SOTI

第 11 卷，第 2 期

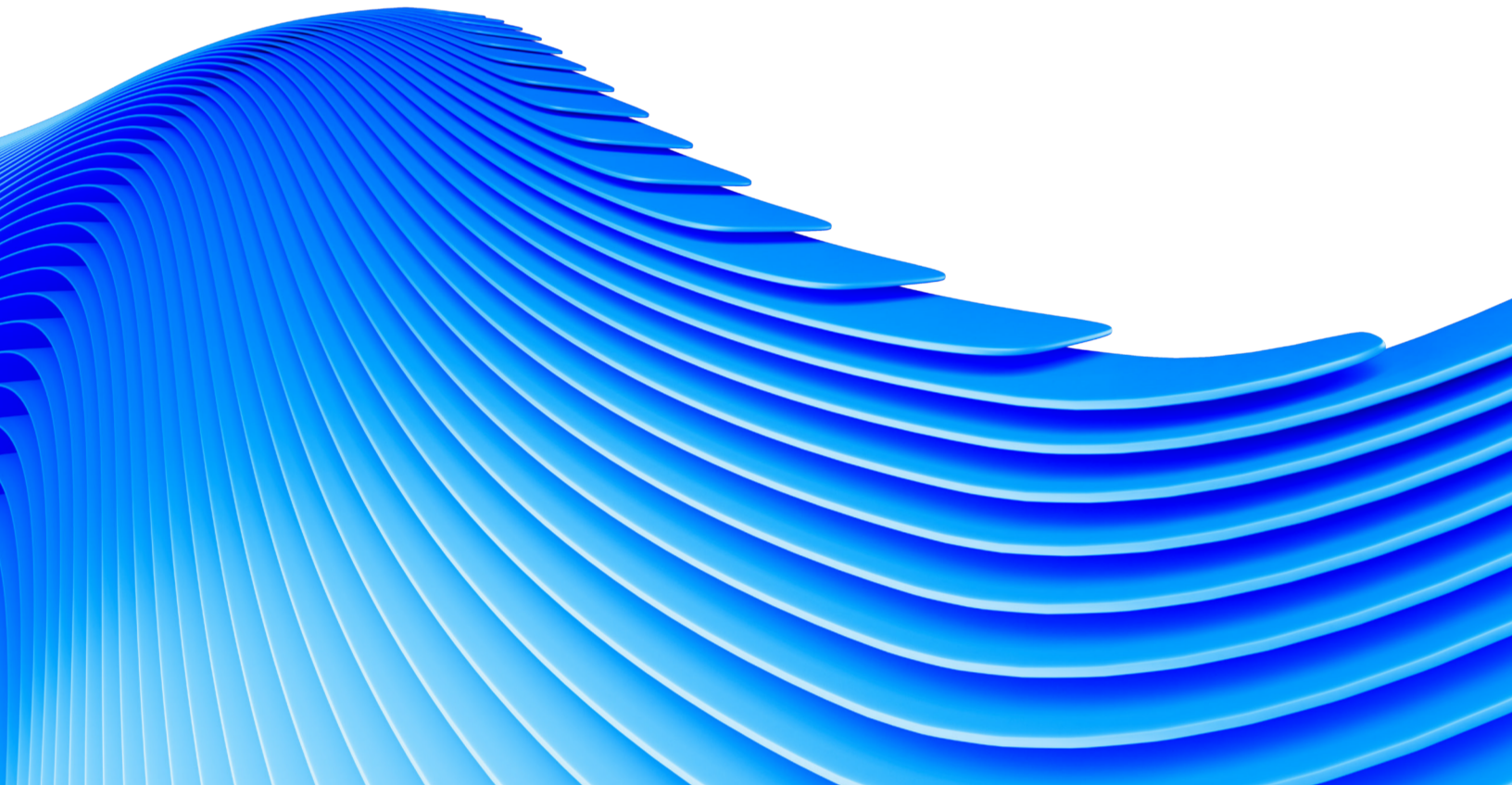
2025 年应用程序与 API 安全现状

AI 如何改变数字格局

Akamai

互联网现状/**安全性**

内容



引言

2025 年初，Web 应用程序安全领域呈现出前所未有的复杂态势，攻击手段也愈发精密。企业遭遇的 Web 应用程序攻击急剧增长——单单 2024 年，Akamai 便观察到超过 3110 亿次的 Web 应用程序攻击和 API 攻击，同比增加 33%。而此类攻击的激增，与云服务、微服务架构以及人工智能 (AI) 驱动的应用程序的加速采用密切相关。地缘政治因素进一步加剧了这种状况，高科技、商业和社交媒体行业遭受的第 7 层（应用层）分布式拒绝服务 (DDoS) 攻击最为严重。值得注意的是，攻击者现在正在部署由 AI 生成的杀伤链，使其整个攻击生命周期实现自动化。

与此同时，API 已成为主要攻击目标。Akamai 记录显示，2023 年 1 月到 2024 年 12 月期间，共发生超过 1500 亿次 API 攻击。AI 驱动的软件即服务 (SaaS) 工具通过 API 与核心平台的集成显著扩大了攻击面。由此带来的财务影响非常严重。目前，API 安全问题每年会给企业造成大约 870 亿美元的损失，并且预测表明，如果不采取足够的干预措施，到 2026 年此数字可能会超过 1000 亿美元。在日益复杂的 API 生态系统中，影子 API 和僵尸 API 成为特别脆弱的攻击媒介。

AI 对 Web 应用程序和 API 安全防护的作用

AI 技术增强了威胁检测和响应能力，在改变 Web 应用程序和 API 安全形势的同时也带来了新的挑战。在 Web 应用程序中，AI 用于自动完成威胁检测、预测潜在的漏洞以及缩短事件响应时间。然而，AI 也使得攻击者能够生成 AI 驱动的恶意软件和复杂的网络内容抓取手段，并利用动态攻击方法实现攻击生命周期的自动化。

对于 API 来说，AI 在管理和保护大量的 API 交互方面发挥着至关重要的作用。AI 驱动的工具对于检测异常情况、识别滥用模式以及实时自动应对威胁必不可少。AI 驱动的 API 管理将通过整合预测性分析和自动安全措施来持续发展演变，以抵御日渐复杂的攻击。尽管取得了这些进步，但撞库攻击和业务逻辑利用等依托 AI 技术对 API 进行的攻击仍然是一个重大问题，需要强大的安全框架来有效应对这些威胁。

存在分歧又相互关联：Web 应用程序和 API 攻击策略

虽然 Web 应用程序攻击和 API 攻击是相关的，但这两类攻击针对的是应用程序基础架构的不同方面：

- **Web 应用程序攻击**针对 Web 应用程序中面向用户的组件（例如面向公众的登录页面），并且往往采用不太复杂的技术。
- **API 攻击**则侧重于利用应用程序的 API 端点和后端逻辑中的漏洞，这需要更深入地了解 API 的结构和行为。

两者的主要区别在于其攻击面和复杂性。Web 应用程序攻击通常以应用程序的可见部分为目标，而 API 攻击会利用不同软件组件之间的通信渠道。但是，一旦成功，它们都可以使攻击者在未经授权的情况下访问敏感数据和系统资源。

同时了解针对 Web 应用程序攻击和 API 攻击的网络安全措施至关重要，因为现代应用程序的功能越来越多依赖于 API。企业预计两年内 Web 应用程序的数量将增加 39%，因此 Web 和 API 安全的相互依赖关系将变得更加明显。忽视任何一方面都会导致企业容易受到利用应用程序前后端漏洞的复杂、多媒介攻击的威胁。

Akamai 的独特视角：揭示威胁模式

Akamai 的网络基础架构处理着全球超过三分之一的 Web 流量，所以 Akamai 能够深入分析当前复杂局面，并对威胁模式提供独特见解。这种视角与来自 Akamai 研究和数据科学团队的见解相结合，使 Akamai 能够提供既全面又具备可操作性的情报。其分析结果可以为安全负责人提供必要的战略性见解，帮助他们确定降低风险的重点领域，从而最大限度地提高安全投资回报率。

报告的关键见解

AI 驱动的 API 比传统 API 风险更高。

大多数人工智能 (AI) 驱动的 API 皆可通过外部访问，并且许多 API 依赖不完善的身份验证机制，这一漏洞随着 AI 驱动的 API 攻击量不断增加而加剧。

AI 为攻击者的技术进步推波助澜。

随着 AI 的发展，恶意软件、漏洞扫描、针对 AI 集成系统的攻击和先进的网络内容抓取功能等方面也出现了长足进步。

32%

OWASP 十大 API 安全风险相关事件的增幅

API 安全事件在不断增加，开放全球应用程序安全项目 (OWASP) 十大 API 安全问题揭示了会暴露敏感数据和功能的身份验证及授权漏洞。

30%

与 MITRE 安全框架相关的安全告警增幅

攻击者正在使用自动化和 AI 等先进技术来利用 API。MITRE 框架可以帮助防御者更快、更准确地识别这些攻击。

33%

全球 Web 攻击量的同比增幅

攻击量的激增与云服务、微服务以及 AI 应用程序的快速采用密切相关，这些服务和应用程序会扩大攻击面并带来新的安全挑战。

2300 多亿次

商业企业遭受的 Web 攻击量，这使得该行业成为受影响最大的行业，其遭受的攻击量几乎是高科技行业（遭受攻击第二多的行业）的三倍。

73%

亚太地区及日本 (APJ) 遭受的 Web 攻击总数的同比增幅，

从 2023 年的 290 亿次飙升至 2024 年的 510 亿次。

37%

欧洲、中东和非洲 (EMEA) 地区以 API 为目标的 Web 攻击量占比，

该地区是所有地区中遭受此类攻击最为密集的地区。

94%

第 7 层分布式拒绝服务 (DDoS) 攻击的季度增幅

（2023 年第一季度到 2024 年第四季度）。

11.9 万亿次

北美地区遭受的第 7 层 DDoS 攻击的数量，

从 2023 年第一季度到 2024 年第四季度的两年内。

7 万亿次

高科技行业遭受的第 7 层 DDoS 攻击量

（2023 年 1 月到 2024 年 12 月），使其成为受攻击最严重的行业。

7.4 万亿次

APJ 地区遭受的第 7 层 DDoS 攻击量，从 2023 年第一季度到 2024 年第四季度的两年内。

20%

EMEA 地区遭受的与 API 相关的第 7 层 DDoS 攻击量占比，

表示此地区在所有地区中遭受的此类攻击最为密集。

不断改进我们的 API 威胁情报

Akamai 与 Noname Security 的整合显著增强了我们对 API 威胁的研究与报告能力，并为 API 特有的风险提供了全新的视角。Akamai 正在使用这个新的数据集（仍处于数据集成的早期阶段）来改进我们现有的威胁情报，并提供对 API 安全问题的深入分析。

关联告警与安全框架

随着时间的推移，这个新的数据集会将更深层次的安全告警细节与以下重要网络安全框架及合规标准关联起来：

- MITRE 对抗性战术、技术与通用知识库 (ATT&CK)
- 通用数据保护条例 (GDPR)
- 支付卡行业数据安全标准 (PCI DSS)
- 国际标准化组织 (ISO)
- 开放全球应用程序安全项目 (OWASP)

这些改进显著增强了 Akamai 为客户提供强大保护措施的能力。通过与这些框架接轨，各企业可以更清楚地了解自身的安全态势、遵守法规要求以及有效地优先处理其安全工作。这种全面的方法让企业能够战略性地分配资源，并制定有针对性的策略来保护其 API 和敏感数据。

分析 30 天的数据样本

为了撰写本报告，我们分析了 30 天的数据样本，以突出攻击者在各类网络安全框架和合规标准下的普遍活动特征（图 1）。我们也提供了对 MITRE 和 OWASP 告警更深层次的见解。此外，我们还将研究这些风险和安全事件如何影响合规标准。

	30 日活动	月度增长
OWASP	**5,907,000**	**32%**
MITRE	**2,817,000**	**30%**
ISO	**832,000**	**22%**
GDPR	**669,000**	**21%**
PCI DSS	**881,000**	**16%**

图 1：根据安全框架和合规标准细分的安全告警

MITRE 告警

在 30 天的时间内，我们发现客户中与 MITRE 技术相关的事件增加了 30%。值得注意的是，攻击者经常使用 T1078（有效帐户），利用合法凭据对系统或网络进行未经授权的访问。由于 API 往往依赖令牌进行授权，因此获得这些令牌的攻击者可以在不被发现的情况下访问敏感数据。

我们还发现了 T1566（网络钓鱼），其中攻击者发起了网络钓鱼活动，窃取了可用于未来攻击的 API 令牌或凭据。由于 API 扩大了攻击面，因此越来越多的攻击者开始利用它们实施入侵。此外，与 T1190（利用面向公众的应用程序）相关的告警揭示了攻击者使用应用程序缺陷来渗透网络。所观察到的另一种技术是 T1580（云基础架构发现），其中攻击者通过 API 调用探测暴露的云端点，以此利用 API 进行侦察。

虽然 MITRE 没有专门的 API 安全矩阵，但其框架对于希望了解针对 API 的攻击者技术的安全团队和企业来说仍然至关重要。通过将攻击者的策略与 API 的特定行为进行关联，安全团队可以确定攻击阶段及相关的策略、技术和程序，从而增强事件响应和威胁检测能力。此方法使防御者能够更有效地降低风险。

OWASP 告警

OWASP 十大 API 安全风险是一项重要资源，提供针对漏洞影响和严重性的具备可操作性的见解。它使开发人员和安全团队可以有效地确定各项计划的优先顺序，并通过更新来确保信息能够在不断快速演变的威胁形势下保持相关性。

在 30 天的样本期内，我们的分析发现，与 OWASP 相关的事件增加了 32%。值得注意的是，失效的对象属性级授权 (BOPLA)、失效的功能级授权和失效的身份验证等漏洞会将敏感数据或关键功能直接暴露给攻击者。授权机制不足使攻击者能够升级权限、接管帐户并访问机密信息，这使其成为针对 API 的最危险的攻击媒介之一。

失效的对象级授权 (BOLA) 仍然是一项严重的 API 安全漏洞，但由于它依赖于业务逻辑缺陷，因此难以进行检测。这通常会导致漏报或检测率低。为了解决此问题，企业应采用在用户与其通常访问的资源之间建立明确关系的 API 安全解决方案。这需要通过能够识别异常访问模式的先进机器学习算法来设置行为基准。

BOPLA 会利用 API 中细微的字段级访问问题，而这些问题在安全测试过程中经常会被忽视。与需要更改整个对象 ID 的 BOLA 不同，BOPLA 攻击以对象内的特定属性为目标。例如，在其响应中暴露敏感个人身份信息 (PII) 的 DELETE API 调用构成了一个 BOPLA 漏洞。这种细微之处使得 BOPLA 问题比 BOLA 攻击更为普遍。

