SOTI

第 10 卷，第 01 期

10 YEARS
OF SECURITY INSIGHT

潜伏在阴影之中

攻击趋势揭示了 API 威胁

Akamai

互联网现状/安全性

目录

为何监测能力很重要

今年是 Akamai 发布《互联网现状 (SOTI)》报告并通过该报告来分享安全研究见解的第 10 年。多年来，随着企业运营方式和威胁形势的演变，这些报告的关注点也发生了变化。从 2024 年开始，我们不再将 Web 应用程序攻击和 API 攻击视为一个主题，而是使用新的数据集，以便 Akamai 研究人员可以将这两种类型的攻击分开研究。在本报告中，我们将关注以 API 为目标的 Web 攻击所占百分比（如需了解更多详细信息，请阅读“方法”部分）。这将有助于我们更好地了解攻击者对 API 进行攻击的方式，并制定行之有效的抵御策略。

很多公司最近的一些变革都是基于 API，这些变革改善了员工和客户体验。但遗憾的是，数字化创新和 API 经济的迅猛发展也为网络犯罪分子提供了新的可乘之机。因此，监测能力是 API 安全中一个至关重要的方面。一旦影子 API 或恶意 API 等盲点得以揭示，安全团队就可以开始解决先前未察觉到的漏洞。

在 2024 年的第一期 SOTI 报告中，我们将重点介绍以 API 为目标的各种攻击（包括传统 Web 攻击），并通过常见问题领域（例如，可通过数据进行监测的安全态势和运行时挑战）来应对 API 滥用带来的危险。此外，我们将按行业和区域说明这些危险，以便您更准确地评估您公司面临的风险。我们还会提供一些真实案例分析，强化合规要求，并说明法规趋势如何影响您的安全策略。在本报告结尾部分，我们将介绍有助您提升对 API 环境的监测能力的措施，以便增强您的整体安全态势。

报告的关键见解

- 在 2023 年 1 月至 12 月这 12 个月期间，共有 29% 的 Web 攻击以 API 为目标，这表明 API 是网络犯罪分子的重点攻击目标。
- 对 API 的攻击包括开放式 Web 应用程序安全项目 (OWASP) 十大 API 安全风险清单以及 OWASP 十大 Web 应用程序安全风险中强调的风险，还有使用结构化查询语言注入 (SQLi) 和跨站点脚本攻击 (XSS) 等屡试不爽的方法来渗透其目标的攻击者所带来的风险。
- 业务逻辑滥用成为一个严重问题，因为在缺乏 API 行为基线的情况下，识别异常的 API 活动变得尤为困难。企业若缺乏解决方案来监视 API 活动中的异常情况，将面临运行时攻击的风险。例如，数据抓取作为一种新兴的数据泄露媒介，可利用经身份验证的 API 从企业内部缓慢窃取数据。
- API 已成为当今大多数数字化转型的核心。因此必须了解行业趋势以及相关应用场景，例如会员欺诈、滥用、授权问题和盗刷攻击。
- 企业在安全策略流程中应尽早考虑合规要求和新出台的法规，以避免未来可能需要重新设计策略。

API：重要的攻击媒介

从设计角度来看，API 是数据管道。因此，一旦攻击者通过漏洞利用或针对业务逻辑的攻击等常用手段实现未经授权的访问，API 便可能将数据暴露给攻击者。2022 年，Gartner 预测 API 滥用和数据泄露到 2024 年几乎将会翻倍增长。时间如梭，现在的情况是备受瞩目的 API 事件比以往更加常见。开放式 Web 应用程序安全项目 (OWASP) 是以其十大安全风险清单而闻名的非营利组织。实际上，去年他们发布了一份专门关于 API 风险的单独清单，名为“OWASP 十大 API 安全风险”，以帮助企业辨识 API 所带来的特有威胁。

Akamai 的研究发现，API 正在成为攻击目标，攻击手段不仅包括传统攻击方式，还有针对 API 设计的特定攻击技术，因而需要采取多种保护措施。实际上，我们发现，从 2023 年 1 月到 12 月，近 30% 的网络攻击以 API 为目标（图 1）。除非企业能够正确地保护其 API 或摸清其环境中使用的所有 API，否则随着 API 使用需求的增加，这些攻击也很可能会继续增加。了解攻击面的完整范围首先从一份全面准确的 API 清单开始。

