪

此外，每年遭受 DDoS 攻击的公司数量都是有增无减，但现在的攻击方法已经大为不同。首先，受攻击资产的类型和体量发生了变化。例如，攻击者不再对相同或相似的端点发起 10 次攻击，而是针对网络空间中的不同 IP 发动 100 次攻击。这些攻击不仅针对第 3 层，还同时针对第 7 层。

目标行业

2023 年，金融服务业、博彩业和制造业遭受分布式拒绝服务 (DDoS) 攻击的事件次数急剧上升，尤其是欧洲、中东和非洲地区，超过了其他所有地区的总和。

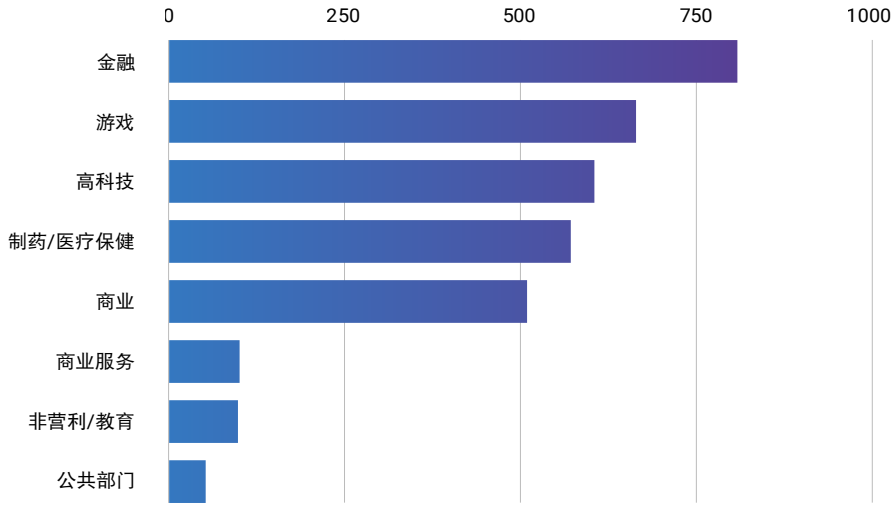


DDoS：仍在延续，2024 年 3 月

金融服务行业更是成为第 7 层 DDoS 攻击增长的重灾区。自 2021 年以来，Akamai 发现，针对金融服务公司的 DDoS 攻击数量出现了不同于其他行业的显著增长。2023 年，在所有行业中，金融服务机构遭受的攻击数量占攻击总数的三分之一 (35%) 以上，从而超越游戏业，成为更受攻击者觊觎的目标。Akamai 的分析师发现，全球 63% 的 DDoS 攻击针对的是银行业。在欧洲、中东和非洲，几乎四分之三 (72%) 的攻击集中在银行业，而在亚太地区这一数字甚至达到了 91%。然而在美国，DDoS 攻击则更平均地散布在银行业、保险业和其他金融服务机构中。

美洲：金融服务业遭受的 DDoS 攻击占比为 28%

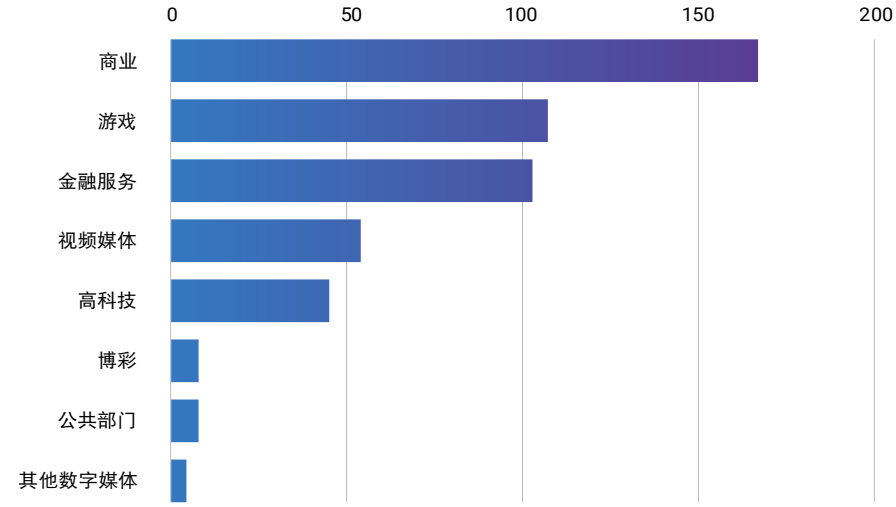
2023 年 6 月 – 2023 年 12 月



DDoS：仍在延续，2024 年 3 月

亚太地区：金融服务业遭受的 DDoS 攻击占比为 11%

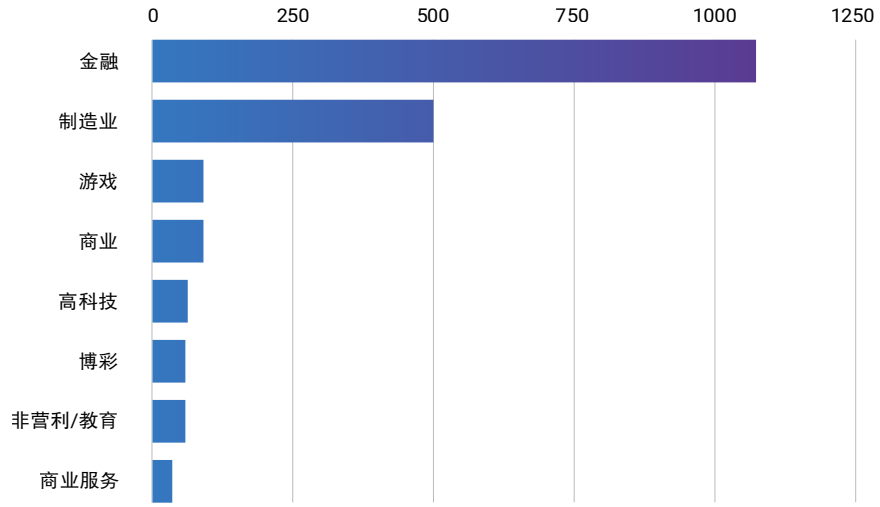
2023 年 6 月 – 2023 年 12 月



DDoS：仍在延续，2024 年 3 月

欧洲、中东和非洲地区：金融服务业遭受的 DDoS 攻击占比为 66%

2023 年 6 月 – 2023 年 12 月



DDoS：仍在延续，2024 年 3 月

在最近的一个示例中，Akamai 的一家金融服务客户遭受了一起复杂的第 7 层 DDoS 攻击，网络攻击者利用自动化技术并制造出了高度分散的攻击。这种攻击使用 HTTP GET 泛洪，主要目标是不可缓存的 URL（例如主页和登录端点）。我们利用各种主动式的控制措施，成功防御了此次攻击，避免了对客户的源端点造成影响。此次攻击的来源热图突出显示，对云服务提供商、Tor 出口节点以及匿名或开放的代理节点的使用量出现增加：