一个实际的例子是，在仅使用电子邮件地址的取消订阅请求中，API 响应无意间包含了用户的全名和地址。这种将敏感数据暴露给未授权方的问题之所以会发生，是因为安全测试通常关注的是整个对象而不是单个属性。此疏忽会导致 API 安全评估中检测到的 BOPLA 漏洞增加。

另一个严重漏洞是不受限制的资源消耗，攻击者可以利用此漏洞来通过耗尽资源或类似于 DDoS 的攻击导致服务中断。此漏洞会带来服务影响之外的其他风险，包括由于过度使用云资源而导致运营成本增加以及暴力破解攻击风险增加。如果不进行适当的速率限制，攻击者便能够快速探测 API，进而可能危及安全。此外，这些攻击会产生大量流量，导致企业的成本大幅增加。

在第三方 API 集成过程中，由于验证不充分、数据过滤和缺乏安全机制而导致的不安全的 API 使用是另一个重要的威胁媒介。随着企业在数字化转型中越来越多地依赖第三方 API，这个问题越来越令人担忧。近期的一项研究表明，超过 80% 的受访企业遇到了与第三方 API 相关的问题，这凸显出采用 Zero Trust 安全模式的重要性。虽然此漏洞本身可能不会直接造成灾难性后果，但如果与验证不完善或不安全的依赖关系等其他薄弱环节相结合，它便会成为一个重大安全威胁。例如，金融 API 对未经验证的第三方交易的信任可能会导致安全漏洞。

与 PCI DSS 和 GDPR 相关的安全告警分别增加了 16% 和 21%，而与 ISO 27001 相关的告警增加了 22%。

确保 API 合规性

用于确保 API 合规性的最佳实践包括，为每个告警标记其违反的具体合规标准和监管标准、让企业直接了解关键的合规问题以及提供具备可操作性的指导来解决这些问题。这种主动方法可帮助企业保持法规合规性，从而降低风险，减少发生监管罚款、法律后果和声誉受损等会造成严重经济损失的情况。例如，在 API 漏洞导致 40 万客户的数据被暴露之后，一家航空公司面临 2000 万英镑的罚款，这凸显出在 GDPR 监管下 API 安全防护措施不足所带来的严重后果。

合规标准是企业保护敏感数据、保障客户安全以及履行法律和监管义务的重要保障。PCI DSS、GDPR 和《健康保险流通与责任法案》(HIPAA) 等法规和标准要求安全地处理支付数据和 PII 等敏感信息。我们的数据分析结果表明，与 PCI DSS 和 GDPR 相关的安全告警分别增加了 16% 和 21%，而与 ISO 27001 相关的告警增加了 22%。

GDPR

GDPR 强调在整个 API 生命周期内整合数据保护和客户隐私。这涉及安全设计、强大的身份验证和授权、速率限制、定期漏洞测试、加密和持续的风险评估，甚至在早期开发阶段也是如此。这些措施可确保数据的机密性、完整性和可用性。

PCI DSS

同样，PCI DSS 强调通过将安全防护融入设计、编码和测试阶段来保护用于处理支付卡数据的 API。它要求防范 Web 漏洞并进行定期测试，以识别和解决安全漏洞。

第 10 项和第 11 项要求特别要求对请求、响应、身份验证尝试及系统更改等 API 活动进行全面日志记录和监控。日志必须至少保留 12 个月，并且最近三个月的日志必须随时可供查阅分析。此外，它还建议企业在发生重大变更后执行外部漏洞扫描。为了确保 PCI 合规性，企业必须实施严格的控制措施，包括速率限制、日志记录、基于角色的访问控制 (RBAC) 以及会话管理，以确保 API 能够抵御威胁和风险。

ISO 27001

ISO 27001 标准提供了一个可靠的框架，用于有效地管理信息安全风险、增强企业安全态势以及在同行与客户之间建立信任。推荐的实践包括：

- 实施访问控制（例如，API 密钥）以验证用户身份
- 采用端到端数据加密
- 监控 API 是否存在异常行为
- 执行全面的风险评估，以识别潜在的 API 漏洞

这些合规要求突出了 API 安全与监管框架之间的关键交集。正确的实施不仅可以保护敏感数据，还能够同时满足多项合规要求。如需详细了解现有和新的全球标准，请跳转至本报告的合规性部分。

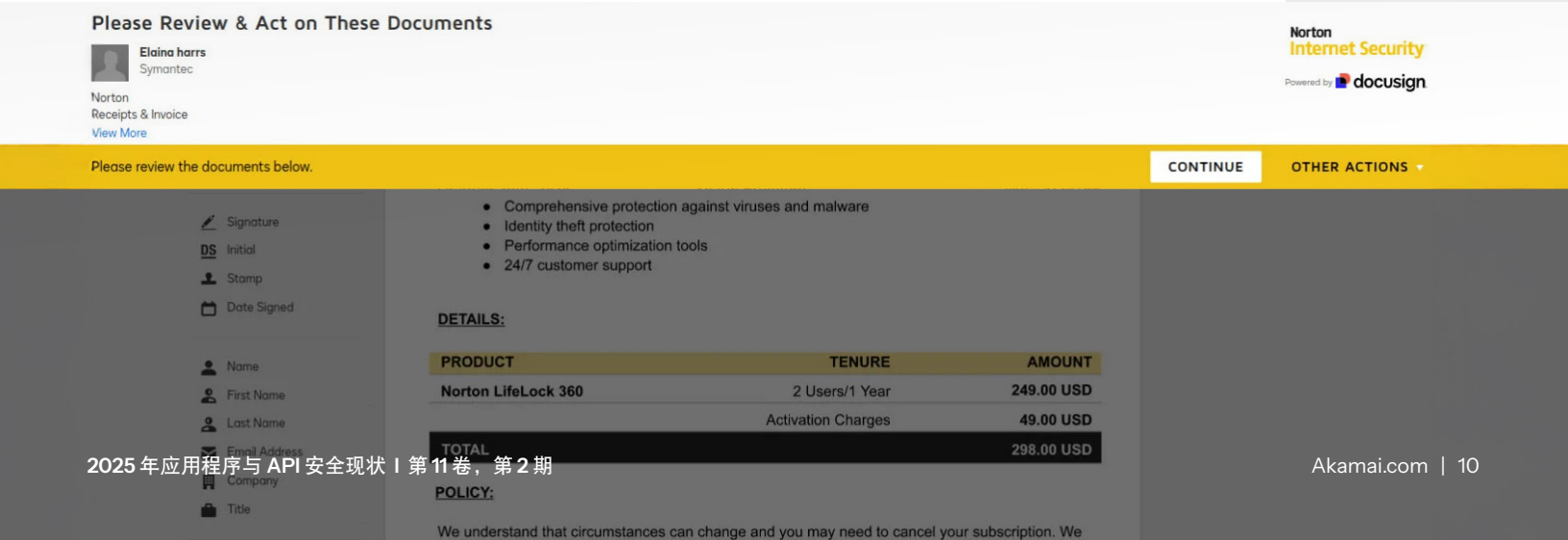
API 监测能力漏洞：隐藏的数据通道

API 滥用

2024 年 11 月，Bleeping Computer 报道了针对电子签名解决方案提供商的一次重大攻击。攻击者利用该提供商文档管理和跟踪 API 中的核心组件，向大量潜在受害者发送了欺诈性发票。如果收件人在不知情的情况下签署了这些文档，攻击者便可以向不同的企业索取付款。

此事件凸显出 API 滥用的恶劣影响——恶意攻击者可以利用 API 执行超出其预期设计用途的操作，并将它们转变为意料之外的攻击渠道。生成式 AI 的出现进一步加剧了这些风险，因为它可以自动完成漏洞发现和速率限制绕过，为更快速、更复杂的攻击提供了便利。

来源：bleepingcomputer/Wallarm



API 滥用检测中的挑战

安全团队在检测 API 滥用方面遇到了巨大障碍，主要是因为必须建立区分正常行为和可疑行为的基准。此挑战表明，迫切需要进行实时行为监控以抢先发现异常行为和威胁。

我们的《2024 年 API 安全影响研究》揭示了一个令人担忧的趋势：只有 13% 的受访企业会每天对其 API 进行测试，相比 2023 年的 37% 有明显下降。鉴于当前的威胁形势，这种大幅下降尤为令人担忧。每日 API 测试的急剧减少会使企业面临更高的安全风险，因为它显著降低了企业检测和应对快速变化的威胁的能力，进而可能导致严重漏洞在很长一段时间内得不到解决。

在开发周期内进行频繁的自动化测试让企业能够尽早发现并解决问题，从而避免在生产环境中进行成本高昂的补救操作。在 API 漏洞利用越来越多地采用自动化和隐蔽方法的时代，主动测试在降低风险方面发挥着至关重要的作用。

不受管 API：僵尸 API 和影子 API

API 资产监测能力对于企业来说仍然是一项严峻挑战，它包括官方 API 跟踪和敏感数据识别。《2024 年 API 安全影响研究》揭示了一项巨大差距：尽管 47% 的应用程序安全团队拥有完整的 API 清单，但未能确定用于处理敏感数据的 API。资深安全专业人士也反映了类似的不足，其中 42% 的人面临着这种疏忽问题。令人担忧的是，拥有完整 API 清单并了解敏感数据暴露的企业，其数量占比已从 2023 年的 40% 下降到 2024 年的 27%。该安全影响研究还强调，僵尸 API 和影子 API 是导致 API 安全事件的主要原因之一。

不完整的清单主要遗漏了僵尸 API 和影子 API。僵尸 API（即，由于未完全停用、人员流动或其他原因而仍然处于活动状态的过时接口）会产生易受攻击的攻击媒介。影子 API（那些在标准审批流程之外作为快速解决方案开发的 API）也会带来类似的威胁。研究表明，三分之一的恶意 API 交易都以影子 API 为目标。

事实证明，Web 应用程序防火墙 (WAF) 等传统的安全措施不足以抵御这些威胁。企业需要先进的 API 发现和监控解决方案来有效识别易受攻击的端点。

全面的 API 清单构成了有效安全策略的基石，使企业能够监控使用模式、跟踪版本历史记录、识别漏洞以及满足合规和监管要求。此战略性方法可以让企业清楚地了解其数字基础架构，最终加强风险管理并增强整体安全态势。

安全现状聚焦

2025 年第一季度，我们发现了一起通过 API 滥用对某家电子商务公司发起的攻击。该公司发送短信的 API 缺少适当的身份验证，攻击者可以使用超过 200 个不同的 IP 地址、一个身份验证令牌和大量随机手机号码（合法和虚假号码）来利用它。

攻击策略简单但有效：通过注册多个手机号码并向欺诈性号码发送短信来使该公司不堪重负，从而直接造成经济损失。受影响的公司需要支付短信网关服务费用才能在其应用程序与移动服务之间进行短信传递，因此当攻击者注册手机号码时，该公司便会产生意外的财务费用，这些费用可能会损害该公司的品牌或声誉。采用多层安全措施的纵深防御策略可以应对此类攻击并显著降低相关的风险。

我们的告警显示，攻击者在此次攻击中发起了 11,057 次 POST 请求，其中有 5,659 次成功获得了响应（图 2）。

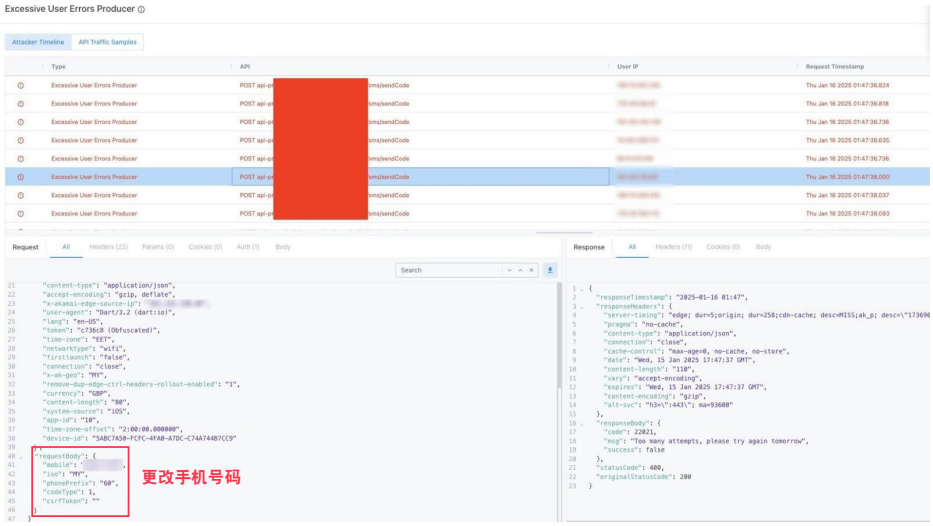


图 2：攻击者利用请求对不安全的 API 进行泛洪攻击

这些自动请求几乎完全相同，只有一个关键参数不同：

正文参数 **mobile**：检测到以下模式 - **<number>**

此类请求会使服务器过载并导致拒绝服务，或者它们可以指示对 API 成功进行未经授权的访问。传统 WAF 缺少检测这些复杂攻击的能力。但是，为正常 API 行为创建基准的先进 API 安全解决方案可以通过行为分析来识别此类攻击、主动降低风险并防止攻击者造成更严重的损失。

Web 攻击：同比比较和趋势

Akamai 的研究表明，在 2023 年 1 月到 2024 年 12 月的报告期内，以 Web 应用程序和 API 为目标的 Web 攻击大幅增加（图 3）。月度攻击量从 2023 年初的接近 140 亿次增加到 2024 年 10 月的超过 290 亿次。这表明，从 2023 年第一季度到 2024 年第四季度，Web 攻击增加了 65%。