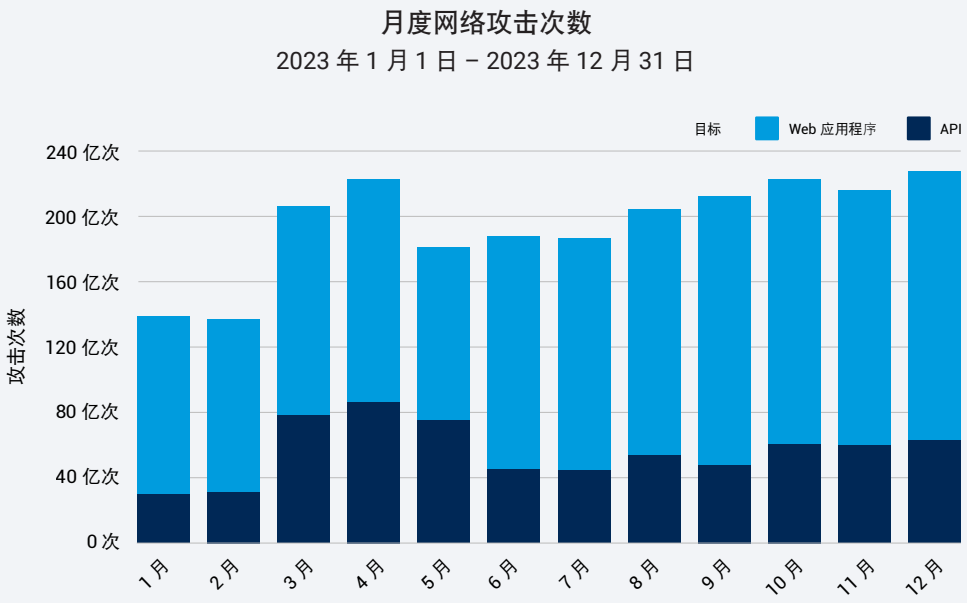


图 1：针对 API 的网络攻击从 1 月份的 22% 增长到 12 月份的 28%，2023 年 3 月至 5 月期间出现几次波动

此外，我们还在全球范围内观察到一些有意思的趋势，欧洲、中东和非洲地区 (EMEA) 地区遭受的以 API 为目标的 Web 攻击占比最高 (47.5%)，紧随其后的分别是北美地区 (27.1%) 和亚太及日本 (APJ) 地区 (15%)。在国家/地区层面上，遭受此类攻击最多的区域分别是西班牙 (94.8%)、葡萄牙 (84.5%)、荷兰 (71.9%) 和以色列 (67.1%)。值得一提的是，相比之下美国遭受的以 API 为目标的 Web 攻击仅占比 27.6%。

区域攻击情况存在差异的原因有很多，例如监管环境、地缘政治冲突、基础架构类型、入学机会和教育差异、商业模式和社会因素等。但是，还必须注意的是，您可能会发现某个网络攻击趋势最初在一个地区或行业中出现，然后又会转移到其他地区或行业。因此，我们有必要跟踪更广泛的趋势。如需了解区域级趋势的更详细讨论内容，请阅读本报告中的“亚太地区及日本概况”和“欧洲、中东和非洲地区概况”。

API 成为攻击重灾区

对攻击者攻击公司 API 的方式以及他们常用策略的研究阐明了您应当关注的防御区域。在过去 12 个月里，HTTP 协议 (HTTP)、结构化查询语言注入 (SQLi) 和数据收集攻击是攻击者青睐的一些手段（图 2）。在 HTTP 攻击中，攻击者会将各种协议中的漏洞用于恶意用途，例如读取敏感数据和欺骗客户端或服务器等。另一种常用手段是活动会话，它与可疑攻击流量在会话期间会被标记和拦截的各种情况有关。对于数据收集，顾名思义，它与搜集或收集信息相关的攻击有关，攻击者可以将收集到的这些信息用在今后的其他攻击中。（如需查看攻击媒介定义的完整列表，请参阅本报告结尾部分的附录。）