匿名系统发起的 DDoS 攻击

2024 年第 1 季度针对一家金融机构发起的一次应用层攻击的示意图，攻击范围覆盖 100 多个国家/地区，Akamai 帮助抵御了此次攻击

DDoS 攻击者能够构建和协调分布极为广泛的攻击基础架构，利用遍布全球众多国家和地区的广泛网络中的动态 IP 地址。

攻击者使用的工具和技术

很不幸的是，DDoS 攻击者及其使用方法并不是一成不变的。攻击者不断摸索利用攻击来牟利的套数，他们在调整技术，利用新工具和寻找新方法。有很多因素证明了这一演变。

自动化：攻击者使用自动化脚本和爬虫程序来模仿合法用户行为，使得检测显著变得更加困难。此外，攻击者现在会转为利用机器学习算法，通过它们来适应和规避传统的检测方法。

多媒介攻击：攻击者越来越多地采用多媒介策略，结合运用不同的攻击类型（例如 GET 和 POST 泛洪）与 DNS 目标（例如放大攻击和碎片攻击）以及其他组合攻击方式，从而实现彻底耗尽网络和应用程序资源的目的。

以 API 为目标：随着企业在应用程序的使用中越来越依赖于 API，攻击者也发现了新的机会，可以在其 DDoS 攻击中利用 API 漏洞。这些攻击的目标是耗尽服务器的资源，其手段包括同时发出成千上万的连接请求，或者利用逻辑漏洞，从而导致服务中断。

利用物联网设备：物联网设备数量急剧增长，然而通常未能得到妥善保护，这为僵尸网络提供了庞大的武器库。这些设备经常遭到劫持，利用其网络连接和计算能力来发起大规模的 DDoS 攻击。

复杂程度提高

DDoS 攻击利用这些新的工具和技术，复杂性和攻击频率也随之提升，攻击者会使用错综复杂的方法绕过传统的防御措施。下面列出了一些明显的趋势：

加密：明显转向基于 HTTPS 的 DDoS 攻击的趋势，使得抵御攻击更加困难。这些攻击会进行加密，伪装成合法流量，这加大了检测并筛选掉这些攻击的难度，因为传统的 DDoS 防护措施在解密应用层 SSL/TLS 流量方面存在限制。

僵尸网络和代理：由于 DDoS 僵尸网络显著增长以及攻击者普遍使用匿名代理，现在会从大量 IP 地址发送请求（通常每次攻击会有超过 10,000 个 IP）。一些防御措施针对单个 IP 计算请求数量，攻击者使用此策略可以绕过这样的措施。而云托管平台的盛行以及云端服务的采用，只会让策划这些高强度和高度分散的攻击变得更容易。

匿名系统发起的 DDoS 攻击

近期针对 Akamai 金融客户的应用层 DDoS 攻击的示意图：每秒交易数 (TPS) 达到 650,000，吞吐量达到 20 Gbps，请求总数超过 90 亿

DDoS 攻击者能够构建和协调分布极为广泛的攻击基础架构，该基础架构主要源自云提供商。

防御者采用的方法也在不断发展，有一种方法会根据每个 TLS 指纹跟踪请求，这种指纹由多个 TLS 层信号组成，例如密码类型及其顺序。虽然这种方法容易产生误报，但如果能够正确使用，当攻击者从大量的机器和 IP 发起攻击时，此方法可提供更有效的防御措施，因为被入侵的设备上安装的是同一个软件。这些设备会表现出类似的环境特征，其中之一就是共享 TLS 库。

常见要素溯源

虽然市场上提供的工具经常变化，但攻击技术的发展表明，攻击方法正朝着更复杂、更难于检测的方向发展。其中包含：

- **被入侵的物联网设备：**攻击者在发起大规模的 DDoS 攻击时，仍会使用僵尸网络中被入侵的物联网设备，这突显出这些设备长久以来存在漏洞。
- **DDoS 出租服务：**DDoS 出租服务的出现，降低了发起攻击的门槛，就算不具备全面技术知识的个人也能够发起大规模攻击。

- **规避技术：**先进的规避技术越来越常见，如随机化标头参数和动态请求参数等。利用这些技术后，更难将恶意流量从合法请求中区分开来，为传统的检测和抵御方法带来了更大的挑战。

此类攻击常用的漏洞

在第 7 层 DDoS 攻击中，攻击者利用的漏洞通常与 Web 应用程序处理用户输入和管理数据的方式相关。在抵御这些漏洞的过程中，结合运用多种安全措施至关重要。

近年来，在开展应用层 DDoS 攻击时，被利用的最著名的一个漏洞是 HTTP/2 快速重置漏洞，该漏洞在 2023 年底便已面向大众广泛宣传。此类攻击利用了 HTTP/2 协议中的漏洞，而该协议是互联网及所有网站的运营基础协议。与上一季度相比，利用此类漏洞发起的 HTTP DDoS 攻击流量在一个季度内总体增长了 65%，说明了利用此漏洞的攻击的严重性和影响。

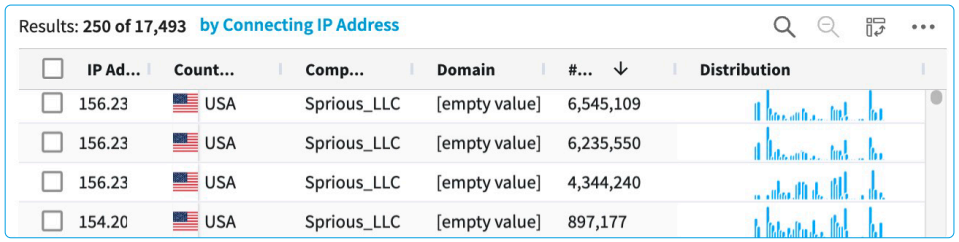
这个特殊的漏洞使得攻击者可以利用云计算平台和 HTTP/2 来造成更大的影响，这样利用相对较小的僵尸网络即可进行海量 DDoS 攻击。这些攻击重点针对的行业包括游戏业、IT、加密货币、计算机软件和电信业，美国、中国、巴西、德国和印度尼西亚是这些攻击的最大源头。

为了进行应对，许多行业在全行业协调开展了披露 HTTP/2 快速重置漏洞 (CVE-2023-44487) 的工作，以阐明使用此漏洞的 DDoS 攻击。此攻击针对各类提供商，一些领先的云提供商和 CDN 服务提供商均在此列。