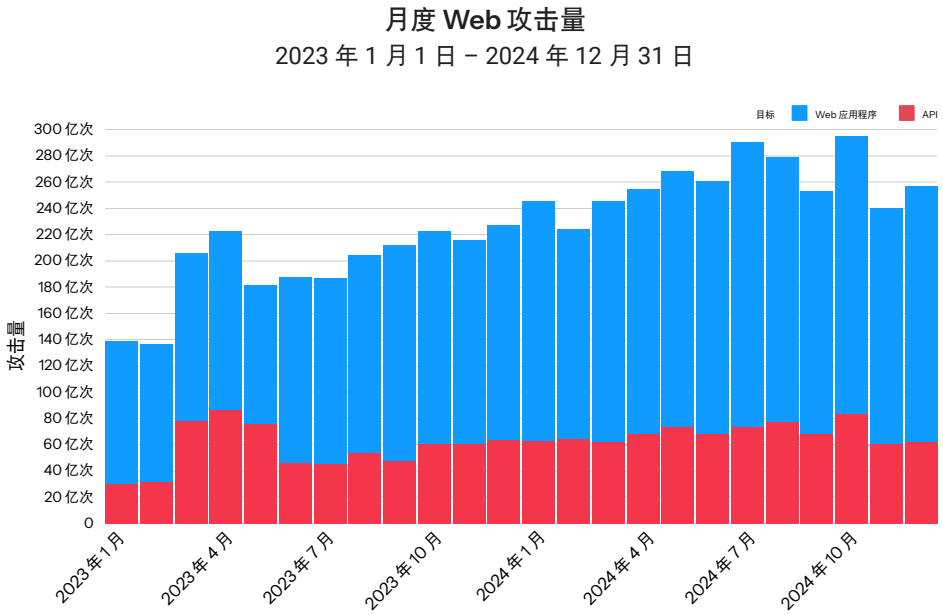


图 3：以 Web 应用程序和 API 为目标的传统 Web 攻击继续增加，2023 年第一季度到 2024 年第四季度期间增加了 65%

主要媒介：融合了传统和现代的基于行为的风险

在保护其企业的数字基础架构免受各种威胁（包括传统 Web 攻击以及针对固有漏洞和错误配置的现代攻击）的侵扰时，网络安全专业人员面临着复杂性不断升级的问题。

API 请求限制违反：日益严重的威胁

一项为期两年的 API 端点综合分析表明，API 请求限制违反是各企业关注的一个领域（图 4）。在请求或响应不符合预定义参数或既定要求（例如，超过速率限制或提交了无效的数据输入）时，便会出现这些违反行为。

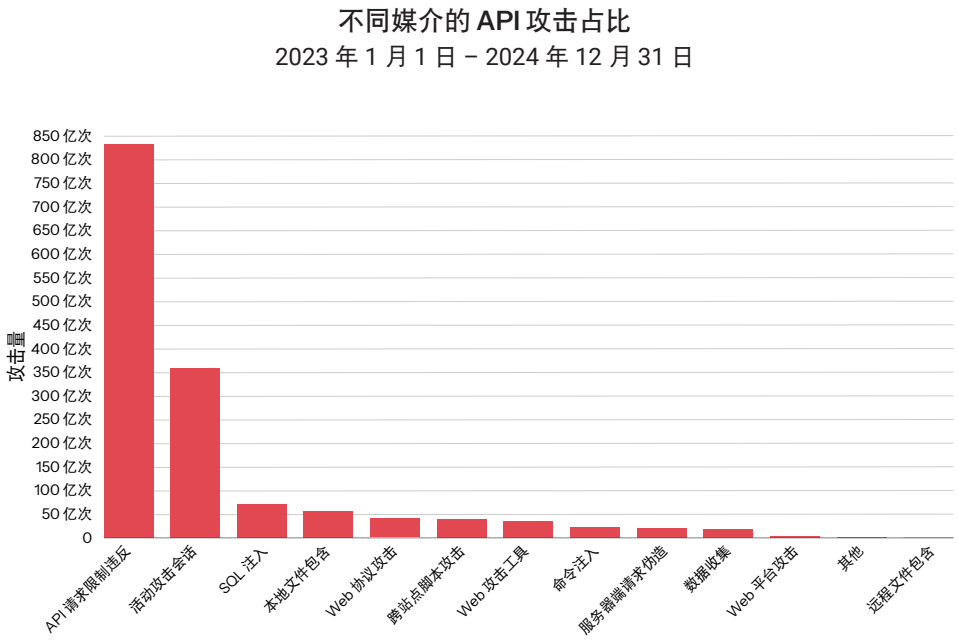


图 4：过去两年内记录了超过 830 亿次请求限制违反

API 请求限制违反是一项日益严重的威胁，过去两年内记录了超过 830 亿次攻击。从 2023 年到 2024 年，此攻击媒介猛增 24%，这凸显出 API 滥用的危险性。这些违反行为的泛滥可作为潜在 API 滥用的一项关键指标，它可能会引发一连串的负面影响，包括系统性能降级、服务中断以及更容易遭受有针对性的攻击。

活动攻击会话：需要富有创造性的解决方案予以应对的独特攻击

Akamai 的解决方案采用了创新的安全工具来应对 API 特定攻击所带来的独特挑战。这些解决方案的核心是一项用于检测活动攻击会话的专有机制，它可用作战略性防御工具。此系统使用 Akamai 自己的威胁情报来识别和跟踪可疑行为，让企业能够主动阻止威胁，防止它们升级为全面攻击。

此系统会对攻击者进行标记并实施“受罚区”方法。就现代攻击而言，攻击者主要使用自动化来执行其侦察和攻击活动。Akamai 可以快速识别这些漏洞扫描会话，通过暂时屏蔽客户端来做出反应，并将这些会话标记为活动攻击会话。此策略可有效阻止潜在攻击者进行侦察和利用网络漏洞。

通过限制恶意攻击者的机会窗口，企业可以大幅增强其 API 安全态势。此方法可以针对各种潜在攻击提供强大的防护能力，并显著提高整体网络安全弹性。

我们的数据充分表明了此策略的重要性。就整体排名而言，活动攻击会话在 Web 应用程序和 API 中高居首位（图 5）。2023 年，它造成了超过 690 亿次攻击。2024 年，该数字飙升至超过 1130 亿次攻击，同比大幅增加 63%。

按媒介划分的 Web 攻击量

2023 年 1 月 1 日 – 2024 年 12 月 31 日

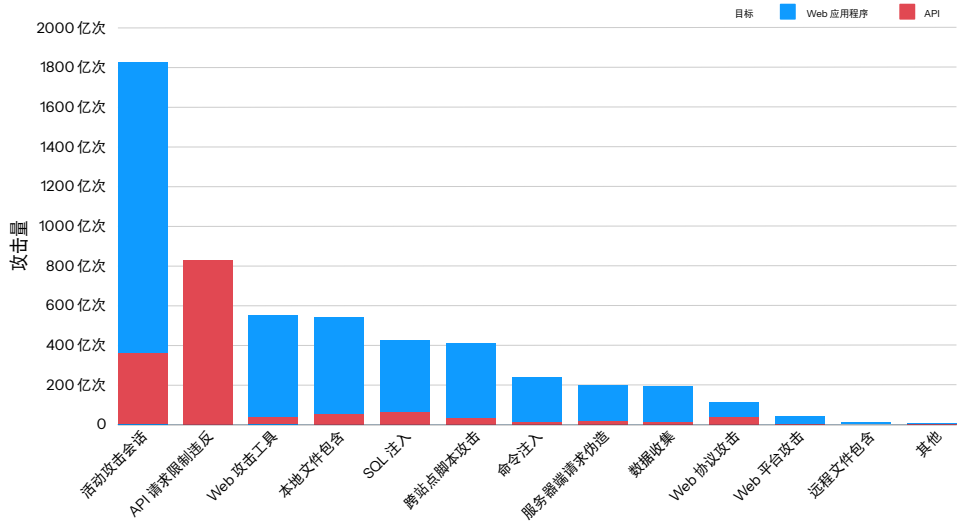


图 5：对于 Web 应用程序和 API 来说，活动攻击会话造成的攻击量远超所有其他攻击媒介，这凸显出攻击者会在预定目标的网络中无休止地寻找漏洞

我们为何不能忽视现代基础架构中的传统 Web 漏洞

尽管出现了基于行为的复杂攻击方法，并且人们对传统 Web 漏洞的认识有所提高，但注入攻击仍然展现出很高的有效性。我们从 2023 年 1 月到 2024 年 12 月的数据表明，攻击量出现大幅激增，其中结构化查询语言注入 (SQLi) 和命令注入分别同比增长 60% 和 34%。这些漏洞使恶意攻击者能够执行未经授权的命令、破坏系统完整性并在未进行适当身份验证的情况下访问敏感数据，凸显出它们在网络安全领域的持续相关性。

SQL 数据库凭借其在数据存储方面的可靠性和可扩展性而闻名于世，因此长期以来一直被广泛采用，这也导致这些系统成为持续攻击的目标。值得注意的是，四大广泛使用的数据库都采用基于 SQL 的架构，这进一步强调了此攻击媒介的关键性。

虽然 OWASP 十大 API 安全风险清单经过了多次修订（例如，在其 2023 年的更新中将注入攻击替换为安全错误配置），但与注入攻击相关的风险仍然至关重要。与此同时，本地文件包含 (LFI) 和跨站点脚本攻击 (XSS) 等其他既有媒介也会继续大量出现。根据 2024 年观察到的真实攻击，我们的 2025 防御者指南阐明了 XSS 攻击利用技术的复杂性，包括远程资源注入、cookie 窃取、网站涂改和会话劫持。

这些发现结果凸显出实施多层防御策略的迫切性。网络安全专业人员必须将适当的输出编码、强大的内容安全策略以及先进的 WAF 相结合，才能有效地应对这些日益复杂的攻击。

第 7 层 DDoS 攻击：同比比较和趋势

从 2023 年 1 月到 2024 年 12 月，Akamai 的研究记录表明，针对 Web 应用程序和 API 的第 7 层（应用层）DDoS 攻击量急剧增加（图 6）。月度攻击量从 2023 年初的略高于 5000 亿次猛增到 2024 年 12 月的超过 1.1 万亿次。这表明，从 2023 年第一季度到 2024 年第四季度，第 7 层 DDoS 攻击增加了 94%。

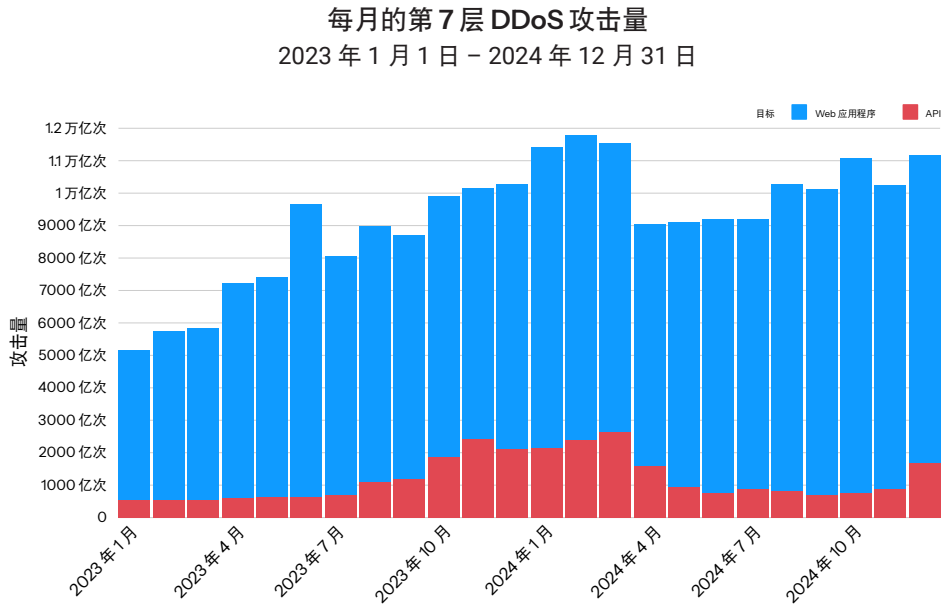


图 6：以 Web 应用程序和 API 为目标的第 7 层 DDoS 攻击量继续增加，2023 年第一季度到 2024 年第四季度期间增加了 94%

针对应用程序和 API 的第 7 层 DDoS 攻击

在以 Web 应用程序和 API 端点为目标的第 7 层 DDoS 攻击不断发展变化的过程中，HTTP 泛洪攻击始终是主要的威胁媒介。这些攻击会使用大量看似合法并专注于执行资源密集型操作的请求来淹没 API 资源，从而使它们不堪重负。攻击者改进了他们的技术，精心设计了第 7 层 DDoS 攻击来利用 Web 应用程序逻辑或 API 中的特定漏洞，这使得检测和抵御工作的变得更加复杂。此外，爬虫程序攻击也变得日益复杂，它们产生的流量模式能够逼真地模仿合法的 API 用途。

攻击者的 AI 变速箱：通过手动或自动方式在 API 道路上畅行无阻

生成式 AI 技术通过 API 彻底改变了业务集成，这“推动”了 API 的广泛采用和实际应用。AI API 市场正呈现爆发式增长，预计将从 2025 年的 444.1 亿美元增长至 2030 年的 1791.4 亿美元，年复合增长率高达 32.2%。但是，在 AI 采用出现激增的同时，针对 API 的 AI 驱动型攻击也大幅增加。已暴露的 API 漏洞的增加在很大程度上可以归因于攻击者通过手动或自动方式利用 AI 作为进行侦察和利用漏洞的工具。

AI 赋能的 API 攻击策略

- 战略定位：攻击者利用 AI 工具来识别和分析目标 API 中的特定组件，并针对特定漏洞利用 AI 生成的恶意代码来精心设计定制攻击。此方法可以针对 API 薄弱环节实现精准且有效的攻击。
- 自动攻击：通过实现攻击流程的自动化，网络犯罪分子可以显著减少其投入的时间和精力，同时快速确定并利用 API 安全方面的薄弱环节。这种自动化通常涉及 AI 赋能的爬虫程序，这些爬虫程序对企业和个人都构成重大威胁。
- 容量耗尽型攻击：攻击者会将 AI 作为攻击手段向 API 发送大量流量，以利用巨大的流量和速度淹没安全系统。自动 DDoS 攻击正是这种策略的典型例证，在此策略下 AI 赋能的爬虫程序会发起持续攻击，同时能够动态地适应防御措施。
- 基于行为的攻击：AI 会分析流量模式，能够发起运行在典型告警阈值之下的低速缓慢攻击，从而规避检测。这些攻击通常以常见的 API 漏洞（例如 BOLA 和失效的身份验证）为目标。

AI 赋能的 API 的讽刺之处

矛盾的是，AI 赋能的 API 已被证明非常不安全。大多数 AI 赋能的 API 可以从外部进行访问，其中很大一部分依赖于不完善的身份验证机制，这导致它们更容易受到攻击。我们的《2024 年 API 安全影响研究》显示，生成式 AI 工具中的 API 是引发零售/电子商务安全团队所报告的 API 事件的主要原因。

不断演变的 AI 威胁形势

AI 技术的进步极大地促进了 API 威胁形势的不断演变。据报道，去年 AI 驱动的 API 漏洞数量创下了历史新高，并且有消息称，在由美国网络安全和基础架构安全局记录在案的所有遭到利用的漏洞中，大多数都与 API 相关，而这种情况首次出现。

AI 赋能的 Web 应用程序攻击和防御策略

通过引入新的攻击媒介和防御能力，AI 对 Web 应用程序安全也产生了深远影响。AI 在一些关键领域中显著改变了针对 Web 应用程序攻击的网络安全形势，包括 AI 增强的恶意软件、AI 赋能的漏洞扫描、针对包含 AI 功能的系统的攻击、先进的网络内容抓取和 AI 赋能的 WAF 系统。