利用我们最新的数据集，我们能够监控针对 API 的更多攻击媒介。典型案例：服务器端请求伪造 (SSRF) 是我们在去年的 SOTI《钻过安全漏洞》中提到的新兴攻击媒介之一，可用于获取敏感信息或执行命令。

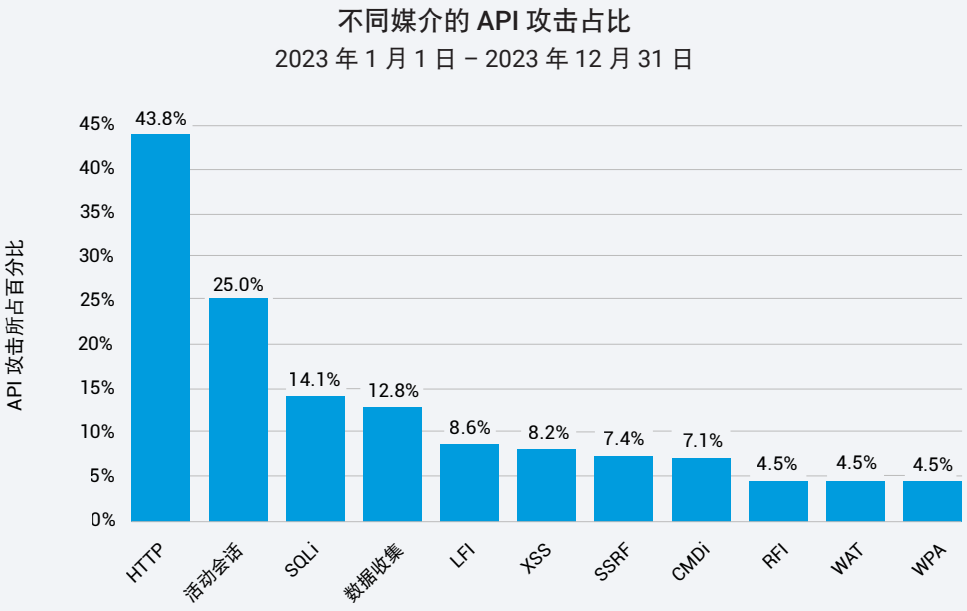


图 2：虽然本地文件包含 (LFI) 不是针对 API 的主要攻击媒介，但它仍然是一个值得关注的领域，因为它可能会被用于渗透预定目标。不过，深入了解针对 Web 应用程序和 API 的攻击分布情况后，可以发现 LFI 仍是主要攻击媒介之一

我们的研究结果还表明，爬虫程序请求是一个值得关注的领域。根据 Akamai 的数据，2023 年全球范围内几乎三分之一的可疑爬虫程序请求都以 API 为目标。虽然这些爬虫程序请求不一定都是恶意请求，但攻击者可以将它们用作攻击手段，执行可能会导致信息盗窃的撞库攻击和数据抓取。

我们强调这些类型的攻击是想说明，除了 OWASP 十大 API 安全风险、针对访问的攻击、数据滥用/抓取以及配置错误之外，企业还需要跟踪许多直接攻击并让其渗透测试团队和红队进行检测。

API 安全方面的真实经验教训

Akamai 与全球企业开展密切合作，收集与 API 使用相关的详细信息并执行高级行为分析，以识别安全漏洞和 API 滥用迹象。从 Akamai 对 API 活动的看法来说，我们通常会看到 API 活动存在两个截然不同的问题：态势问题和运行时问题。

1. 态势问题与企业 API 实施中的缺陷有关。指示态势问题的告警可帮助安全团队识别并修复高优先级漏洞，提前避免攻击者利用这些漏洞。

2. 运行时问题是需要紧急回应的主动威胁或行为。虽然这些告警通常在本质上非常关键，但与其他类型的安全告警相比，它们更隐蔽，因为它们采用了 API 滥用的形式，而不是较为明确的基础架构入侵尝试。

最常见的态势问题

下面列出了我们观察到的最常见的态势问题，并简要概述了这些问题未得到解决时对企业的潜在影响。

影子端点

影子端点是过时或旧版本的 API，它们未被停用或未进行文档记录。有时，它们指的是僵尸、恶意或旧版 API，会带来较高的利用风险，因为它们不受企业的标准安全控制措施和方法的约束。