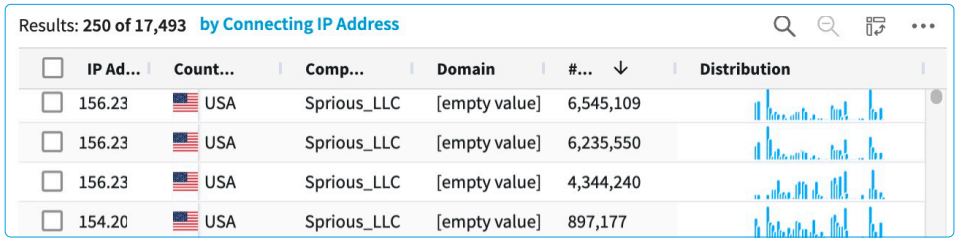
真实示例：一起 DDoS 攻击中对自动化技术的使用

在同一批 DDoS 攻击中，攻击者通常使用多种 DDoS 工具开展攻击，而每种工具会将多种技术结合起来使用，以便绕过安全产品，或者至少降低安全产品的效率。下面使用 Akamai Web Security Analytics 得到的分析数据，举例说明一起这样的攻击。

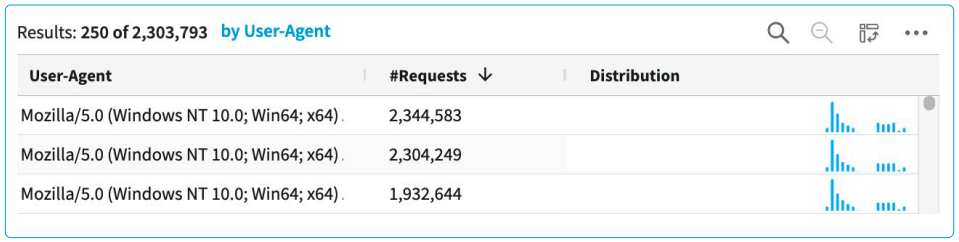
- 发现攻击来自 17,000 个 IP 地址



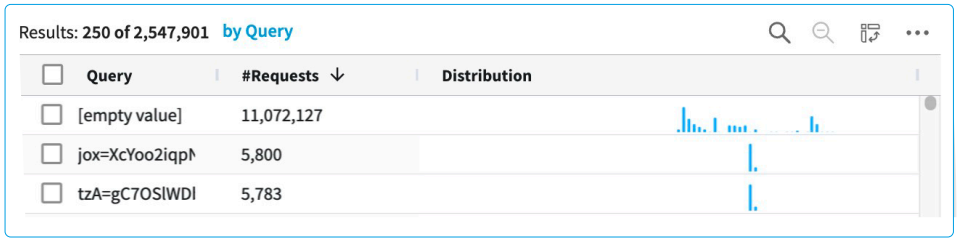
- 攻击源自 400 多个网络



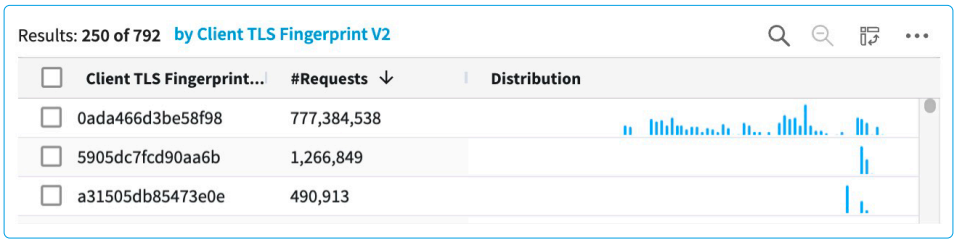
- 2,303,793 个不同的用户代理



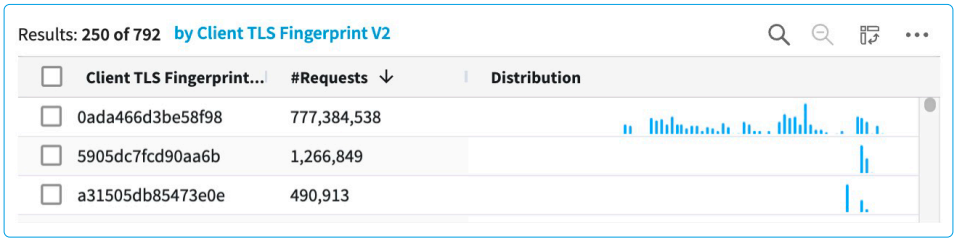
- 2,547,901 个不同的随机查询字符串



- HTTP 标头轮换（例如，Accept-Language、Referer）



- TLS 设置轮换



抵御此类复杂攻击需要采取分层保护策略。将主动控制措施和被动控制措施结合使用不失为一种有用的方法，例如，在速率限制中，使用请求匹配和源流量特征的高级组合，或者使用源声誉控制措施。

攻击手段不断升级：TLS 信号仿冒

近期的观察表明，恶意攻击者在其 DDoS 工具中，会更频繁地使用 TLS 信号，使得此类连接看起来更像是来自合法的 Chrome 浏览器，从而规避检测措施。攻击者并没有使用需要大量资源的 Chrome 无头版本（可能会减缓攻击速度），而是可能采用了 TLS 库的修改版本，使得他们可以设置和模拟任何真正浏览器的 TLS 信号。虽然有一些工具设计用于复制 TLS 指纹，但在 DDoS 攻击工具中，这类工具并不常见。这种攻击类型的使用，表明攻击者的技术能力和对防御的深入了解都有所提高，正因为如此，第 7 层 DDoS 攻击的防御策略必须包括定期对最新攻击趋势开展研究。这似乎也表明，包括 TLS 欺骗在内的 DDoS 工具变得越来越常见。

准备好打造您自己的防御之道

一探究竟：评估风险和识别漏洞

您可以通过确定关键资产及其中可能易受 DDoS 攻击的位置，来大幅增强第 7 层 DDoS 抵御策略。此风险评估可以帮助您根据资源的重要性和易受攻击性，确定哪些资源需要优先保护。在了解了潜在的攻击媒介及其影响之后，企业可以实施具体的应对措施，例如速率限制、Web 应用程序防火墙和行为分析，从而有效地缓解风险。此外，采用连续风险评估，您就可以根据新出现的威胁和不断变化的业务需求来发展防御策略。

不同的行业和企业可能会采取不同的方法来进行应用层 DDoS 风险评估。例如：

电子商务：在开展大型促销活动之前开展风险评估，可能会发现结账流程中存在严重漏洞。可以采取的抵御措施包括实施 Web 应用程序防火墙 (WAF) 和速率限制来保护该服务。