AI 增强的恶意软件

网络安全专家已观察到利用 AI 来攻击 Web 应用程序的先进恶意软件。在 2024 年针对法国用户的电子邮件攻击活动中，攻击者部署了可能在生成式 AI 帮助下设计的恶意代码，以执行 AsyncRAT 恶意软件。此示例凸显出 AI 辅助的恶意软件创建和部署呈现日益增长的趋势，这给 Web 应用程序安全专业人员带来了新的挑战。

AI 赋能的漏洞扫描

AI 彻底改变了针对 Web 应用程序的漏洞扫描，并提供了强大的防御和攻击能力，可用于有益用途，也可以用于恶意用途。现在，这些 AI 驱动的工具能够自动搜索常见的漏洞，例如 SQLi、XSS、跨站点请求伪造以及服务器端请求伪造 (SSRF)。此外，它们会对潜在的影响进行 AI 驱动的分析，并针对补救措施生成 AI 赋能的建议。

针对包含 AI 功能的系统的攻击

在 Web 应用程序中集成 AI（尤其是大语言模型 (LLM)）带来了新的安全漏洞。*提示注入攻击*以 AI 系统为目标，其目的是覆盖模型的安全措施。现已修补的 Slack AI 漏洞便是一个值得关注的例子，该漏洞允许通过间接提示注入从私人渠道收集数据。*数据中毒攻击*会通过操纵一小部分数据集来破坏 AI 模型行为，从而可能导致系统完整性受损。*越狱技术*可以绕过 LLM 的安全措施，让攻击者能够覆盖限制、提取敏感数据以及生成有害输出。这些新兴攻击媒介需要企业提高警惕并制定新的防御策略。

先进的网络内容抓取

AI 增强了网络内容抓取功能，这给 Web 应用程序安全带来了新的挑战。这些 AI 赋能的抓取工具现在提供更高效的数据提取方法，并且能够更好地规避反抓取措施。自 2020 年代初以来，先进的网络内容抓取功能便一直在利用 AI 来处理数据，但最近 LLM 抓取的频率显著增加。这主要是因为基于代理的查询兴起，它推动了对实时（非静态）数据源的需求增长。

遗憾的是，这导致 Web 应用程序请求的平均成本（取决于请求复杂程度、托管基础架构等因素）在每次请求 0.01 美元到 0.50 美元不等。虽然商业最初是受 LLM 抓取增加影响最大的行业，但形势已发生变化——其他行业（例如，金融服务、博彩、数字媒体和视频媒体）现在正在经受此转变的冲击。

AI 赋能的 WAF 系统

好的一面是，先进的 WAF 系统也得到了 AI 技术的支持，能够更有效地识别和抵御各种网络威胁，包括爬虫程序、DDoS 攻击、内容抓取程序和扫描器。AI 赋能的 WAF 系统有助于应对复杂的网络攻击，因为具有静态规则集的传统 WAF 难以抵御零日威胁并需要手动更新。

多层机器学习策略可实现模式识别、自适应学习、异常检测并缩短响应时间。通过使用数十亿的日常事件进行训练并实施具备持续监控功能的分层方法，AI 赋能的 WAF 系统能够主动防范不断变化的威胁并始终保护客户安全。

行业趋势

从 2023 年第一季度到 2024 年第四季度，商业在所有行业中遭受的 Web 攻击最多，其攻击总量几乎为高科技行业（遭受攻击第二多的行业）的三倍（图 7）。此外，同一时期内商业行业遭受的 API 攻击量也远远超过了其余 10 大行业的 API 攻击总数。

按行业划分的 Web 攻击量

2023 年 1 月 1 日 – 2024 年 12 月 31 日

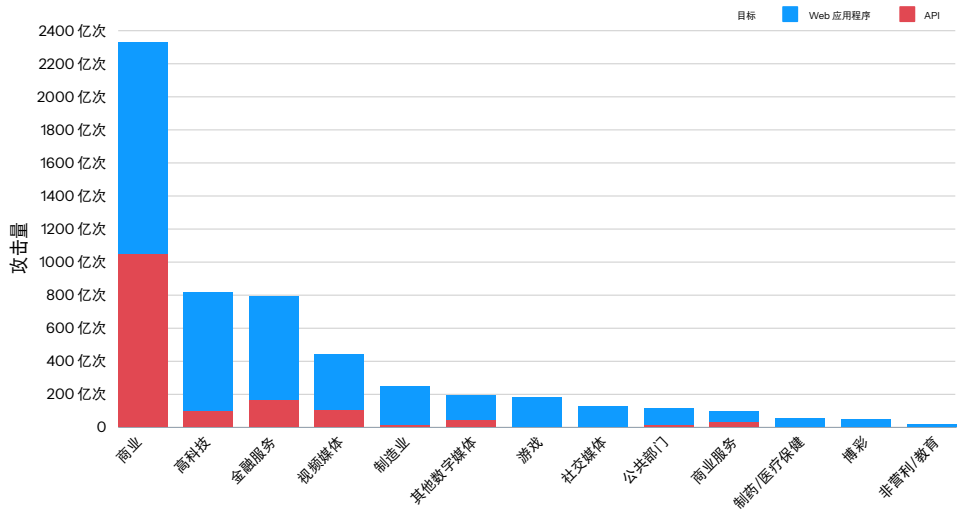


图 7：商业、高科技和金融服务是遭受 Web 攻击最多的三大行业

总体来看，在第 7 层（应用层）DDoS 攻击方面，高科技行业遭受的攻击比任何其他行业都多，2023 年第一季度到 2024 年第四季度期间该行业遭受的攻击超过 7 万亿次。排在高科技之后的是社交媒体和商业（图 8）。但是，在同一时间段内，商业行业遭受的针对 API 的第 7 层 DDoS 攻击量再一次大幅超过了所有其他行业的总和。

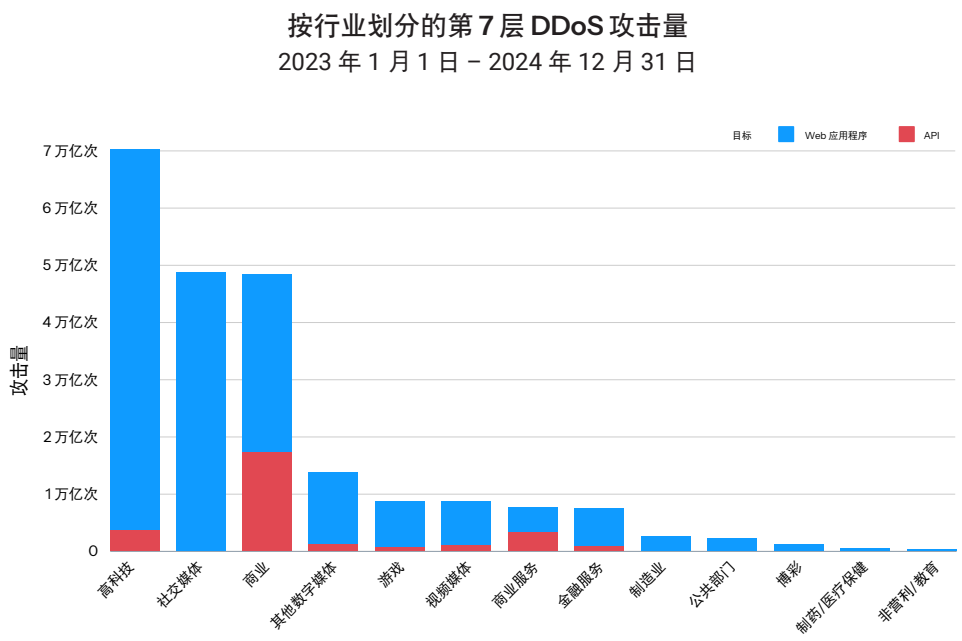


图 8：按行业划分的第 7 层 DDoS 攻击量

商业

从 2023 年到 2024 年，除了遭受超过 2300 亿次 Web 攻击（占所有 Web 攻击量的 40% 以上）之外，商业行业还经历了规模空前的第 7 层 DDoS 攻击。Akamai 的数据显示，2023 年到 2024 年期间该行业遭受的此类攻击超过 4.8 万亿次。

这个总攻击量代表了一种战略定位模式，其中 Web 应用程序承受了大约 64.25% 的攻击，而 API 占剩余的 35.75%。此分布反映出攻击者利用两种媒介来入侵商业平台，并凸显了现代威胁形势的多面性。

商业实体是利润尤为丰厚的目标，因为它们集中了敏感的客户数据、付款信息和金融交易。窃取的付款凭据、遭到入侵的客户账户和敏感的 PII 所带来的直接变现途径能够为攻击者带来直接的经济奖励。与遭到泄露的数据需要其他步骤才能转化为经济利益的部分行业不同，商业平台往往为攻击者提供了可直接利用的资产。

零售业是主要目标

在更广泛的商业行业中，零售业是遭受攻击最为严重的细分行业。由于其自身的一些独有特性，它面临的攻击量格外庞大。

零售业务通常需要维护复杂的数字生态系统，包括各种平台和系统。它们积极的数字化转型计划往往优先考虑上市速度，而不是全面的安全防护，这便带来了安全漏洞。全渠道策略的采用无意中增加了攻击面的复杂性。此外，对第三方供应商的广泛依赖也导致形成了一个包含众多潜在风险点的复杂供应链。

美国联邦调查局互联网犯罪投诉中心称，季节性流量模式会形成可预测的高流量时段，攻击者会专门针对这些时段发起攻击，其中冬季假日期间的网络犯罪事件会激增 25% 到 30%。电子商务平台也面临着更大的威胁，12 月份遭受的网络攻击量比全年平均值增加了 31%。

Web 应用程序攻击的演变

在技术进步和攻击者方法不断变化的推动下，Web 应用程序攻击正在经历重大转变。攻击者使用日益复杂的技术来利用 Web 应用程序中的漏洞，并调整其策略以规避不断发展变化的安全措施。自动攻击工具的兴起以及与机器学习算法的结合，让攻击者能够对零售商的 Web 应用程序发起更精准且更具针对性的攻击活动。

此外，向微服务架构和 API 驱动型开发的转变也扩大了攻击面，因此有必要重新评估传统的安全模式。这种演变要求网络安全专业人员采取主动方法，强调了持续监控、自适应防御机制以及对 Web 应用程序环境中新兴攻击媒介的深入了解的重要性。

爬虫程序威胁形势

随着技术进步，爬虫程序威胁形势也在快速变化，尤其是攻击者整合了生成式 AI 功能。这种演变通过更快的零日漏洞利用和绕过传统防御措施的复杂规避技术改进了攻击策略。有证据表明，针对零售商的基于 AI 的爬虫程序欺诈攻击在 2022 年 8 月到 2024 年 4 月期间持续增加，其中 2024 年 1 月飙升了 137%。检测挑战进一步加剧了这些威胁，企业通常需要花费四个月时间才能识别出爬虫程序攻击，同时在此期间不得不承受经济和声誉损失。

现在，爬虫程序已成为零售网络环境中的核心媒介，为实现帐户接管、信用卡欺诈和礼品卡滥用提供了便利。它们利用从某个遭到入侵的网站窃取的数据来助长针对其他网站的撞库攻击，从而成为更广泛的攻击活动的推动因素，这在所有零售生态系统中产生了复合效应。此活动促进了网络欺诈的“工业化”，并且全球犯罪团伙利用自动化工具来扩大行动规模，这远远超出了手动方法所能达到的效果。

如需获取相关建议来更好地保护零售业务 Web 应用程序和 API 免受与 AI 及爬虫程序相关的攻击，请跳转到抵御措施部分。

金融服务

金融服务业已成为 Web 攻击的主要目标，并且持续遭受第 7 层 DDoS 攻击。2023 年 1 月到 2024 年 12 月期间，该行业遭受的 Web 攻击总数超过 790 亿次。而同一时间段内，针对 Web 应用程序和 API 的第 7 层 DDoS 攻击总数超过了 7610 亿次。

这一前所未有的攻击量表明，金融服务业是攻击的重灾区并对攻击者有着莫大的吸引力。有多个因素推动了此次激增，包括该行业在全球经济基础设施中的关键作用、金融数据的高价值以及造成巨大破坏的可能性。

金融服务的数字化

金融服务的数字化扩大了网络犯罪分子的攻击面。AI 驱动的个性化、银行即服务和嵌入式金融解决方案的采用带来了新的漏洞。地缘政治冲突（尤其是俄乌战争）助长了针对金融机构的黑客活动。经济因素（包括加密货币的兴起以及加密货币储备的潜在实施）提高了攻击者对金融行业的兴趣。

Web 应用程序攻击正在发生快速转变，在适应新技术的同时也在利用新出现的漏洞。现在，攻击者会利用先进的 AI 和机器学习算法来绕过传统的安全措施并发起更具针对性、更持久的攻击。无服务器架构和微服务的兴起产生了新的攻击媒介，而 API 的日益普及也为恶意攻击者增加了更多潜在的入口点。此外，向移动应用程序和基于云的应用程序的转变要求对安全策略进行重新评估，因为这些平台在数据保护和访问控制方面带来了独特的挑战。

银行业成为主要攻击目标

在金融服务行业内，银行业是遭受 Web 攻击最多的细分行业（图 9）。与商业行业一样，撞库攻击也正在成为银行业的主要威胁媒介。

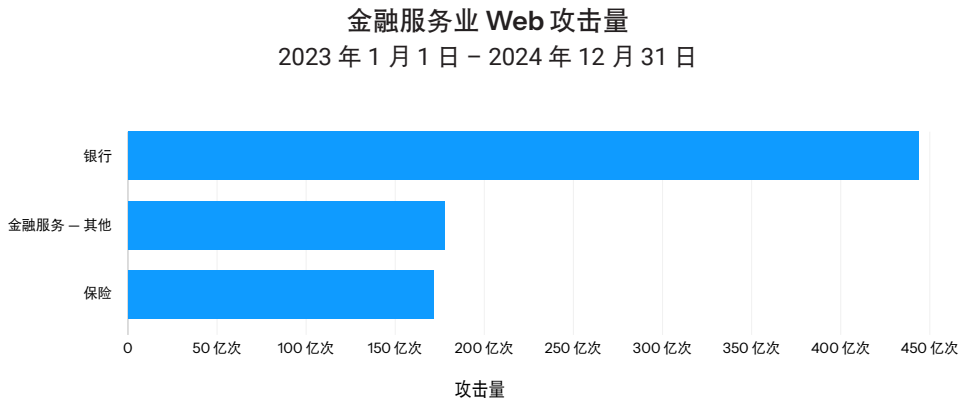


图 9：银行业是金融服务业中遭受 Web 攻击最多的细分行业

网上银行服务的普及及其账户访问权限的重要性相结合，使得该领域成为网络犯罪分子觊觎的目标。成功实施攻击带来的经济奖励非常可观，即使是少量遭到入侵的账户也可能产生巨大收益。银行业不愿意实施可能会给用户带来不便的严格安全措施（例如多重身份验证），这反而无意中导致其更容易受到攻击。