未经身份验证的资源访问

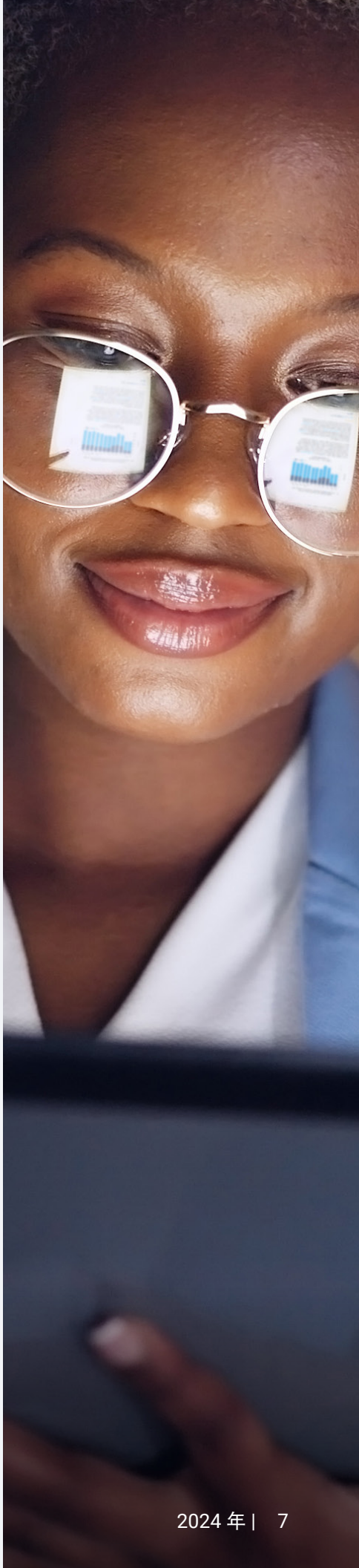
未经身份验证的资源访问是指用户或系统能够不提供任何形式的身份验证而访问 API 资源的情况，通常由 API 实施或配置中的缺陷所导致。虽然很多未经授权的资源通过隐匿被隐藏起来，但找到这些资源的攻击者可能会利用它们来访问敏感数据或应用程序功能。

URL 中的敏感数据

在某些情况下，可能会在某个 API 请求的 URL 中观察到密码、身份验证令牌、信用卡详细信息以及个人身份信息 (PII) 等敏感数据。URL 中的数据往往存储在攻击者或许可以访问的位置（例如，存储在日志和缓存中），从而会产生敏感数据泄露和合规问题等重大风险。

宽松的 CORS 策略

宽松的跨源资源共享 (CORS) 策略是指 API 允许超出必要范围的源（例如，协议、域和端口）发出访问请求。过于宽松的策略会让攻击者更容易从不受信任的来源访问敏感资源，以及更容易实施跨站脚本攻击 (XSS) 等攻击技术。



客户端错误过多
当系统观察到失败的 API 资源请求数量异常高时，就会生成客户端错误过多告警。虽然很多客户端错误是配置错误和其他非恶意错误造成的，但客户端错误过多告警可能表示攻击者正在探测 API 实施以寻找漏洞。

最常见的运行时问题

对所观察到的运行时告警执行类似的分析时，我们发现了以下代表潜在主动威胁的常见 API 安全问题。

未经身份验证的资源访问尝试
该衍生问题比上一节中所述的未经身份验证的资源访问态势告警更加紧迫。在此类问题中，我们发现攻击者未进行适当的身份验证就能够对敏感 API 资源进行明确的访问尝试。即使观察到的尝试未成功，这些情况也表明攻击者在主动尝试寻找并利用 API 漏洞。如果不进行及时干预，此尝试过程有可能最终取得成功。

JSON 属性异常
使用异常 JSON 有效负载（例如，意外数据类型、异常大小或过于复杂）的 API 活动可能表示攻击者在主动尝试利用容易受到攻击的 API。此活动可能表示攻击者在尝试执行各种恶意操作，例如注入攻击、拒绝服务、数据外泄或利用 API 逻辑缺陷。