金融服务：对于银行业应用程序，风险评估可能会发现登录页面是 DDoS 攻击的主要目标。然后，银行可以将针对端点定制的速率限制与行为检测结合使用，来区分合法用户和攻击流量。

了解特定漏洞之后，就可以实施有针对性的防御措施，并在攻击期间增强关键服务。

避免分工不明：明确角色和职责

在制定有效的第 7 层 DDoS 防御策略的过程中，务必要明确相关的角色和责任。只有这样，在发生攻击时才会尽可能确保井然有序地开展工作和高效地做出响应。如果角色不明确，响应工作可能会一片混乱，职责重叠而且防御工作漏洞百出。明确职责可以帮助每位团队成员明确自己的具体任务，例如监控流量和识别异常，以及实施抵御策略和与利益相关者沟通等等。这种井井有条的工作方式有助于将攻击影响降到极低，维护服务可用性并保护关键资产。

实际上，有过多的决策者而角色并不明确时，在 DDoS 攻击期间反而会导致响应延误。例如，如果网络运营团队和网络安全团队分别决定采取不同的缓解方法，而缺乏相互配合，他们可能会无意中抵消对方的努力或者忽视关键漏洞。正确的策略需要预先定义角色，例如制定事件响应负责人、通信协调员和技术响应团队，确保在面对攻击时敏捷地采取一致的行动，尽可能缩短停机时间，并简化事件后分析。

量身选择合适的工具

检测和抵御应用层攻击颇具挑战性，其中一项原因就是很难区分合法流量和恶意流量。为了应对这些不断演变的威胁，建议采用多层面的防御方法：

- **重点采用始终开启方案还是按需方案：**确保 DDoS 安全控制措施始终保持活动状态，并持续更新事件响应计划，以快速解决新出现的威胁。
- **建立具备恢复能力的可靠架构：**预测可能出现的单点故障，因为攻击者可能会针对多种服务发起攻击，包括 DNS、Web 应用程序、API 以及数据中心和网络基础架构。使用合适的架构对于防范第 7 层 DDoS 攻击至关重要。在选择这些架构时，需要注意的事项包括选择边缘还是基于 CDN 的 DDoS 防护措施，后者是始终开启的保护。不要高估可靠性。当今 DDoS 攻击的规模可以很轻易地攻陷大多数基础架构。
- **评估您的提供商的 SLA**，并确保与您的策略保持一致。
- **审查提供商的准备情况：**在选择提供商时，原则是提供商应该定期展示其关键网络组件审查过程并评估不同的 DDoS 防护机制，以深入了解提供商能否有效地应对当前的攻击方法。
- **查阅您的 DDoS 攻击响应行动手册：**整合您的 IT、运维、安全和客户沟通人员，以增强应对攻击的准备措施。
- **紧急 DDoS 防护：**制定好计划，在发生紧急情况时，能够让 DDoS 抵御解决方案提供商立即提供援助。如果您有 DDoS 防护供应商合作伙伴，请拨打他们的 DDoS 支持热线。

检测和抵御方法

要想在第 7 层有效防范 DDoS 攻击，您需要采取多种检测和抵御策略。您可以运用多种方法，每种方法都有自己的优势和关键考量因素。

基于行为和异常的检测

优势：这种方法依靠使用机器学习和统计分析来了解您的正常流量模式，从而识别可能表明发生 DDoS 攻击的异常流量。这种方法对于复杂的、以前未曾发现过的攻击非常有效。

考量因素：这种高效的检测存在一段学习期，可能需要几周的时间来建立“正常”流量的基准，而在此期间检测功能可能不会那么有效。如果没有经过准确的训练，模型可能会返回误报。

基于速率和吞吐量的检测

优势：此方法易于实施，监控请求的速率和大小，在流量超过预定义的阈值时触发告警或缓解流程。它可以高效快速地识别大规模高容量的攻击。

考量因素：合法的流量高峰（例如在促销活动期间的流量）可能会被误认为是 DDoS 攻击。此方法可能无法检测到一直处于监控中的低容量、低速率的攻击。

基于签名的检测

优势：此方法是将流量与数据库中的已知威胁模式进行对比，从而快速确定并阻止识别出来的威胁。对于常见的和以前已经识别出来的攻击媒介，这种方案极为高效。

考量因素：此方法无法检测到新出现的攻击方式，也无法检测到修改过而无法与现有签名匹配的攻击。为了确保有效性，此方法需要定期进行更新。

质询-响应测试

优势：此方法会对传入流量发出质询，确认流量是人还是爬虫程序生成的。CAPTCHA 或 JavaScript 计算可以有效地防御爬虫和自动攻击工具。

考量因素：如果实施了过于激进的质询策略，可能会干扰用户体验。更复杂的爬虫可能具备绕过一些质询-响应策略的能力，因此您需要定期更新质询机制。

混合方法

将多种检测和缓解策略结合使用，可以提供更全面的防护。例如，使用基于异常的检测来标记可能的攻击，然后将基于速率和基于签名的方法作为补充来实现更全面的检测范围，这样就能打造出更可靠的防御机制。质询-响应测试可以进一步从合法用户中筛选掉复杂的爬虫程序。

传统方法

IP 和地理位置筛选：阻止或限制来自特定 IP/CIDR 范围以及与您的业务无关的地理区域的流量，可以减少您暴露在源自这些区域的攻击中的危险。在业务用户的来源位置已知且位置数量有限时，这种方法非常有用，然而持续维护和更新可接受来源名单经常造成难题。此外，经验丰富的攻击者会利用代理来绕过地理位置拦截。虽然如此，在防御第 7 层 DDoS 攻击时，这仍然是一种常用的选择，可以作为初始防御策略。

应用层协议分析：此方法审查应用层协议中的数据来检测异常或恶意模式，实现了主动式防御机制，用于抵御第 7 层 DDoS 攻击。此方法可以防范能够绕过传统安全措施的复杂 DDoS 攻击，但不利之处在于，深度数据包检测会造成资源高度占用，并且误报（会无意中阻止合法流量）的可能性更高。

寻找稳妥而平衡的方法，打造多层 DDoS 防御策略

打造多层 DDoS 防御策略需要采取精妙的方法，根据企业的具体风险概况以及不断演变的网络威胁形势来量身打造。此策略的核心是要求进行初始评估，用以确定关键资产和可能的攻击媒介，然后实施基准防护措施，如速率限制和防火墙。高级步骤需要混合使用多种方法：对新威胁采用基于异常的检测，对已知攻击采用基于特征的检测，以及采用质询-响应机制来筛选掉爬虫程序。

