Akamai

白皮书

威胁客户信任的攻击媒介

安全性和品牌信任从未像现在这样高度相互依存。随着应用程序和 API 的广泛应用，品牌在全球范围内的展示方式正经历着变革，同时，全球网络攻击数量急剧上升，这使得在不损害客户体验的前提下，确保数字应用程序的安全成为世界各地安全团队的首要任务。

出色的客户体验可以建立品牌信任，进而对业务绩效产生可衡量的影响。企业在权衡网站性能、数据保护以及这两者之间的各种因素时所做的安全决策，往往会对客户体验造成不利的影响。保护企业的控制措施如果过于繁琐，会在多个方面给客户带来不便，削弱了客户的信任，最终导致收入的减少。

安全决策也会影响企业的发展和创新。随着企业不断推进数字化进程，将数据和应用程序迁移至云端，不计其数的攻击者都瞄准这些迁移举措所暴露出的攻击媒介。现在，安全解决方案必须不断演进，以预先防范攻击者日益变化的策略和复杂的多媒介攻击（这些攻击可能同时或快速连续地以不同形式发起）。为此，您需要选择能够协同工作的安全解决方案，以确保贵公司的安全，并维护客户对您品牌的信任。

您应当重点关注哪些攻击媒介?

受到威胁的最新重要目标：API

应用程序几乎驱动着业务的方方面面，而用于连接各种软件以及在各种应用程序之间实现通信的应用程序编程接口 (API) 已成为攻击者钟爱的新目标。为什么？涉及 API 的应用程序和业务流程的启动和部署速度往往比安全团队进行相关评估的速度更快，从而导致出现错误配置和漏洞。这些漏洞正是攻击者所瞄准的目标。他们通过滥用业务逻辑，成功实施 API 攻击，从而能够渗透进您的环境，窃取数据，甚至进一步发起其他攻击。而且他们的攻击目标不仅仅是能够穿过您的 Web 应用程序防火墙的 API。即使您的 Web 应用程序防火墙进行身份验证，API 仍然易于遭受攻击，这表明攻击者现在会定期侦察以确定要利用的特定 API。

需要牢记的是，任何 API 都有可能成为攻击目标。例如，在医疗保健等行业，物联网设备的互操作性使 API 成为了企图窃取个人身份信息 (PII) 或发动勒索软件攻击的犯罪分子垂涎三尺的目标。因此，保护 API 需要从了解与您企业相关的每个 API（也称为您的 API 资产）开始。

Akamai API Security 可以真正地帮助您清点自己的资产，并提供对每个 API 历史行为的监测能力，以便您了解正常的 API 行为和滥用的 API 行为。在掌握这些信息之后，您便可以搜寻活跃的威胁，进而在攻击者达成其目标之前及时阻止滥用行为。

比以往更复杂且更易于部署：恶意爬虫程序

爬虫程序每时每刻都在您的网站中活动着。实际上，您在搜索引擎优化方面所做的一切努力都是为了获得它们的青睐。恶意爬虫程序与良性爬虫程序混杂在一起，前者会伺机发起一系列网络攻击。恶意爬虫程序最臭名昭著的行为是垄断有限的库存，例如囤积限量版运动鞋或者大量音乐会门票或酒店预订，但在分布式拒绝服务 (DDoS) 攻击中，爬虫程序也采用了大致相似的方法，通过发送数量过多的请求导致贵公司的网站不堪重负，其目的是让贵公司的网站离线。

很多人不知道的是，DDoS 已成为相对简单且低成本的攻击形式，新的一批攻击者正在利用这种攻击形式让价值数十亿美元的公司和关键公共基础架构（包括学校、医院、机场和公用事业提供商）陷入瘫痪。这些攻击者会造成大规模服务中断，导致受害者每分钟损失巨额收入。与过去传统的攻击者显著不同的是，这些攻击几乎都是由老练的民族国家攻击者、政治黑客以及职业网络犯罪分子借助僵尸网络发动的，僵尸网络是由爬虫程序感染并控制的联网设备（可以是用户设备或简单的物联网设备）组成的大型网络。