路径参数模糊测试尝试
路径参数模糊测试是故意在 API 请求中发送意外或格式错误的数据的另一个示例，重点是 RESTful API 用于指定某些资源或操作的 URL 部分。它是攻击者用于进行侦察以发现潜在易受攻击 API 的另一种技术，可以通过数据外泄或服务中断尝试来攻击这些 API。

不可能的时间旅行
在分析 API 活动时，会出现 API 调用的时间戳、地理位置或顺序不合逻辑的情况，这表明攻击者正在尝试通过某种方式来操纵 API。此外，此行为类型有可能表示存在多种可能的威胁，例如欺诈活动中包含的数据篡改。

数据抓取

数据抓取是指以不符合 API 的预期用途和服务条款的方式和数量从 API 中自动提取数据。攻击者往往会缓慢收集此类数据以避免被检测到，并以这种方式窃取知识产权、收集敏感客户数据或获得某种好处。当攻击者在 API 内悄悄进行数据收集时，虽然是少量缓慢的数据抓取，但却可能引发大规模的数据泄露攻击。

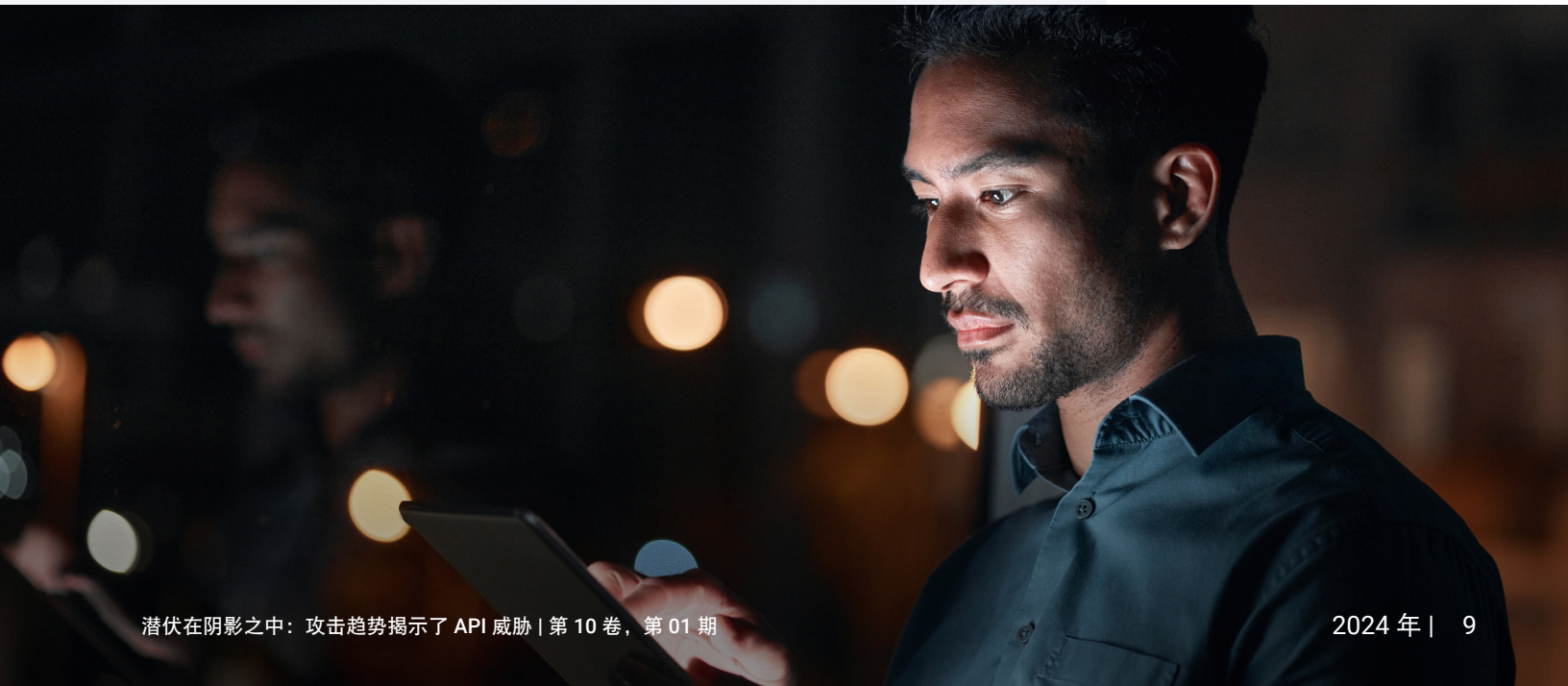
最后，当您考虑态势和运行时问题时，不妨退一步看看 API 所面临的三种其他更常见的挑战，这可能对您会有所帮助：