有几个因素进一步加剧了银行业成为主要攻击目标的情形。对停机时间的敏感性让勒索有了可乘之机，因为攻击者会利用人们对服务中断的担忧。此外，攻击手段（包括使用 AI 和机器学习来规避检测）变得日益复杂，这给传统防御机制带来了重大挑战。监管环境，包括严格的合规要求和安全漏洞可能带来的罚款，使银行业面临的网络安全挑战变得更加复杂。

高科技

高科技仍然是 Web 攻击和第 7 层 DDoS 攻击的主要目标行业。在我们的报告中，高科技行业包括电信、企业软件和硬件以及消费者软件和硬件等细分行业。我们的数据显示，此行业在 2023 到 2024 年期间遭受的 Web 攻击总数超过了 817 亿次，位居商业行业之后。另外，高科技也是遭受第 7 层 DDoS 攻击最多的行业：两年内遭受的攻击量超过 7 万亿次。

高科技行业的 Web 应用程序经常会采用复杂的数据库查询和动态内容，这会产生一些漏洞，攻击者可以利用这些漏洞轻松地使服务器不堪重负。这些漏洞导致该行业遭受高频率的第 7 层 DDoS 攻击。值得注意的是，尽管区块链采用去中心化架构，但区块链网络遭受的 DDoS 攻击显著增加，攻击者会使用 HTTP 泛洪攻击和垃圾交易等方法来阻碍合法交易。在高科技行业中，运营中断会造成严重的经济影响，这促使攻击者部署能够使基本服务瘫痪的 DDoS 攻击。现代软件开发对以 API 为中心的架构的依赖带来了额外的风险，因为攻击者经常在 HTTP 泛洪攻击中利用未安全编码的端点。

电信业面临类似的挑战

遭受大量 API 攻击的电信业面临着类似的网络安全挑战。在此高科技细分行业中，Web 应用程序和 API 威胁包括数据泄露、DDoS 攻击和供应链漏洞。这些漏洞已导致发生多起备受瞩目的数据泄露事件。

例如，2025 年 1 月，研究人员在一个主要电信网络中发现了严重的 API 漏洞，导致 3,000 家公司面临安全风险。相关调查发现了重大安全漏洞，包括“了解您的客户”验证流程中的薄弱环节，以及授予内部系统访问权限的后端 API 路径遍历漏洞。

物联网带来了新的攻击媒介

在技术飞速发展的时代，高科技行业仍在努力应对不断演变的 Web 应用程序和 API 漏洞。这种发展变化包括物联网 (IoT) 设备的广泛采用，但由于很多设备都缺少强有力的安全措施，因此带来了新的攻击媒介。多云基础架构的加速采用往往会导致环境配置不当，从而产生潜在的攻击入口点。

以不安全方式生产的物联网设备以及构建的云系统中的漏洞越来越容易成为 AI 驱动的复杂攻击的目标。SaaS 平台面临更高的 API 攻击风险，因为它们有广泛的攻击面。AI 解决方案的激增以及对第三方 SaaS 平台的依赖增加，显著扩大了高科技行业中的整体 API 攻击面。随着企业继续采用这些技术，被利用的可能性也在增加，因此需要采取强有力的安全措施和严密监控。

区域级趋势

注意：为了使读者能够更轻松地获取数据并方便突出北美（N. America）、亚太地区及日本（APJ）、欧洲、中东和非洲（EMEA）以及拉丁美洲（LATAM）等各地区的攻击趋势，我们更改了地区报告的格式。我们还提供了一张一览表，以方便快速查看本节中讨论的数据（图 10）。

Web 攻击数据　第 7 层 DDoS 攻击数据

地区	Web 攻击量	第 7 层 DDoS 攻击量	主要的 Web 攻击媒介	遭受攻击最多的区域	遭受攻击最多的行业
亚太地区及日本	800 亿次，14% API	7.4 万亿次，6% API	活动攻击会话、LFI、XSS	澳大利亚（203 亿次）、印度（173 亿次）、新加坡（159 亿次）	金融服务、商业、社交媒体
				新加坡（4.7 万亿次）、印度（6070 亿次）、韩国（2830 亿次）	社交媒体、其他数字媒体、商业
欧洲、中东和非洲地区	1160 亿次，37% API	2.6 万亿次，20% API	活动攻击会话、API 请求限制违反、LFI	英国（303 亿次）、荷兰（195 亿次）西班牙（142 亿次）德国（128 亿次）	商业、视频媒体、金融服务
				德国（5690 亿次）、英国（5060 亿次）	商业、其他数字媒体、视频媒体
拉丁美洲	30 亿次，12% API	2580 亿次，18% API	活动攻击会话、WAT、SSRF	巴西（193 亿次）、墨西哥（20 亿次）	商业、金融服务
				巴西（1750 亿次）、墨西哥（390 亿次）	商业、金融服务
北美	3270 亿次，29% API	11.9 万亿次，16% API			

图 10：地区一览，2023 年 1 月至 2024 年 12 月（LFI 表示本地文件包含；XSS，跨站点脚本攻击；WAT，Web 攻击工具；SSRF，服务器端请求伪造）

两种应用程序和 API 攻击趋势

我们分析了 24 个月报告期（从 2023 年 1 月到 2024 年 12 月）内 Web 应用程序和 API 攻击及第 7 层 DDoS 攻击的地区比较，发现了两种主要趋势（图 11）。

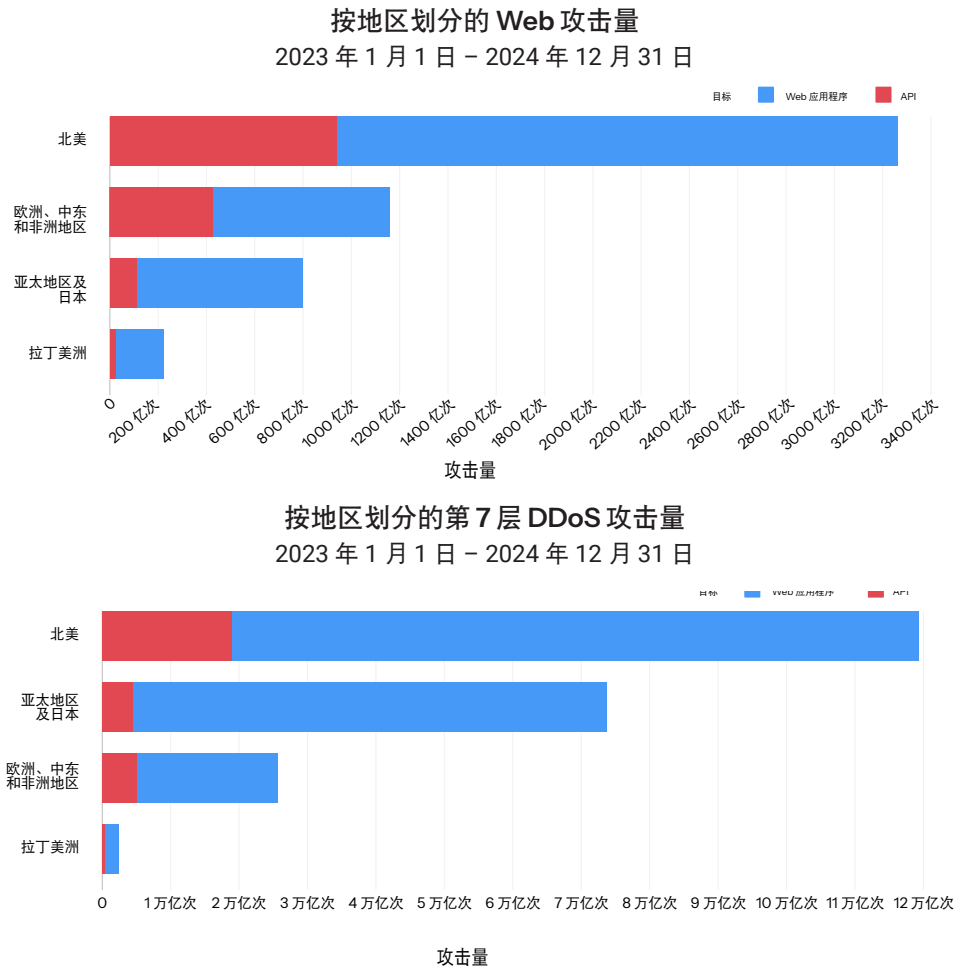


图 11：在报告期内，从全球范围来看，EMEA 地区遭受的 API 攻击量占比最高，而 APJ 地区遭受的第 7 层 DDoS 攻击总数排名第二

攻击趋势 1： API 攻击在 EMEA 地区十分普遍，可能的原因在于该地区的 API 采用率高于其他地区，以及开放银行业务和 PCI DSS v 4.0 促进了 API 的使用并且可能会带来安全风险。（有关 API 特定风险的详细讨论，请参阅不断改进我们的 API 威胁情报部分。）

EMEA 地区延续了我们首次在 2023 年观察到的趋势，这 24 个月内遭受的针对 API 的 Web 攻击最为密集：在该地区遭受的总计 1160 亿次 Web 攻击中，有 37% 以 API 为目标。相比之下，北美地区记录了总计 3270 亿次 Web 攻击，其中 29% 针对 API。在 APJ 地区，800 亿次 Web 攻击中有 14% 以 API 为目标，而 LATAM 地区紧随其后，30 亿次 Web 攻击中有 12% 以 API 为目标。

此外，EMEA 地区遭受的针对 API 的第 7 层 DDoS 攻击也最为密集 (20%)，其次是 LATAM 地区 (18%)、北美地区 (16%) 和 APJ 地区 (6%)。总体来看，针对 API 的第 7 层 DDoS 攻击尝试占每个地区 Web 攻击总数的比例相对较小。我们预计，随着时间推移，这些占比会由于各种原因（包括更先进的爬虫程序驱动的攻击和针对 API 漏洞的 AI 驱动型攻击的激增）而上升。

攻击趋势 2：在全球范围内，APJ 地区遭受的第 7 层 DDoS 攻击量排名第二，达到了 7.4 万亿次（北美地区遭受的此类攻击量为 11.9 万亿次）。随后是 EMEA 地区（2.6 万亿次）和 LATAM 地区（2580 亿次）。此趋势最初是在我们的 SOTI 报告《数字堡垒受到围攻》中观察到的，并且我们仍然认为这是由于 APJ 地区针对社交媒体的密集攻击尝试所致。

深入了解 APJ、EMEA 和 LATAM 地区的趋势

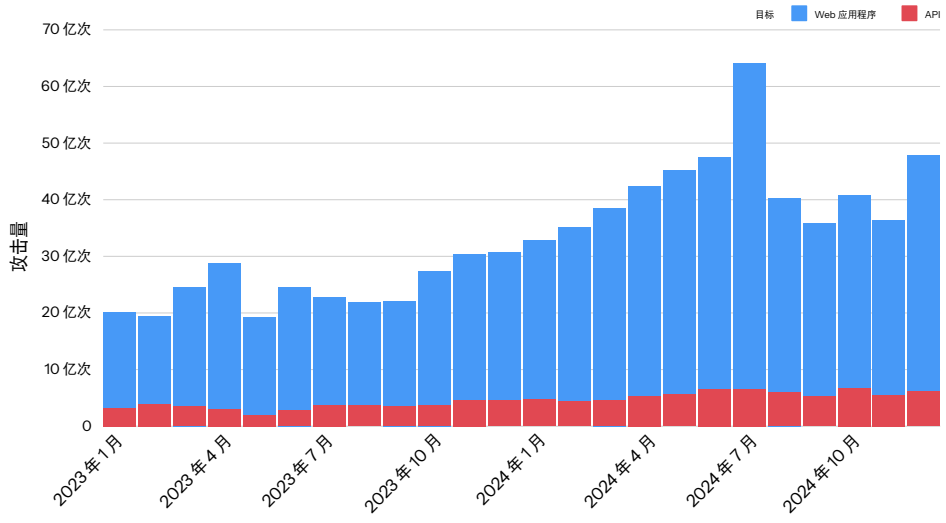
在本部分中，我们将重点介绍 APJ、EMEA 和 LATAM 地区一些主要趋势。此外，我们还收录了这些地区内特定区域的数据，在这些区域我们拥有足够的攻击事件数据，可以提供具有统计意义的见解。

Web 应用程序和 API 攻击：流量分析

通过比较各地区的月度 Web 攻击量，可以发现它们之间存在显著差异（图 12）。

APJ 地区：月度 Web 攻击量

2023 年 1 月 1 日 – 2024 年 12 月 31 日



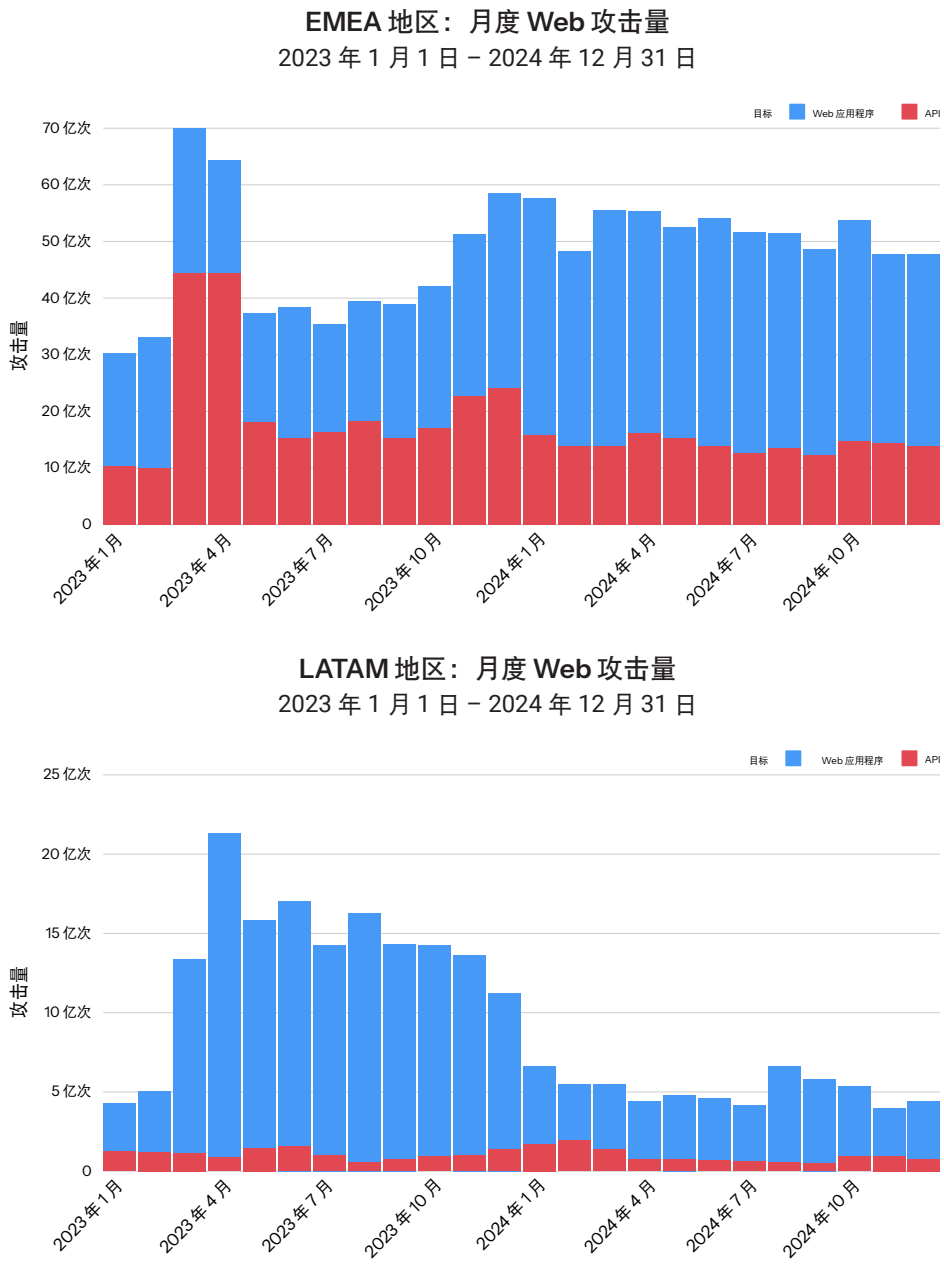


图 12：Web 应用程序攻击活动促使 APJ 和 EMEA 地区的 Web 攻击总数增加，而 LATAM 地区的攻击急剧减少

APJ 地区遭受的 Web 攻击总数同比大幅增加 73%，从 2023 年的 290 亿次增加到 2024 年的 510 亿次。在 EMEA 地区，同比增长幅度适中，为 16%（从 540 亿次增加到 620 亿次），但这种小幅增加受到了数据中记录的异常事件的影响，如果将此事件剔除，则增幅将接近 33%。在 LATAM 地区，Web 攻击总数从 2023 年的 160 亿次大幅减少到 2024 年的 600 万次，同比降幅高达 61%。