爬虫程序也用于发动会引发帐户接管攻击的撞库攻击。撞库攻击是指攻击者利用从大规模数据泄露事件中窃取的一系列用户名和密码，试图在多个其他机构上进行大范围的登录尝试。攻击者会部署爬虫程序来执行数百万次帐户接管尝试，由于许多用户习惯性地重复使用用户名和密码，导致这些尝试中有一小部分能够成功接管帐户。在攻击者获得帐户访问权限后，该攻击便成为帐户接管攻击。

撞库攻击只是攻击者用于接管合法帐户的众多方法之一。一旦他们控制了某个帐户，他们便会窃取会员积分并转移数字资产、用光礼品卡余额，以及使用存储的信用卡信息进行欺诈性购物。他们甚至可能将整个帐户打包出售给其他攻击者。一旦您的客户遇到此类问题，他们对您的信任几乎不可避免地会受到严重损害。然而，即便是未能成功的撞库攻击也会对您的品牌造成损害。因为在这些登录尝试过程中，大量爬虫程序涌入您的网站，会极大降低资源可用性，并导致响应时间增加，从而给您的客户和网站访客带来极其糟糕的体验。

最后，抓取类爬虫程序也有良性和恶意之分，但其影响并不总是显而易见，这些爬虫程序可能在不经意间降低网站性能并污染各企业作出重要决策所需的指标，因此它们对您品牌所产生的副作用可能比它们抓取内容产生的影响更加糟糕。

Akamai 有一套解决方案，专门用于抵御恶意爬虫程序所带来的威胁：

Akamai App & API Protector（含 Malware Protection 附加模块）是防范数据、PII 和其他帐户信息被盗的基础手段，可用于阻止爬虫程序驱动的 DDoS 攻击以及勒索软件、恶意软件等。此产品旨在保障客户对您网络资产的持续访问，并在您遭遇攻击时确保网站性能不会下降。

Akamai Bot Manager 可以检测所有爬虫程序流量并在边缘抵御恶意爬虫程序。它使用 AI 模型来分析爬虫程序行为，并部署浏览器指纹识别和机器学习 (ML) 算法来逐步提升检测的准确性。这样不仅有效保护用户免受欺诈活动的侵害，还能提升用户体验的流畅性。

Akamai Content Protector 不仅可以防止抓取类爬虫程序窃取可用于恶意用途的 Web 内容，还可以防止网站性能下降。利用 ML 驱动的检测功能，我们能够根据风险等级对潜在的恶意抓取类爬虫活动进行分类，从而采取恰当的应对措施。

另一个用于保护客户的基础解决方案是增强安全帐户访问。Akamai Account Protector 可以阻止通常由爬虫程序配合进行的人为欺诈，同时允许受信任的用户顺畅、安全地访问您的网站，从而鼓励他们更长时间和更经常地访问您的网站。

恶意脚本的成本：客户端威胁

类似于爬虫程序，第三方脚本大多是有益的。它们通常用于启用各种功能、营销工具、分析工具等，以便全面提升整体用户体验 (UX)。但它们也会将网络浏览器变为危机四伏的客户端威胁面。

客户端威胁意在诱骗客户访问恶意内容。它们会利用在用户（通常为您的客户）操作的计算机（即客户端）上运行的应用程序中的漏洞来实施攻击。因此，客户端安全涉及一系列技术和策略，旨在保护客户免受网页上恶意活动的侵害。

脚本攻击不仅会给企业带来沉重的经济损失，还会损害与客户、合作伙伴以及支付处理方之间建立的信任关系。所以，支付卡行业数据安全标准 (PCI DSS v4.0) 的新要求着重强调了客户端安全的重要性也就不足为奇了。为了确保符合相关安全标准，任何在线处理支付卡业务的企业都必须清晰了解自身网站上正在运行的脚本、这些脚本的变更时间以及它们何时停止运行。