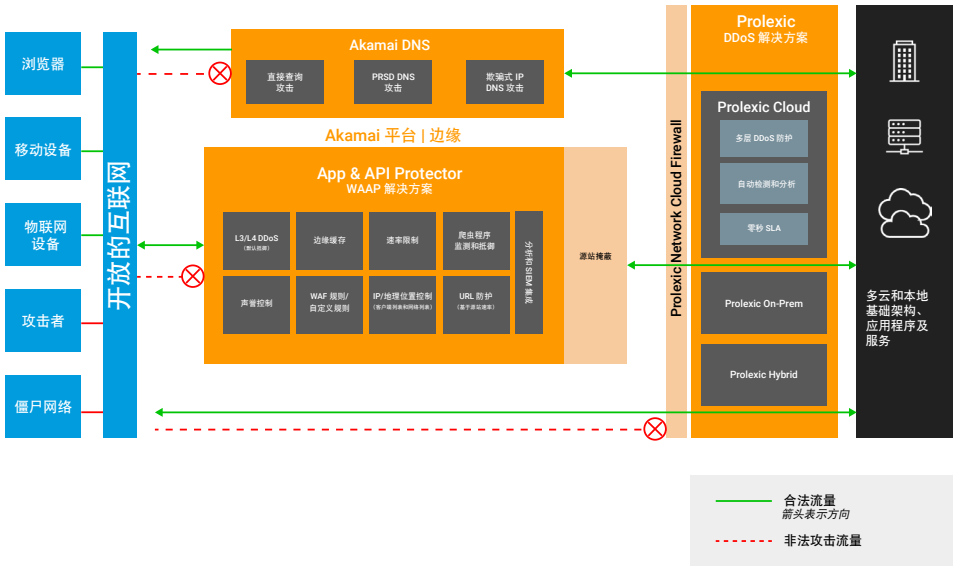
此外还可以融入自适应的威胁情报，例如确定已知和新出现 DDoS 攻击源的 TLS 指纹模式的算法，让安全系统可以自动调整其抵御措施，来阻止或质询显示该指纹的流量，从而有效地抵御攻击。在攻击期间和攻击之后，要想尽可能减少损害和保持客户信任，实施全面的事件响应和恢复计划非常关键。根据过去的攻击和新出现的趋势不断学习和调整，可以确保防御策略的有效性和恢复能力。

一家金融机构在应对复杂的多媒介 DDoS 攻击时的表现，清晰地展现出了制定平衡的多层防御策略的重要性。这些机构成为主要攻击目标的原因是，停机会对其运营和客户信任造成巨大的影响。

通过结合采用多种检测和抵御方法，例如流量异常检测，使用速率限制、IP/地理位置筛选、IP 声誉和实时威胁情报等传统方法，并辅以可靠的事件响应计划，金融机构可以保护关键资产免于中断，同时确保向客户提供的服务的连续性。这种全面的方法展示了在当今的数字化环境中，企业如何防御多层面的 DDoS 攻击。

未雨绸缪：借助 Akamai 边缘架构打造深度防御策略

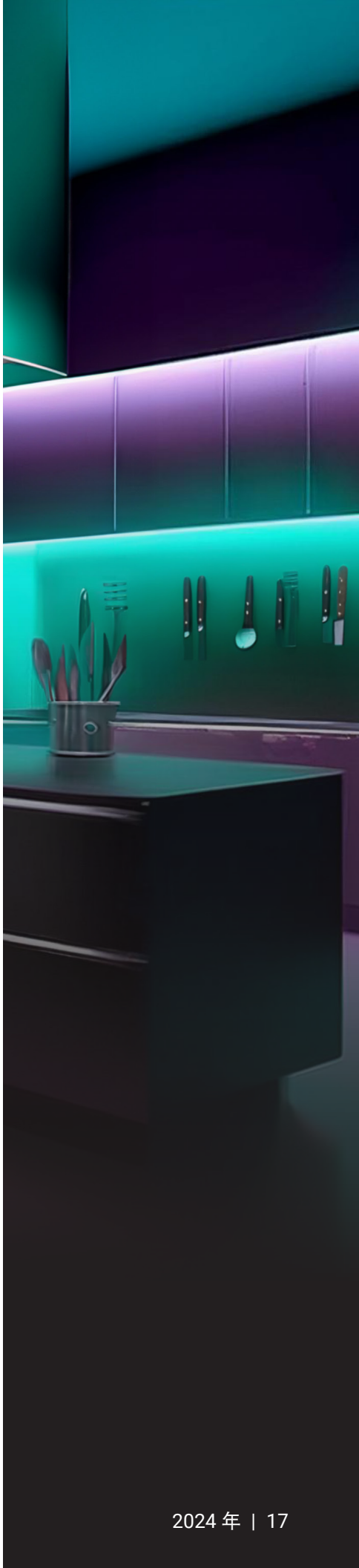
针对应用层 DDoS 防护，Akamai 采用了多层次、全面且具备自适应能力的方法，旨在保护网站、应用程序和 API 抵御大部分复杂的攻击。我们的 App & API Protector 使用了多种重要功能，可以提供全面的保护，将可见性和抵御措施、API 安全以及第 7 层 DDoS 防护融于单个产品中，提供广泛的保护功能。



使用 Edge DNS、App & API Protector 以及 Prolexic 解决方案的全面 DDoS 防护的参考架构

Akamai 的 DDoS 防护策略基于边缘防御架构而构建，通过 Akamai 的大规模分布式平台路由流量，在该平台中实时检查每个请求。此方案可以在边缘位置防御 DDoS、Web 应用程序和 API 攻击以及恶意爬虫程序，阻止这些威胁因素进入应用程序或基础架构。这种方法可以维护快速、高度安全且始终可用的架构，能够随着攻击规模而扩展，从而增强业务连续性。

Akamai 提供了一套强大的工具和组成要素，涵盖主动和被动控制措施，可在整体防御策略中各司其职。



主动控制措施

主动控制措施有助于防止攻击的发生，侧重于加强安全状况以尽可能减少漏洞。其中包括：

- **IP 控制措施（拦截 IP、CIDR 范围和 ASN）：**作为一个基础防御层，这些控制措施可以阻止通过威胁情报确定的已知恶意 IP 地址或范围。
- **地域控制措施（拦截特定地理位置）：**通过允许或限制来自特定地区的流量，企业可以先发制人，主动防止自身暴露于源自高风险区域的攻击中。
- **Web 应用程序防火墙 (WAF) 规则：**针对已知的漏洞和攻击媒介（例如 FiberFox 等 DDoS 工具）实施规则，可以打造出可靠的第一道防线。
- **IP 声誉控制措施：**启发式地使用情报，根据 DDoS、Web 抓取和其他恶意活动的已知恶意资源，先发制人地阻止或审查可疑流量。
- **平台 DDoS 情报：**利用来自遍布全球的 Akamai 边缘平台的 DDoS 攻击见解，打造主动式防御策略，用于对抗应用层 DDoS 攻击。
- **缓存：**优化内容缓存，从边缘缓存来服务请求，这样可以显著减少源站服务器上的负载，间接减少 DDoS 影响。
- **Site Shield：**源站掩蔽，即通过 Akamai 边缘网络来仅允许流向源站的请求，这样可以进一步减少服务器负载。