Web 应用程序攻击量的增加似乎推动了 Web 攻击总数的增加，因为 API 攻击量仍然处于较低水平，尤其是在 APJ 和 LATAM 地区。

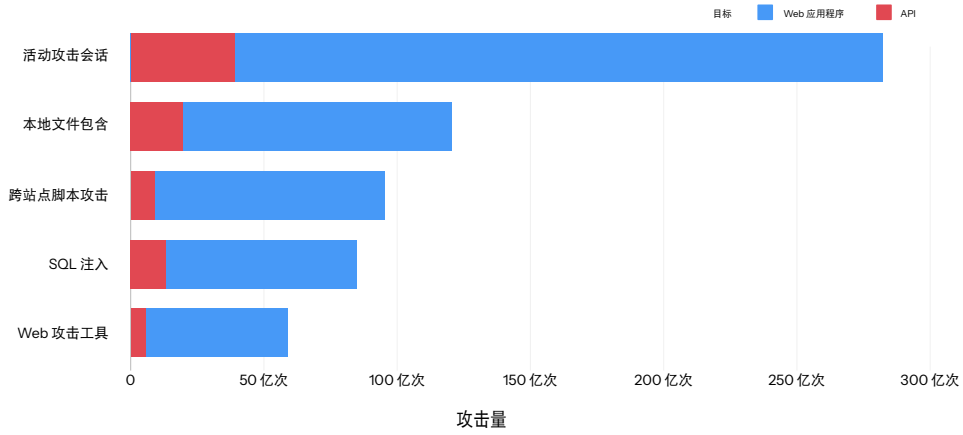
在 EMEA 地区，继 2023 年上半年出现激增（与针对西班牙商业行业的大规模集中攻击相关）之后，API 攻击水平有所下降并在 2024 年全年保持较低水平，但与其他地区相比仍然较高。

在 LATAM 地区，Web 攻击量有所下降，因为攻击者将其目标从商业行业转向其他行业（包括制药和商业服务），并且转为采用其他攻击类型，例如勒索软件。

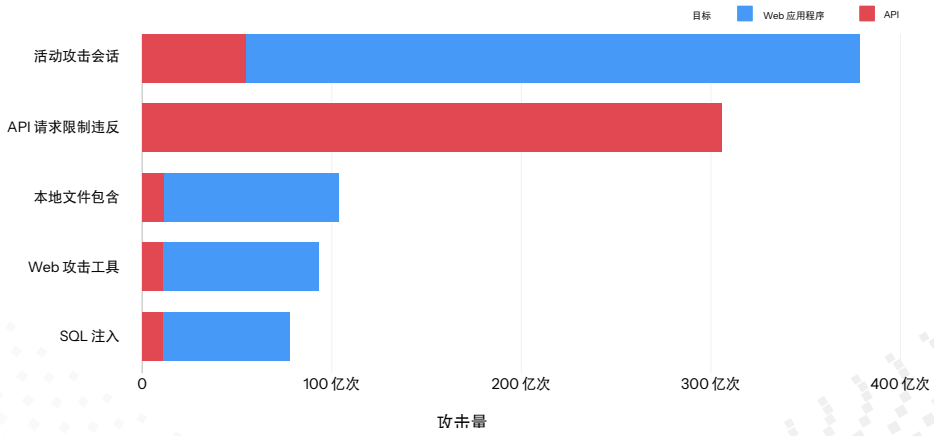
Web 应用程序和 API 攻击：流行的策略

在过去两年里，攻击者继续依赖屡试不爽的传统方法，但基于行为的现代 Web 攻击媒介的使用率也很高（图 13）。

APJ 地区：按媒介划分的 Web 攻击量
2023 年 1 月 1 日 – 2024 年 12 月 31 日



EMEA 地区：按媒介划分的 Web 攻击量
2023 年 1 月 1 日 – 2024 年 12 月 31 日



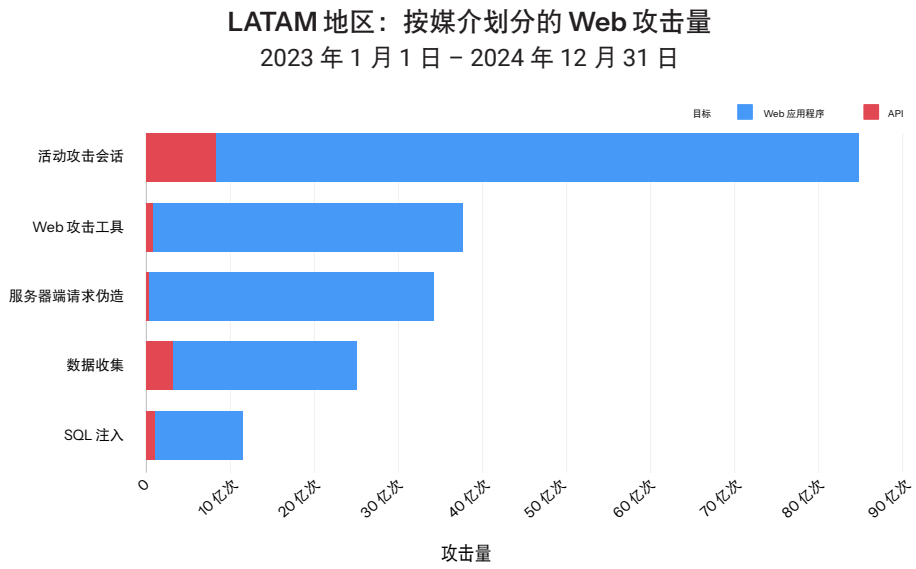


图 13：在各个地区，主要攻击媒介包括传统方法和专门针对 API 滥用的基于行为的现代方法

与全球趋势一致的是，各个地区的传统攻击媒介持续存在，包括 LFI、SQLi 和 XSS，以及 LATAM 地区观察到的 SSRF。我们在 2025 防御者指南中强调了 XSS 的持久影响以及它与防范传统 Web 漏洞的持续相关性。

在此期间，随着攻击者越来越多地关注 API 滥用，不同以往的是，有关基于行为的现代攻击媒介的问题不断增加。攻击者使用这些媒介来发现漏洞以进行利用。通过在地区层面上跟踪这些媒介，Akamai 研究人员观察到：

- 每个地区的主要攻击媒介是活动攻击会话，我们对此采用了智能控制措施，以主动拦截一段时间内来自已知攻击者的请求。
- API 请求限制违反是 EMEA 地区第二大最常见的攻击媒介，该地区遭受的以 API 为重点目标的攻击最为密集。攻击者会尝试通过规避速率限制和数据输入等要求来滥用 API。
- 在每个地区中，Web 攻击工具都位列前五名。攻击者使用此媒介来探测目标，以获取目标上可能被用于恶意目的的安全防护、配置或潜在漏洞信息。

如需详细了解这些主要的攻击媒介，请参阅 Web 攻击部分。

Web 应用程序和 API 攻击：主要目标

通过具体研究攻击者在每个地区的攻击重点，我们发现，APJ 地区的澳大利亚（203 亿次）、印度（173 亿次）和新加坡（159 亿次）遭受的 Web 应用程序和 API 攻击最多，其次是日本（63 亿次）、中国大陆（62 亿次）、韩国（49 亿次）、新西兰（29 亿次）和中国香港特别行政区（22 亿次）。

在 EMEA 地区，受 Web 应用程序和 API 攻击影响最大的国家/地区是英国（303 亿次）、荷兰（195 亿次）、西班牙（142 亿次）和德国（128 亿次）。随后是奥地利（82 亿次），以及法国（75 亿次）、意大利（41 亿次）、瑞士（37 亿次）、比利时（35 亿次）和以色列（33 亿次）。

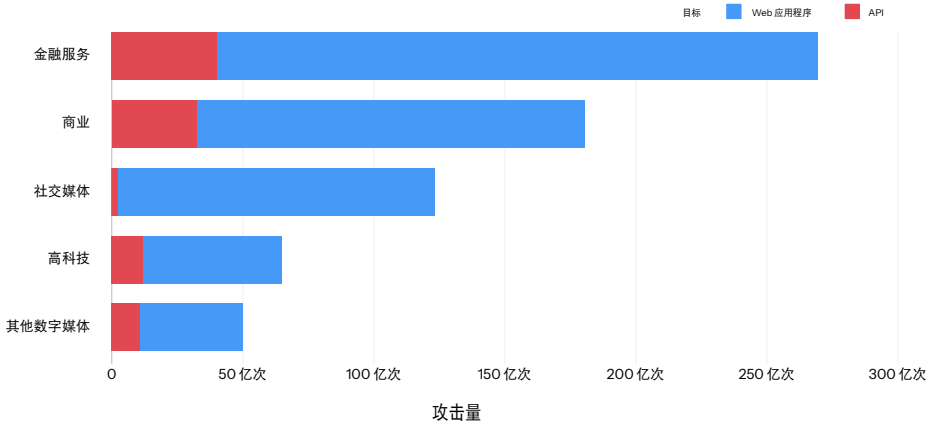
在 LATAM 地区，Web 应用程序和 API 攻击集中在巴西（193 亿次），紧随其后的是墨西哥（20 亿次）和智利（4 亿次），但它们遭受的攻击只占该地区的一小部分。

行业目标

通过行业趋势分析发现，在 APJ、EMEA 和 LATAM 地区，商业和金融服务始终位列遭受 Web 攻击最多的三大行业（图 14）。

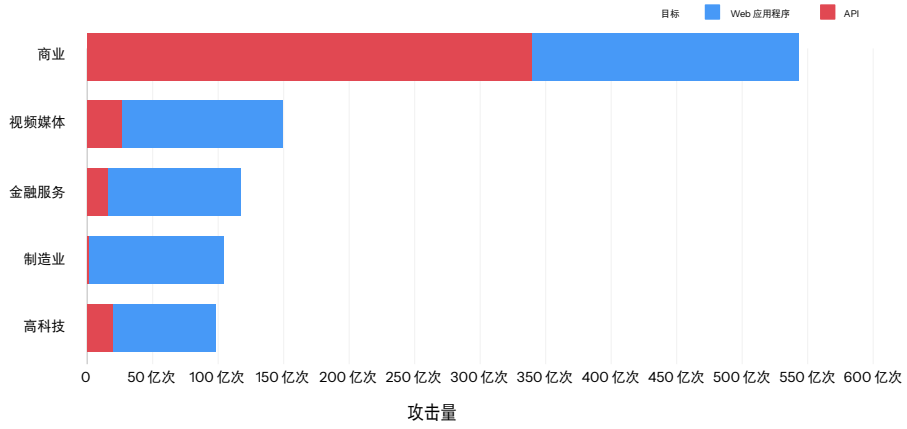
APJ 地区：按行业划分的 Web 攻击量

2023 年 1 月 1 日 – 2024 年 12 月 31 日



EMEA 地区：按行业划分的 Web 攻击量

2023 年 1 月 1 日 – 2024 年 12 月 31 日



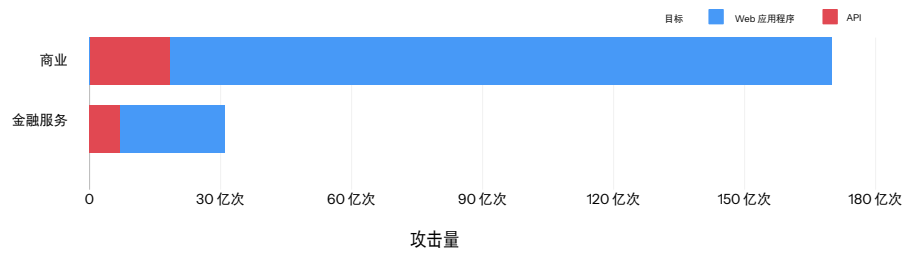


图 14：商业和金融服务位列 APJ、EMEA 和 LATAM 地区遭受攻击最多的三大行业

在 APJ 地区，金融服务业遭受的 Web 攻击总数最多，达到了 270 亿次；商业位居第二，达到了 180 亿次，其同比增长幅度分别为 52% 和 161%。其他数字媒体是遭受 API 攻击最多的行业，占比达到 22%，随后是商业 (18%) 和金融服务 (15%)。

在 EMEA 地区，商业是受 Web 攻击影响最大的行业，遭受的攻击量达到 540 亿次，是排名第二的视频媒体业的三倍多。尽管攻击集中度很高，但针对商业实体的 Web 攻击总数同比下降了 10%，因为该地区 2023 年出现的激增导致此数据出现了偏差。然而，由于针对金融服务业 (152%) 和制造业 (96%) 等其他行业的攻击增加，EMEA 地区的 Web 攻击总数仍然同比增长 16%。通过仔细研究该地区针对 API 的攻击，我们发现针对商业行业的 Web 攻击总数中有 63% 都以 API 为目标。