1. 监测能力——您是否采取了适当的流程和技术控制措施来确保自己的安全计划能够保护所有 API？这是一个关键问题，因为 API 通常是转型的一部分或嵌入到新产品中，因此许多 API 没有像传统网络业务那样的指导、保护和验证措施。

2. 漏洞——您的 API 是否遵循最佳开发做法？您是否避免了 OWASP 中最常见的编码质量不佳问题？此外，您是否在跟踪和检查漏洞？

3. 业务逻辑滥用——您是否有预期流量的基准？您是否确定了可疑活动的构成要素？

至关重要的是具备对您 API 的监测能力和进行调查的能力，以及能够建立相关流程来快速抵御威胁。不管是面向客户的 API，还是内部 API，都是如此。



行业趋势突显出供应链攻击的危险性

API 是企业数字化转型的核心。但是，API 的存在也导致企业面临的风险增加，并且带来了巨大的安全挑战。在报告期内，影响商业行业的企业的 Web 攻击中有 44.2% 以 API 为目标，紧随其后的是商业服务行业的企业，相关占比为 31.8%（图 3）。攻击者更倾向于选择商业行业是由多种因素造成的，包括其生态系统的复杂性、对 API 的高度依赖性以及存在大量机密的客户信息。

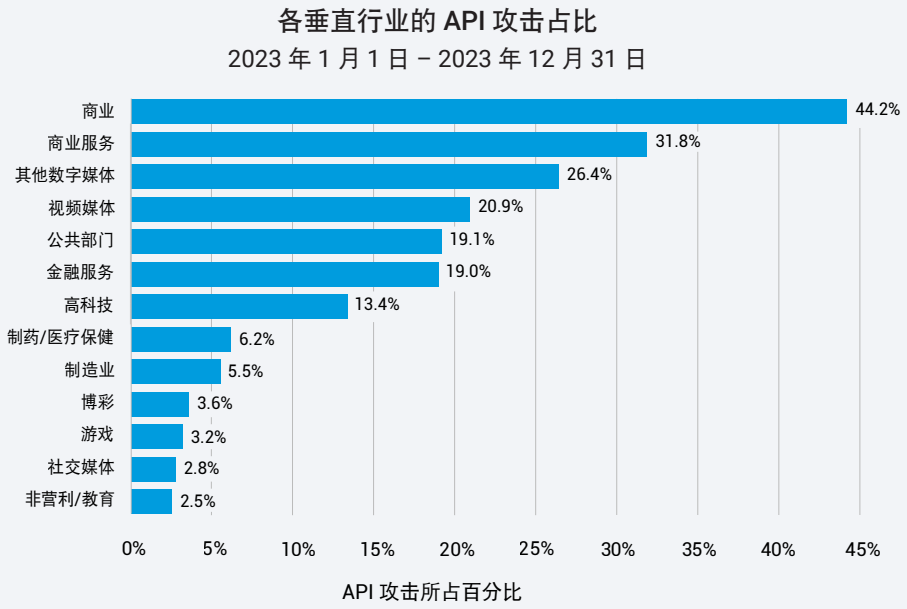


图 3：2023 年商业垂直行业和商业服务垂直行业遭受的 API 攻击占比最高。与欧洲、中东和非洲地区的金融服务业不同，美国的金融服务业尚未采用开放银行业务，因此遭受的攻击占比未进入前五名。

应当注意的是，商业服务行业位列第二的原因在于供应链攻击带来的潜在危险。提供商业服务的第三方公司可能拥有与其附属企业相关的机密信息，甚至可以访问其环境，攻击者可能会将这些用作通向高价值目标的路径。

对我们的数据进行仔细调查后发现，没有垂直行业能够免受 API 攻击。例如，医疗保健行业的医疗物联网 (IoMT) 的爆炸式增长和数据互操作性工作推动了 API 的使用。医疗保健行业正面临巨大风险，因为人们尚未完全了解 API 在该行业中产生的安全影响。