被动控制措施

被动控制措施是对检测到的攻击的响应，旨在减轻其影响并保持服务可用性。

- **速率限制（速率策略）：**这些策略对于防止突然出现的流量高峰非常关键，这些高峰可能预示着 DDoS 攻击。您可以根据客户特定的流量概况来设置和定制配置。速率限制通常可以作为第一道防线，帮助保护客户的源站服务器免遭大量分散的 DDoS 攻击。
- **慢速 POST 防护：**此控制措施专门针对慢速 HTTP POST 攻击，针对意图耗尽服务器资源的异常流量模式做出响应。

- **WAF 中的自定义规则：**您应该能够快速定制规则来应对新出现的威胁，从而实现灵活动态的防御机制。
- **爬虫程序监测和抵御：**利用机器学习功能来检测浏览器仿冒，您可以识别并阻止通过自动化技术发起的复杂 DDoS 攻击。
- **使用智能减载技术进行 URL 防护：**利用控制措施，限制对源站服务器的过多请求并优先处理合法用户而非恶意流量，这样可以帮助您在遭受 DDoS 攻击期间维护服务正常运行。
- **平台 DDoS 情报：**减载是一类 URL 防护措施，使用来自遍布全球的 Akamai 平台的情报，使得客户能够创建主动防御策略来抵抗应用层 DDoS 攻击。

多种要素叠加，运用秘诀打造平衡方案

- 示例：大型金融服务企业利用 Akamai WAAP 解决方案打造深度防御策略

一些企业可能会发现自身更经常地遭受 DDoS 攻击。例如，根据 Akamai 的研究，2023 年，超过三分之一的 DDoS 攻击针对的是金融服务机构。Akamai 有一家大型金融服务企业客户，该客户发现自己的登录页面遭到了针对性的攻击。而该客户能够采用一套成熟的防御方案。您也可以这样做。

攻击者简介：黑客行动主义者

目标：登录端点

方法：HTTP POST 泛洪攻击

攻击来源：约 66,000 个 IP 地址，来自约 140 个国家/地区

秘诀

抵御 HTTP POST 泛洪攻击

组成要素：

主动控制措施：

- **IP 控制措施**：使用威胁情报来阻止与已知恶意实体关联的 IP 地址或 CIDR 范围。
- **地域控制措施**：将来自以庇护黑客组织而闻名的地区的流量拉入禁止名单，例如与“Anonymous Sudan”相关的地区。
- **Web 应用程序防火墙 (WAF) 规则**：实施专门用于应对已知 DDoS 工具和手段的规则，包括 HTTP GET 泛洪的典型模式。
- **IP 声誉控制措施**：认真监控或（实时）主动阻止来自声誉分数较差的来源的流量。
- **平台 DDoS 情报**：应用来自 Akamai 全球 DDoS 攻击数据的见解，预测和应对新出现的威胁媒介。
- **Site Shield**：启用防火墙访问控制列表 (ACL)，仅允许来自 Akamai 边缘网络的流量，阻止其他流量。

被动控制措施：

- **速率限制**：建立速率策略，防范流量中突然出现的峰值，为主页的每秒请求数量设置合适的阈值。通过以下方法来调优速率限制：(1) 将测量请求速率的时间窗口缩短到每秒一个请求，以及 (2) 根据连接 IP 来源的地理位置和声誉分数应用速率限制，同时将金融机构的公司 IP 地址和合作伙伴等来源列入允许名单。
- **WAF 中的自定义规则**：创建定制规则，用于在检测到攻击后应对其中的特定特征。在自定义规则中使用流量采样控制措施有助于进行流量分析，从而更高效地发现热门攻击来源，而在自定义规则中使用 IP/地域控制措施有助于快速缓解攻击。
- **爬虫程序监测和抵御**：使用浏览器仿冒检测来识别和阻止模仿合法用户行为而实则是泛洪攻击的请求。
- **URL 防护**：实施控制措施，以便限制特定于登录 URL 的请求速率，保留合法用户的带宽。使用代理、Tor 出口节点、基本爬虫程序、低声誉 IP 等类别来设置智能减载，有助于优先处理真实的用户流量，而不是那些疑似恶意来源。

准备方法：

审查阶段：

- **审查配置**：对当前的安全状况进行全面的审查。根据您的调查结果配置主动控制措施，确保妥善管理了所有相关的地域和 IP 控制措施。
- **配置优化**：调整配置来识别和抵御不正常的流量模式，包括 HTTP POST 泛洪攻击的特征。

检测和抵御阶段：

- **监控和告警**：Akamai 的边缘防御架构可以监控传入流量，发现其中表明可能出现了 DDoS 攻击的模式。您可以针对符合已知 DDoS 方法（例如 HTTP POST 泛洪）的异常流量峰值或模式设置告警。
- **检测和抵御**：在您正确设置了各种主动控制措施后，例如 IP 声誉、缓存以及 IP/地域控制措施，系统就可以自动提供检测和抵御功能。检测到攻击时，各种控制措施，例如速率限制、URL 防护以及浏览器仿冒程序检测功能就会自动运转，无需任何用户干预。
- **分析和调整**：持续分析攻击模式并实时调整防御措施，以应对不断变化的攻击手段。例如，根据近期的攻击流量分析，创建量身定制的规则或速率限制策略。

恢复和攻击后分析：

- **日志分析**：在攻击发生之后，进行详细的流量日志分析，用于识别攻击媒介以及所部署控制措施的有效性。
- **调整**：根据从攻击分析中获得的见解，对主动和被动控制措施进行必要的调整。

建议：

- 定期审查并更新您的防御策略，以适应不断变化的 DDoS 攻击手段。在不同企业中，受其具体需求、威胁状况以及行业最佳实践影响，此类审查工作也会大为不同。金融服务企业可能需要每季度开展此类审查工作，而电子商务平台可以制定每半年审查一次的目标，用于准备应对季节性购物高峰。
- 为安全团队提供持续培训，从而更好地识别和应对新型 DDoS 攻击媒介。
- 开展模拟攻击，测试部署措施的有效性，并让团队为真实事件做好准备。