我们在 LATAM 地区观察到了类似的趋势，针对商业行业的 Web 攻击总数达到 170 亿次，远超其他行业，但针对该行业的攻击同比减少 76%。另一方面，针对制药和商业服务行业的攻击同比分别增加 107% 和 129%。此外，针对商业行业的攻击中 11% 以 API 为目标，而针对金融服务业的攻击中以 API 为目标的比例更高，达到了 23%。

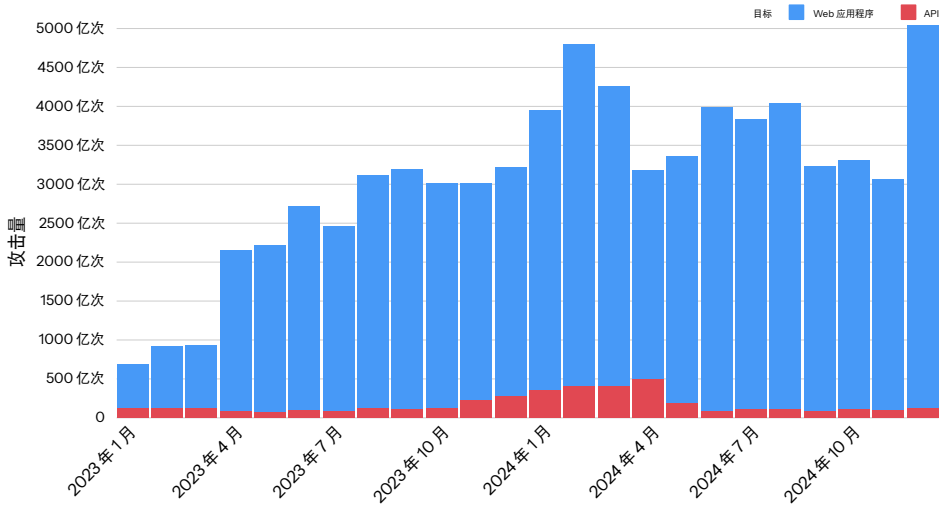
金融服务和商业行业有一些共同的特性，这些特性导致它们成为 Web 应用程序和 API 攻击的目标：都在复杂的生态系统内运作，都高度依赖 API 并拥有高价值的数据。攻击者将传统与新兴的攻击技术相结合，以实现其目标。

第 7 层 DDoS 攻击：流量分析

对各地区的月度第 7 层 DDoS 攻击量进行对比后发现，APJ 地区是攻击高发地区，而 EMEA 和 LATAM 地区的攻击呈现出波动状态（图 15）。

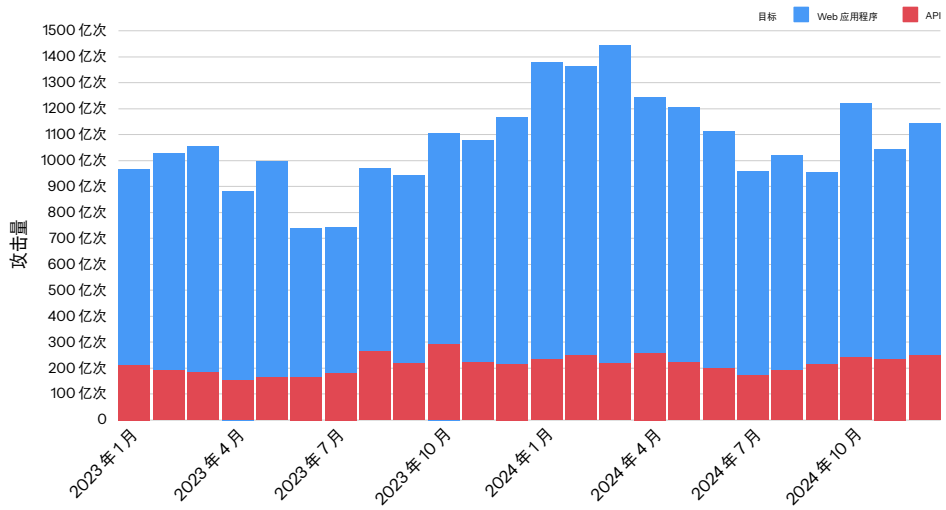
APJ 地区：每月的第 7 层 DDoS 攻击量

2023 年 1 月 1 日 – 2024 年 12 月 31 日



EMEA 地区：每月的第 7 层 DDoS 攻击量

2023 年 1 月 1 日 – 2024 年 12 月 31 日



LATAM 地区：每月的第 7 层 DDoS 攻击量

2023 年 1 月 1 日 – 2024 年 12 月 31 日

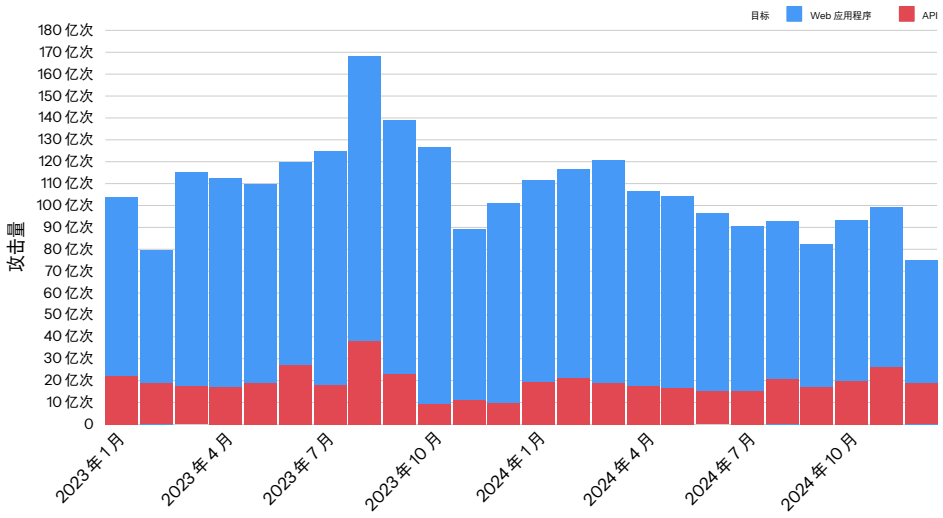


图 15：2024 年，第 7 层 DDoS 攻击量在 APJ 和 EMEA 地区呈上升趋势，而 LATAM 地区的攻击有所减少

APJ 地区遭受的第 7 层 DDoS 攻击量同比增加 66%，达到 24 个月以来的最高点，于 2024 年 12 月达到 5040 亿次的峰值。此增长的主要推动因素是针对社交媒体行业的攻击。

在 EMEA 地区，第 7 层 DDoS 攻击量与 2024 年 3 月达到峰值，接近 1450 亿次，随后减少又再次增加，同比增长达到 20%。这可以归因于地缘政治和技术因素的共同作用。该地区持续紧张的局势助长了黑客活动。AI 增强型工具和 DDoS 即服务平台的兴起降低了网络犯罪分子的准入门槛，从而加剧了这种趋势。

在报告期之初，LATAM 地区遭受的第 7 层 DDoS 攻击尝试大幅增加，与此同时，旨在使 API 资源不堪重负的 HTTP 泛洪攻击（该攻击媒介已在第 7 层 DDoS 攻击：同比比较和趋势部分中进行了详细讨论）也有所增加。攻击活动于 2023 年 8 月达到峰值 168 亿次，随后在报告期的剩余时间内不断减少至最低值 75 亿次，攻击量同比减少 15%。

第 7 层 DDoS 攻击：主要目标

与我们先前的第 7 层 DDoS 攻击分析相比，在每个地区内，我们都观察到受攻击者攻击的地区和行业几乎没有变化。

在 APJ 地区，新加坡遭受的攻击最为密集，达到 4.7 万亿次，其次是印度（1.1 万亿次）、韩国（6070 亿次）、印度尼西亚（2830 亿次）、中国大陆（2460 亿次）、日本（1110 亿次）、澳大利亚（1080 亿次）以及中国台湾（810 亿次）。

在 EMEA 地区，遭受第 7 层 DDoS 攻击量最多的国家/地区是德国（5690 亿次）和英国（5060 亿次），其次是以色列（2050 亿次）、瑞典（1930 亿次）和马耳他（1600 亿次）。意大利（1580 亿次）、瑞士（1470 亿次）、法国（1290 亿次）、荷兰（1110 亿次）和西班牙（960 亿次）均位列前十。

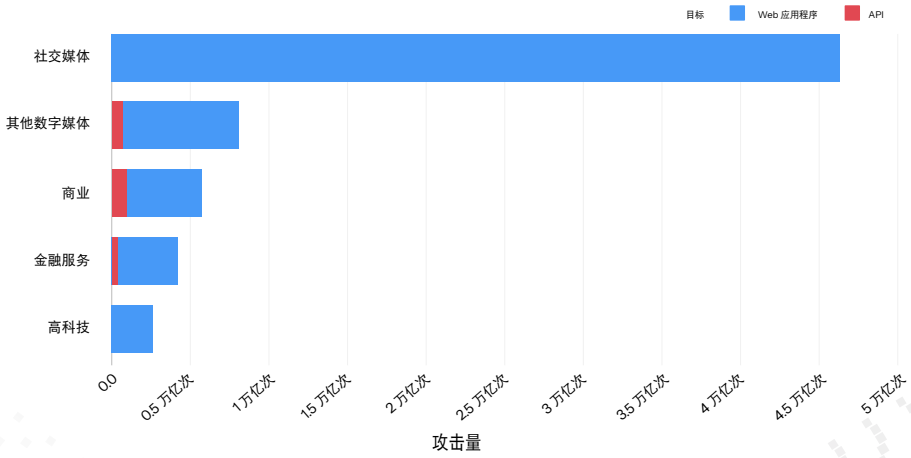
在 LATAM 地区，巴西遭受的第 7 层 DDoS 攻击最多，达到 1750 亿次，其次是墨西哥（390 亿次）和哥斯达黎加（190 亿次）。

行业目标

自我们发布上一期的安全应用程序 SOTI 报告以来，APJ 和 EMEA 地区受第 7 层 DDoS 攻击影响的主要行业没有发生变化（图 16）。正如我们在该报告中详细讨论的那样，从 2023 年 1 月到 2024 年 6 月，APJ 地区针对社交媒体平台的第 7 层 DDoS 攻击激增，这与全球范围内更广泛的军事冲突和高度中介化选举活动相关——这并不让人感到奇怪，因为在地缘政治动荡期间社交媒体平台会接收大量流量。正如预期的那样，在 2024 年的剩余时间里，此趋势因亚太地区及日本和美国的选举而愈演愈烈。这些因素导致针对该行业的攻击量同比增加 130%。

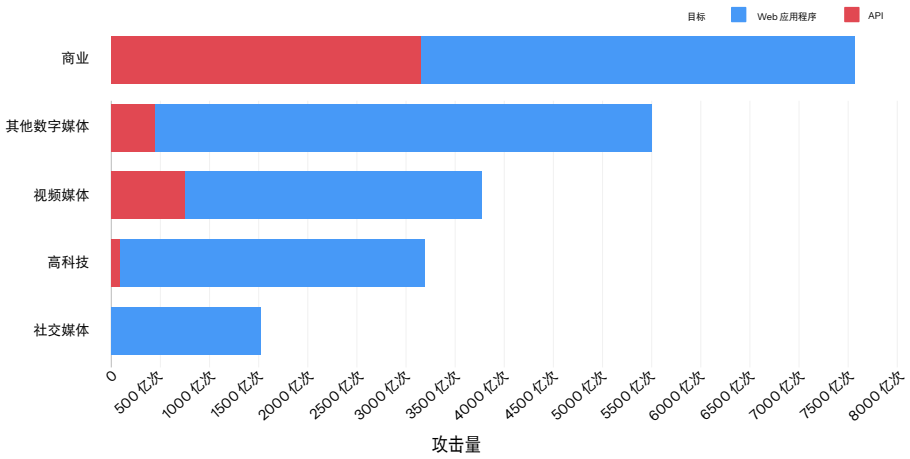
APJ 地区：按行业划分的第 7 层 DDoS 攻击量

2023 年 1 月 1 日 – 2024 年 12 月 31 日



EMEA 地区：按行业划分的第 7 层 DDoS 攻击量

2023 年 1 月 1 日 – 2024 年 12 月 31 日



LATAM 地区：按行业划分的第 7 层 DDoS 攻击量

2023 年 1 月 1 日 – 2024 年 12 月 31 日

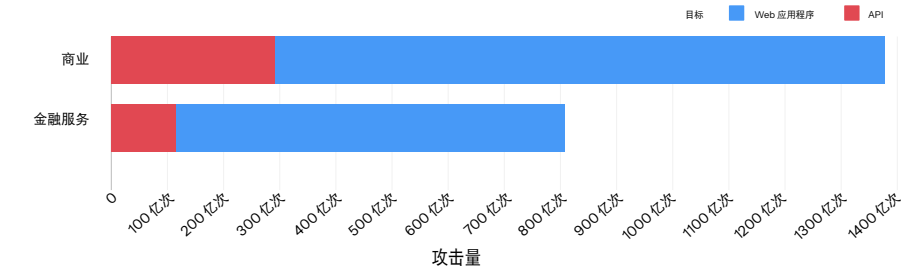


图 16：自我们上次进行分析以来，每个地区受影响的主要行业保持不变；商业始终是遭受针对 API 的第 7 层 DDoS 攻击最多的行业

在 EMEA 地区，商业仍然是受第 7 层 DDoS 攻击影响最大的行业，其次是其他数字媒体和视频媒体。这些攻击同比增加幅度最大的行业包括高科技 (70%)、社交媒体 (23%) 和商业 (14%)。这些变化表明了攻击者在行业与地区之间转移攻击目标的速度有多快，因此值得跟踪更广泛的趋势。

此外，商业也是 LATAM 地区遭受第 7 层 DDoS 攻击最多的行业，排在第二的是金融服务。在报告期内，各行业第 7 层 DDoS 攻击活动的持续水平大致保持一致。

与全球趋势一致，在遭受第 7 层 DDoS 攻击最多的行业中，商业行业在每个地区都面临最高的 API 攻击集中度。在 EMEA 地区，针对商业的攻击中有 43% 以 API 为目标，而在 LATAM 和 APJ 地区，这一比例分别为 21% 和 16%。

由于地缘政治动荡和高可见性服务中断可能造成的经济影响等原因，商业、媒体和金融服务一直是过去两年中 EMEA 和 LATAM 地区第 7 层 DDoS 攻击的主要目标。我们先前详细讨论了针对商业和金融服务业的高水平攻击活动背后的驱动因素和方法。如需了解相关内容，请参阅行业趋势部分。

合规性

全球和北美视角

2025 年的全球网络安全形势具有前所未有的的复杂性和多变性。地缘政治局势紧张，特别是乌克兰和中东地区的冲突持续不断，加剧了网络威胁和国家支持的攻击。黑客活动的兴起，尤其是亲俄团体针对西方国家的黑客活动，让威胁形势变得更加复杂。从经济角度看，各行业的快速数字化转型扩大了攻击面，网络犯罪分子越来越多地以关键基础行业为目标并利用 AI 等先进技术来增强自身的能力。