案例分析

为了让您深入了解我们所看到的针对各行各业的攻击类型，我们提供了几个案例分析，包括这些攻击对企业和客户的真实影响。

商业垂直行业的会员欺诈

欺诈者以会员帐户为目标，因为这些帐户包含可以兑换为现实世界的商品或现金的高价值货币，例如积分、里程或额度。在某个 API 上，Akamai 检测到有用户访问了五个以上的会员帐户。进行调查时，我们确认了这些帐户中的这种行为是欺诈行为。大多数帐户仅由少量的授权用户访问，因此访问多个帐户的用户可能存在滥用行为。为了帮助减少欺诈，最好了解清楚正常行为与滥用行为之间的区别。

SaaS 通知服务中的 API 滥用

Akamai Hunt 团队在属于某个金融服务公司的软件即服务 (SaaS) 通知系统中发现了 API 滥用问题。有效负载内缺少授权标头和签名，这会阻止该公司检查在系统中发出请求和发送通知的人员。因此，有权使用该 API 的任何人都可能滥用它向公司员工和客户发送消息。

潜在的 BOLA 攻击

我们的团队在某个航空公司中发现了潜在的失效对象级授权 (BOLA) 攻击，其中来自近 200 个 IP 地址的已验证用户模糊了 {customer_id} 路径参数，这会在所提供参数有效的情况下返回敏感的用户信息（图 4）。由于此 ID 是一个简单的整数，参数模糊非常容易，但会造成破坏性影响，因为这会导致客户信息泄露。目标 API 会返回敏感信息，例如名字、中间名、姓氏以及有效身份证、国籍、居住的国家/地区和出生日期。

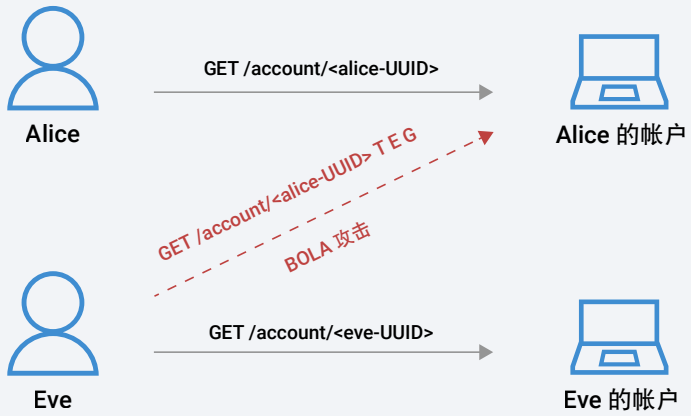


图 4：当攻击者尝试访问他们无权访问的资源来窃取敏感数据时，便会发生 BOLA 攻击

堂而皇之地隐藏起来的盗刷攻击

在另一个案例中，最初是异常的 API 流量，结果却是盗刷攻击。最初，受影响的企业认为 API 流量激增是分布式拒绝服务 (DDoS) 活动造成的。但是，经过仔细检查后可以确定，该攻击试图验证信用卡，而客户系统会以 true 或 false（即，有效或无效）来作出响应。在盗刷攻击中，攻击者会验证被盗信用卡卡号。一旦验证成功，他们会在暗网市场中出售该信息，或者进行其他欺诈交易。

为何必须了解 API 攻击

在大多数 API 环境中，常见的业务问题为编程错误或配置错误，这些错误可在 API 安全计划成熟化过程的发现阶段检测到。虽然这些错误中的大多数从未遭到利用，但是在安全团队深入了解 API 资产及每个 API 上运行的流量后，潜在的损害显而易见。

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态势评估的速度更快。这似乎会不可避免地导致配置错误和漏洞。除此之外，大多数企业内部缺乏 API 安全方面的专业知识，因此使得难解的安全问题变得更加扑朔迷离。