恢复和攻击后分析

在防御应用层（第 7 层）DDoS 攻击时，攻击后阶段对于强化未来的防御措施和了解对手非常关键。这涉及到两个关键步骤：分析攻击模式，以及根据分析结果来增强防御措施。对于制定具备恢复能力的防御策略以及确保在线服务的连续性和完整性，这些步骤至关重要。

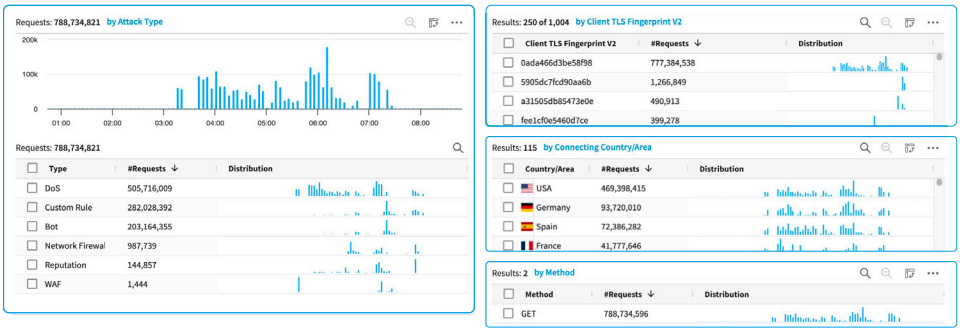
分析流量和攻击模式

处理攻击后的下一步是分析事件，以便了解哪些策略发挥了作用，哪些策略的效果不及预期。此评估要融入长期因素，例如对客户信任的影响、数据完整性以及潜在的财务损失。在这一阶段中，像 Akamai Web Security Analytics 这样全面的安全分析系统是必不可少的工具，可以帮助企业了解攻击流量及其影响。

此分析涉及剖析攻击者使用的攻击手段、技术和流程 (TTP)。要解决的关键问题包括：

- 流量高峰是什么性质?
- 攻击针对了哪些具体的应用程序功能?
- 攻击是否利用了任何已知漏洞?

Akamai Web Security Analytics 可以识别流量中的异常，确定攻击的地理位置源头，并根据观察到的行为对攻击类型分类。以下示例展示了可用于调查 DDoS 攻击的一些流量特征或维度。



图示内容源自 Web Security Analytics，其中提供了前所未有的对安全事件的监控能力和主动分析

根据攻击分析结果，审查并更新防御策略

根据攻击分析结果来审查并更新防御策略，这是企业强化网络安全状况的一个关键组成部分。通过在攻击过后对细节进行检查，企业可以发现其现有防御措施中的漏洞，并做出明智的调整。以下是使用 Akamai Web Security Analytics 来完成此流程的一些例子。

示例 1：根据攻击模式更新 WAF 规则

场景：企业面临的第 7 层 DDoS 攻击针对的是其 Web 应用程序，攻击行为向应用程序的主页发出了大量恶意请求。

审查：攻击分析表明，现有的 Web 应用程序防火墙 (WAF) 规则足以检测到 90% 的攻击流量并加以阻止，然而仍漏掉了大约 10%，因为在地域允许名单中，明确允许了来自该地理位置的攻击来源，导致应用程序不堪重负。

更新：根据此分析，企业更新了其 WAF 配置，以使用与来自该具体地域的攻击流量的特定特征相匹配的自定义 WAF 规则。更改规则之后，可以继续允许该地理位置，但会根据攻击流量的特定特性来阻止它。此外，进一步严格了针对该地理位置的速率限制设置。

示例 2：增强源站防护能力

场景：一家零售网站的登录流程遭到复杂的第 7 层 DDoS 攻击，该攻击利用了自动爬虫程序，并且分布极为广泛。

审查：攻击后分析表明，攻击流量极为分散，来自 150 多个国家/地区，有数百个看起来像是合法浏览器的 TLS 指纹。其中很大一部分流量来自云提供商，一些提供商作为可信合作伙伴来源列入了允许名单中。虽然攻击得到了有效的缓解，但分析结果表明需要额外的防御措施。

更新：为了保护具有大量计算需求的 URL（例如结帐流程），这家企业实施了 URL 防护，这是一项专门设计的功能，用于保护计算密集型的 URL 和 API 端点免遭高度分散的应用层 DDoS 攻击。安全架构师还针对爬虫程序、代理、IP 声誉等启用了智能减载。URL 防护的这种子功能可以首先拒绝来自疑似恶意来源的请求，从而优先处理真实用户流量。

同时，企业决定在 WAF 中启用内置的爬虫程序防护功能，由于采用了本地爬虫程序解决方案，所以之前企业并未充分考虑到这一点，但是本地解决方案在这种高速攻击期间无法随之扩展。

示例 3：针对 API 端点实施速率限制

场景：金融服务应用程序的 API 端点被大量欺诈性交易请求淹没，这表明发生了第 7 层 DDoS 攻击，意图耗尽服务器资源。

审查：攻击模式分析表明，攻击者专门针对没有得到妥善防护并且无法处理大量请求的 API 端点。

更新：作为应对措施，企业对所有 API 端点实施了严格的速率限制，尤其是那些识别为易受攻击的端点。企业还采用了专门的 API 安全附加模块，针对 API 安全性提供多层高级防护功能，包括 API 逻辑滥用、影子 API 威胁和 API 漏洞监控。

策略要点

- **持续监控和日志记录：**建立健全的监控和日志记录系统，及时发现异常情况，并准确评估攻击期间和攻击之后的损害。
- **漏洞管理：**定期更新和修补系统，抵御已知漏洞，减少被利用的风险。
- **攻击模式分析：**使用合适的监测工具，深入分析攻击模式，用来了解攻击者的方法和意图。

攻击后分析

在可靠的第 7 层 DDoS 防御策略中，评估损害和分析攻击模式是至关重要的组成部分。这些步骤不仅有助于了解和抵御攻击造成的直接影响，还可以为持续改进防御机制提供信息，确保更好地准备应对未来的威胁。

维护和更新抵御策略

要维护可靠的第 7 层 DDoS 防御，需要持续监控最新的趋势和技术。

攻击者不断地混用攻击模式，利用新的工具和漏洞。为了积极主动地应对这些威胁，企业必须投入时间和精力开展研究工作、进行监控、评估防御措施、打造自动化防护措施，并与威胁情报社区合作。