这些因素，再加上主要国家/地区面临的全球经济压力和政治转变，为全球的网络安全专业人员带来了前所未有的挑战。保护 Web 应用程序和 API 是企业面临的一项重大挑战。文明黑客、网络安全专业人员和 Akamai 等企业为解决保护这些入口点的迫切需求而付出的努力，与日益增长的合规考虑因素相辅相成。

世界各地的监管机构正在针对应用程序实施更严格的网络安全合规要求。在北美，关注点已转型全面的风险管理策略和强制性事件报告。美国的《关键基础设施网络事件报告法》预计将于 2026 年生效，它要求关键基础设施企业必须对其信息系统进行清点、对网络风险进行分类并评估其网络安全态势，至少每年进行一次。此法案强调了在应用程序中实施强有力的安全措施的必要性，特别是那些在能源、化学制造和信息技术等关键行业中使用的应用程序。

同样，加拿大和墨西哥也在使其法规与国际标准接轨，重点关注数据保护和关键基础设施安全。虽然具体的法规有所不同，但全球趋势是针对应用程序实施更加严格的安全要求，包括增强的输入验证、安全开发实践以及定期安全审计。

API 安全形势正面临着多重挑战，并且由于 API 在实现服务集成和数据交换方面的关键作用，它们正在成为网络犯罪分子的主要目标。为此，世界各地的监管机构出台了更严格的法规，要求企业实施强有力 API 安全措施。

这些措施包括强制性持续 API 发现、监控和抵御不断发展变化的威胁。在北美，重点是对 API 生态系统进行彻底的风险评估，强调安全开发实践、强大的身份验证机制和实时威胁检测能力。AI 驱动的 SaaS 工具（往往通过 API 进行集成）的快速采用显著扩大了攻击面，促使监管机构要求采取更先进的安全方法。

随着 API 环境变得日益复杂，特别是 AI 和机器学习应用的兴起，合规要求也在不断地发展变化，以降低与数据泄露、未经授权的访问和服务中断相关的风险。虽然 APJ、LATAM 和 EMEA 等地区正在制定自己的具体法规，但全球趋势是实现 API 安全标准的统一，以应对现代数字架构的互联互通性。

APJ 地区视角

APJ 地区的监管环境正在经历重大转变，新的合规要求将影响各个行业的企业。新加坡近期对其网络安全法案进行了修订，扩大了法案适用范围，以涵盖物理和虚拟关键信息基础架构系统，包括那些托管在云平台上和位于海外的系统。日本更新了其国家网络安全事件准备和战略中心法律，而印度通过了《数字个人数据保护法案》，对其《信息技术法案》进行了全面修订。澳大利亚出台了自己的 2023-2030 网络安全战略，进一步凸显出该地区对加强网络安全措施的重视。作为该战略的一部分，2024 年底对《澳大利亚关键基础设施安全法》进行了修订，新的《2024 年网络安全法》已成为法律；执法范围现在将包括处理敏感数据的物联网设备、应用程序和 API 等次要资产。这些监管变化正促使各企业重新评估和加强其 Web 应用程序安全实践，并特别强调保护关键基础架构和敏感数据。

PCI DSS v4.0.1 将对处理支付卡数据的企业产生重大影响；合规截止日期为 2025 年 3 月 31 日。该新版本对 Web 应用程序提出了更严格的要求，包括对消费者的浏览器中执行的所有支付页面脚本实施控制以及使用自动技术解决方案来持续检测和阻止基于 Web 的攻击。APJ 地区的企业现在必须进行彻底的差距分析、更新其安全策略并实施必要的技术变更，以满足这些适用于其 Web 应用程序的增强型安全标准。

就 API 而言，APJ 地区越来越重视 API 安全性，部分原因在于开放银行业务计划得到了越来越多的采纳。虽然 APJ 地区尚未像 EMEA 地区那样完全接受开放银行业务法规，但该区域的国家/地区仍然有机会主动解决 API 安全问题。2024 年 8 月，对该地区 API 安全见解的调查显示，内部 API 最常用，但外部用户访问仍然是 API 访问控制的首要问题。这表示企业需要实施强有力的 API 安全措施，包括强大的身份验证和授权协议、数据加密以及持续 API 发现和监控。随着该地区朝着开放银行业务指令的方向发展，企业将需要优先考虑 API 安全，以确保遵守不断发展的法规并防范新兴威胁。

EMEA 地区视角

在地缘政治紧张局势、技术进步和监管变化等因素复杂的相互作用下，EMEA 地区的网络安全形势正在经历重大转变。该地区面临着独特的挑战，乌克兰和中东地区持续不断的冲突加剧了网络威胁和国家支持的攻击。此外，黑客活动的兴起，尤其是亲俄团队针对欧洲国家/地区的黑客活动，也让该地区成为出于政治动机而开展的网络行动的主要目标。

EMEA 地区内的 API 环境正面临着多重挑战。由于 API 在实现服务集成和数据交换方面的关键作用，它们已成为网络犯罪分子的主要目标。AI 驱动的 SaaS 工具（往往通过 API 进行集成）的快速采用显著扩大了攻击面。

为了应对这些不断升级的威胁，欧盟出台了一套全面的网络安全法规。更新后的网络与信息系统 (NIS2) 指令已于 2025 年 1 月起生效，其适用范围显著扩大，涵盖了 18 个关键行业，并要求大中型实体采取严格的网络安全措施。

对于金融行业，自 2025 年 1 月 17 日起实施的《数字运营弹性法案》(DORA) 取代了 NIS2，该法案要求金融服务中使用的应用程序具备强大的信息和通信技术风险管理框架、事件报告机制以及数字运营弹性测试计划。此外，已于 2025 年 3 月 31 日强制生效的 PCI DSS v4.0.1，引入了以不断变化的安全需求、持续的安全流程、灵活的方法和增强的验证程序为中心的新合规要求。即将出台的修订版欧盟支付服务指令 (PSD3) 旨在通过加强数据共享机制、强化安全要求并改进对金融服务业的监督来弥补 PSD2 的缺陷。

于 2024 年 12 月 10 日生效的《网络弹性法案 (CRA)》为在欧盟销售的包含数字元素的产品引入了强制性网络安全标准，要求制造商在互联产品的整个生命周期内实施安全措施。对于应用程序开发人员和用户来说，CRA 将智能手机和平板电脑视为重大风险媒介。这就要求企业将移动终端作为其整体网络安全战略的基本组成部分，并在应用程序的整个生命周期内实施严格的安全措施。

在英国，即将出台的《网络安全和弹性法案》将提升英国的网络防御能力并保护基本公共服务。该法案是对传统监管框架的重要更新将扩大适用范围，以保护更多数字服务和供应链、加强执法力度并提高报告要求。

LATAM 地区视角

LATAM 地区的网络安全形势正在快速地发展变化，既受到了全球技术趋势的影响，也受到了该地区特有的经济和政治挑战的影响。在此背景下，LATAM 各国的快速数字化转型，加上互联互通程度越来越高的系统的脆弱性，使得该地区成为对网络犯罪分子和国家支持的攻击者极具吸引力的目标。商业和金融服务业已成为网络攻击的主要目标。在线零售商、付款处理方、银行、保险公司、金融科技初创公司和加密货币交易所都特别容易受到以其数字基础架构（尤其是其 Web 应用程序和 API）为目标的威胁的侵扰。

LATAM 各国认识到了这些挑战，并且在制定和实施网络安全法规方面取得了长足进步，并且越来越关注 Web 应用程序和 API 安全。巴西在 Lei Geral de Proteção de Dados Pessoais (LGPD) 的实施方面发挥着主导作用，该法律已生效并对数据保护和安全提出了严格要求。虽然 LGPD 并非专门针对 Web 应用程序或 API，但它已促使企业增强其整体网络安全态势，包括其数字接口的安全。

同样，智利也颁布了其《网络安全框架法》，该法律已于 2025 年 1 月 1 日生效。它设立了国家网络安全局，并概述了预防、报告和解决各行业（包括那些严重依赖 Web 应用程序和 API 的行业）网络安全事件的综合措施。此外，2025 年 1 月 1 日，阿根廷发布了《联邦预防网络犯罪和网络安全战略管理计划（2025-2027 年）》。

在 API 专用法规领域，已取得了一些积极的进展。例如，墨西哥实施了专注于金融行业（包括金融科技）的立法，其中对信用机构和清算机构开发安全 API 提出了详细的要求。此方法反映出人们越来越认识到 API 在现代数字生态系统中发挥的关键作用以及实施有针对性的安全措施的必要性。此外，墨西哥的《保护私有主体持有的个人数据联邦法》规范了个人数据的处理并规定了公司和企业的相应义务。

哥伦比亚也一直在推进其监管框架，通过发布针对公共机构网络安全的公共政策来扩大其法律访问，并创建了一个具有不同级别的事件响应报告的数字安全风险管理系统。虽然并非专门针对 API，但这些措施必然会影响企业内的 API 安全实践。

在该地区，采用行业特定举措（例如，开放金融框架）的趋势在不断增强，这些举措设定了保护消费者数据的 API 安全标准。这些框架在金融行业尤其重要，因为 API 的安全性对维护金融交易的完整性和保护敏感的客户信息来说至关重要。随着 LATAM 各国继续将安全进步视为优先事项并将其网络安全法规与国际标准接轨，我们可以预见到会有更全面、更具体的 Web 应用程序和 API 安全指导方针出台。

抵御措施

在不断发展变化的威胁形势下，随着更多先进攻击技术的出现，保护 Web 应用程序和 API 将成为企业面临的一项重大挑战。我们推荐的一些保护和抵御技术包括：

- **制定全面的 API 安全计划：**实施左移和 DevSecOps 方法，将安全性融入从 API 设计到生产后的各个阶段。确保持续发现和监测，以了解完整的攻击面，包括隐藏的 API（影子、遗留和僵尸 API）。通过严格的身份验证和授权（OAuth 2.0、mTLS、基于角色的访问控制/基于属性的访问控制）、速率限制和爬虫程序抵御来增强安全性，以防止滥用。实施实时威胁检测、异常监控和运行时保护，以便在攻击发生时识别并阻止它们。确保遵守 DORA、GDPR、HIPAA、NIS2 和 PCI DSS 等法规，同时强制实施 API 治理策略以维护大规模安全性。
- **实施强有力的网络安全措施：**使用自适应安全引擎，它能够实时对威胁进行持续监控和响应，并提供威胁情报和运行时保护。此外，还可以使用动态应用程序安全测试（DAST）等 API 测试工具来帮助确保满足安全要求（包括安全访问、加密和身份验证）。
- **对威胁进行主动防御：**使用专用 DDoS 防护工具，配置速率限制和 CDN 缓存，并实施补丁管理、访问控制策略和网络分段。还可以通过持续流量监控和混合平台来保护 DNS 基础架构。
- **抵御 API 漏洞：**遵循既有的安全指南（例如 OWASP 提供的指南），确保实现强大的 API 安全防护并解决 API 架构中存在的不良编码实践和错误配置等风险，这些风险会产生让黑客进行未经授权的访问或操纵数据的可利用漏洞。

- **防范勒索软件威胁：**使用分层方法来抵御勒索软件。实施 Zero Trust 解决方案以阻止恶意流量，使用微分段进行详细监测和精准的访问控制，并利用 MITRE ATT&CK 框架来了解攻击模式和改进响应策略。
- **为 AI 做好准备：**采用全面的防御策略，该策略包含爬虫程序防御解决方案、AI 赋能的安全工具、专用防火墙以及主动措施（如持续评估和 Zero Trust 模式），以应对 AI 日益普及所带来的新安全风险。通过多层面防范保护 AI 系统：通过了解模型和数据集来应对特定威胁，例如提示注入和数据中毒；执行主动漏洞测试；并使用集成在开发和运行时环境中的强大防御措施，如行为监控、内容验证和自动攻击响应。

方法

Web 应用程序和第 7 层 DDoS 攻击

此数据表示通过我们的 Web 应用程序防火墙 (WAF) 观察到的流量的应用层告警数量。在针对受保护的网站、应用程序或 API 的请求中检测到恶意负载时，系统就会触发 Web 应用程序攻击告警。当我们检测到对受保护网站、应用程序或 API 的请求数量出现异常时，系统会触发第 7 层 DDoS 告警。恶意和良性请求都可能触发此类爬虫程序告警。通常，这些请求自身是良性的，但出现大量请求表明存在恶意企图。告警并不表示攻击已经得手。虽然这些产品允许的定制程度极高，但我们在收集此处提供的数据时，所采用的方式并未考虑受保护资产的定制配置。

这些数据来自一个内部工具，专用于分析在 Akamai Cloud 上检测到的安全事件。Akamai Cloud 是一个庞大的网络，在全球 130 多个国家/地区将近 1,300 个网络中的 4,000 多个地点拥有约 340,000 台服务器。我们的安全团队使用此数据（每月达到 PB 级）来研究攻击，标记恶意行为并将其他情报馈送到 Akamai 解决方案中。

该数据涵盖了从 2023 年 1 月 1 日到 2024 年 12 月 31 日的 24 个月的时间段。

API 安全攻击数据

Akamai 与 Noname Security 的整合显著增强了我们对 API 威胁的研究与报告能力。此数据集仍然处于集成和分析的早期阶段。为撰写本报告，我们选取了 2025 年第一季度的 30 天数据样本，以分析 API 安全告警根据其对应的安全框架和合规标准的细分情况。此数据集将继续发展，并在未来提供对 API 安全问题的深入分析。

致谢名单

研究总监

Mitch Mayne

编辑与创作

Charlotte Pelliccia　Badette Tribbey

Lance Rhodes　Maria Vlasak

审稿和主题撰稿

Tom Emmons　Stas Neyman

Reuben Koh　Steve Winterfeld

Richard Meeus

数据分析

Chelsea Tuttle

推广材料

Barney Beal　Ashley Linares

营销与发布

Georgina Morales Hampe　Emily Spinks

互联网现状/安全性

《互联网现状/安全性》报告由 Akamai 精心呈献，获得了各界的广泛赞誉。请前往以下网址回顾往期报告，并关注即将发布的新报告：akamai.com/soti

Akamai 威胁研究

关注最新的威胁情报分析、安全报告和网络安全研究的动态。

akamai.com/security-research

访问本报告中的数据

查看本报告中引用的图片和图表的高画质版本。这些图片可免费使用和引用，但前提是注明转载来源，并且保留 Akamai 徽标。

akamai.com/sotidata

Akamai 安全研究

阅读 Akamai 安全研究博客，从快速反应的角度详细了解当今极为重要的研究。

akamai.com/blog/security-research

发布时间：2025 年 4 月。

扫码关注，获取最新云计算、云安全与CDN前沿资讯