抵御这些攻击并非易事。由于第三方脚本数量庞大且持续变化，因此很难对它们进行监控。脚本攻击自身也有各种形式，例如 Web 数据窃取和表单劫持。许多犯罪集团（其中最臭名昭著的便是 Magecart）都是基于这些技术来窃取支付卡数据和 PII。

在当前的数字支付、在线购物和研究环境中，特别是在涉及收集个人和财务数据的结账及支付页面上，客户端安全比以往任何时候都更加重要。您需要了解网站上运行的所有脚本，并具备检测可疑行为的能力，同时实施防御措施来防范攻击。Akamai 提供了专用解决方案来应对这些威胁：

Client-Side Protection & Compliance 可以保护所有用户免受 Web 数据窃取、表单劫持和 Magecart 等客户端攻击，维护客户在浏览器中的隐私和信任。

保护基础架构，守护客户体验

客户体验的核心在于底层数字基础架构，它能够支撑与您品牌有关的一切事物。DNS 安全、可靠性和性能可确保客户能够在需要时随时访问您的服务。从本质上讲，DNS 系统决定了您的在线状态。当 DNS 系统瘫痪时，您的整个数字业务也会瘫痪。正是由于这个原因，攻击者不断地利用 DDoS 攻击手段，针对目标的 DNS 系统进行攻击。鉴于当前各行业竞争日益激烈，为确保客户和潜在客户享受到您品牌所能提供的卓越服务，持续稳定的 DNS 可用性和 100% 的正常运行时间变得至关重要。

Akamai 提供黄金标准的解决方案组合，保护您的数字基础架构免受各种 DDoS 攻击：

为了实现强大的 DDoS 防御能力，Akamai Prolexic 提供了多种保护方案，包括分布在全球 32 个地点的净化中心以及惊人的 20 Tbps 专用防御容量。

Akamai Edge DNS 提供全面、专用、权威的 DNS 解决方案，该解决方案利用 Akamai Connected Cloud 的规模、安全性和容量来管理您的 DNS 区域。

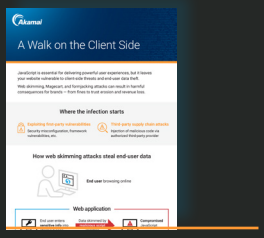
Akamai Shield NS53 是一个强制实施动态安全策略的双向 DNS 代理解决方案。无论您的源站 DNS 基础架构在本地、云端还是采用混合方案，您都可以使用该解决方案来保护基础架构免受资源耗尽型攻击。

我们是您确保客户信任的合作伙伴

在超过 25 年的时间里，Akamai 始终致力于帮助品牌展现魅力。作为内容交付网络的先驱者，我们率先解决了首批数字店面面临的速度问题。在过去十年里，我们借助自身庞大的内容交付网络的流量监测能力，每日不间断地监控和分析威胁。这项持续的研究使我们能够紧跟攻击媒介的演变趋势，自然而然地升级我们的安全解决方案。作为客户的重要安全合作伙伴，我们共同致力于保障客户业务的稳定运行，并精心呵护他们的客户体验。同时，我们给予客户充分的信心，鼓励他们勇于探索并引领行业前沿的新数字体验。

后续步骤

下面提供了一些参考资源，可帮助您考虑保护品牌的下一步最佳措施：



利用客户端保护措施增强网页完整性。

为网站、应用程序和 API 获取一站式、零妥协的安全防御。

了解爬虫程序管理策略的首要考虑因素。

无论您在何处构建内容，以及将它们分发到何处，Akamai 都能在您创建的一切内容和体验中融入安全屏障，从而保护您的客户体验、员工、系统和数据。我们的平台能够监测全球威胁，这使得我们可以灵活调整和增强您的安全格局，让您可以实现 Zero Trust、阻止勒索软件、保护应用程序和 API 或抵御 DDoS 攻击，进而信心十足地持续创新、发展和转型。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，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 6 月。

扫码关注，获取最新CDN前沿资讯