监控领先的网络安全论坛只是一个良好开端。我们建议采用更加规范的方法：

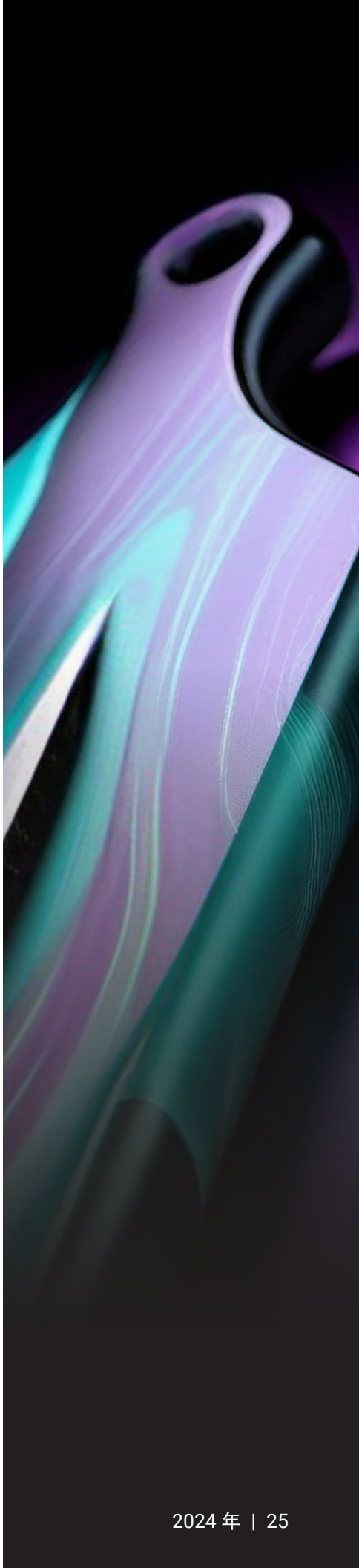
持续监控和评估 —— 定期监控您的网络和应用程序性能，以检测出表明出现了威胁的新模式或异常。使用此数据来评估您现有防御机制的有效性，确定可以改进或调整的领域。

组建防 DDoS 攻击团队 —— 在企业内确立可靠的人员或团队，负责研究和监控 DDoS 攻击形势，并且面向企业内更广泛的部门，每季度至少报告一次任何关键发现和建议。

与威胁情报社区交流 —— 攻击者彼此之间会交流最新、最有效的攻击方法。因此，任何原因都不应该阻止您与其他公司和行业中的同事交流最佳防御实践。随时掌握最新的威胁情报。订阅第三方安全信息源，参与网络安全论坛，并与业内同事合作。此信息可帮助您预测新的攻击媒介，并相应调整防御措施。

寻求网络安全提供商的帮助 —— 技术提供商通常有专职的威胁研究团队，而具有内容交付网络的提供商可以提供其他地方所没有的见解。您应该尽可能地利用这些学习机会。定期与安全咨询专家交流也是理所应当的。

测试自己的防御措施 —— 如果您没做好成功防御的准备，那就是在为失败做准备，实践出真知等等，无论用什么样的套话，主旨都是一样的：定期开展测试和演习会带来回报。



定期开展审查和模拟攻击场景（红队演习），测试您的防御策略的恢复能力。这些练习可以发现您当前设置中的漏洞，并揭示攻击者可能会如何侵入您的系统。

每年至少开展一次网络测试。对于测试案例，近期的攻击概况可以作为一个很好的参考，尤其是您所在行业中发生的攻击。

与社区分享您的经验教训 —— 需要重申的是：正如攻击者会分享他们的攻击工具和手段一样，企业也应该就成功的防御策略进行知识分享。

通过记录成功案例和失败案例，网络安全专家可以提供切实的见解，丰富群体知识库的内容。参与行业论坛，为这一领域中的那些新人提供指导，并参与协作项目，所有这些对于打造一个强大的防御生态系统至关重要。这些工作不仅有助于开发出更有效的策略和工具，而且可以提供多样化的经验和见解，以应对攻击者不断变化的手段。这种协作精神对于在网络安全领域中保持领先至关重要，每一项贡献对于建设一个更强大、恢复能力更好的数字化世界，都具有宝贵的价值。

重要信息

DDoS 威胁的形势一直在变化，攻击者会不断寻求新的方法来绕过防御措施。维护并更新您的第 7 层 DDoS 防护策略是一个持续不断的过程，您需要保持警惕，不断适应新的情况，并采取主动的方法。通过随时了解最新信息、定期进行测试和审查，以及培养持续改进的文化，您就能够针对当前和未来的威胁保持强有力的防御措施。

总结

很显然，第 7 层 DDoS 攻击不仅越来越复杂，而且由于自动化技术的进步以及攻击者之间的协调配合，发起攻击变得更加容易。与此同时，企业必须应对更大规模、更复杂的威胁形势，而且失败的成本还在攀升。

实际上，炮制防御策略并非易事。面对第 7 层 DDoS 攻击，没有任何单一方法能够有效抵御它。正如我们所展示的那样，将多种检测和防御策略结合在一起，采用多管齐下的方法，可以提供最强大的防御。

此外，在选择方法时，应该以具体的需求、流量模式以及所保护应用程序或服务的风险概况为指导。您不能在不了解业务、流量和漏洞的情况下构建防御措施。定期更新和调整这些策略，对于适应不断变化的 DDoS 威胁形势非常重要。

最后，很明显的是，并不是攻击结束之后您的工作就完成了。攻击后分析和调整对于确保持续的防御成功非常关键，而且，这个阶段对于推动知识分享以及您在这个行业中的职业发展也会有很大的作用。

幸运的是，Akamai 可在全过程中很好地为每个步骤提供帮助。从应用程序和 API 保护，到对全球流量的深入见解，再到专家开展的攻击后分析，众多公司纷纷利用此机会，从一家供应商处寻求所需的全部第 7 层 DDoS 防护。

查看 Akamai 第 7 层 DDoS 防护的实际应用。
免费试用 App & API Protector。

致谢名单

编辑与创作

Aseem Ahmed

Barney Beal

审稿和主题撰稿

Abdeslam Bella

Sean Flynn

Alex Marks-Bluth

Nitesh Shrivastava

Prathmesh Verma

Dennis Birchard

Ryan Gao

Pawan Sajnani

Patrick Sullivan

Danielle Walter

营销与发布

Georgina Morales Hampe

Shivangi Sahu

Akamai Security 可为推动业务发展的应用程序提供全方位安全防护，而且不影响性能或客户体验。诚邀您与我们合作，利用我们规模庞大的全球平台以及出色的威胁监测能力，防范、检测和抵御网络威胁，帮助您建立品牌信任度并实现您的愿景。如需详细了解 Akamai 的云计算、安全和内容交付解决方案，请访问 akamai.com 和 akamai.com/blog，或者扫描下方二维码，关注我们的微信公众号。发布时间：2024 年 10 月。

扫码关注 - 获取最新云计算、云安全与CDN前沿资讯