> **API 的安全性出现问题的原因**
>
> 使用 API 的关键业务流程的快速部署 + 缺乏对 API 的监测能力 = 错误配置或易受攻击的 API

防止数据泄露的最佳实践

随着时间推移而遭到利用的未知 API 漏洞通常与编程错误密切相关。如今，涉及 API 的公开数据泄露事件已经司空见惯，这表明攻击者现在会探索 API 资产并进行侦察来识别要利用的特定 API。这种探索以及数据抓取带来的自动化威胁意味着 API 成为了新的数据泄露攻击媒介。如果攻击者成功实施此类攻击，所产生的后果包括品牌和声誉受损、机密数据丢失和客户信任丧失，以及可能会造成经济损失的合规问题和法规问题（具体取决于您所在的地区）。因此，API 安全比以往更重要。

API 数据泄露的条件

生产环境中错误配置或易受攻击的 API + 数据抓取自动化威胁（爬虫程序） = 持续数周或数个月的少量缓慢的数据泄露

防范通过 API 漏洞进行数据泄露的第一个关键方面是，监控您的环境并了解什么是正常情况以及哪些 API 中包含哪些数据。这包括实施安全控制措施来约束所有 API，并实施自动响应以抵御攻击或向安全运营团队发出告警。接下来，在开发阶段进行左移测试可以从一开始就解决掉漏洞和薄弱环节，从而避免它们被攻击者利用。最后，您需要进行演练，对预防措施和危机应对措施进行验证。

Kong 分析人员于 **2023 年**参与的一项研究表明，“API 攻击…目前在美国造成的损失为 106 亿美元。到 2030 年，这一数字将飙升至每年 1980 亿美元。”

合规考虑因素

从传统的企业安全和风险管理角度来看，保护 API 并阻断这些作为新攻击媒介的入口点势在必行。近期与安全和数据保护相关的法律和执法趋势发生了变化，这为解决 API 安全和监测能力问题提供了更多令人信服的理由。

安全始终是全世界数据保护法律中的重要组成部分——没有良好的安全保障便无法实现良好的隐私性。例如，欧盟《通用数据保护条例》(GDPR) 第 32 条规定，处理 PII 的实体“应当采取适当的技术和组织措施来确保其安全水平足以应对相关风险”。《加州隐私权法案》(CPRA) 等其他法律也包含了类似的规定，要求实施“合理的安全程序和做法”以及采取适当措施来保护 PII 的机密性、完整性和可用性。

监管和执法行动同样提高了透明度和问责制的标准。例如，美国证券交易委员会 (SEC) 近期颁布了针对上市公司的一些新规则，要求披露重大安全事件以及与风险、安全治理和监督相关的详细信息。

放眼全球，未能保护 PII 的公司都会面临罚款处罚。例如，SEC 最近对 SolarWinds 的首席安全信息官提起了诉讼，指控其在已知的网络安全风险和漏洞方面存在欺诈行为并未能实施内部控制。该诉讼称，SolarWinds 及其首席安全信息官通过夸大该公司的网络安全实践并低估或未能披露已知风险来欺骗投资者。

因此，虽然很少有专门针对 API 的法律或法规，但很多法律法规都提到了 API 或要求各公司必须遵守相关要求。例如，欧盟的《修订支付服务指令》(PSD2) 和美国的《21 世纪治愈法案》都在推动实施医疗保健服务提供商使用 API 时必须遵守的透明度要求。所面临的挑战在于，涉及的数据既受到严格监管，又容易成为网络犯罪分子的目标。这促使美国国家标准协会 (ANSI)、国际标准化组织和国际电工委员会等组织制定了相关指导原则 (ISO/IEC 27001)。支付卡行业数据安全标准 (PCI DSS) v4.0 等新法规也对 API 提出了相关要求。在技术方面，开放式 Web 应用程序安全项目 (OWASP) 是进行培训时的理想参考资源。结论：构建一个可以进行发现、监控、调查和修复的系统，您将能够满足合规要求。

随着这些采取法律行动的趋势尝试提高网络安全计划的标准，透明度和问责制也必须继续向更高要求迈进。如果公司缺乏对 API 领域的监测能力，那么与此相关的风险以及安全态势中的相应漏洞可能会带来严重的法律和法规问题，因为您无法保护自己看不到的东西。

如需详细了解亚太地区及日本 (APJ) 以及欧洲、中东和非洲地区 (EMEA) 地区的 API 攻击趋势，请参阅后续部分中的区域报告。

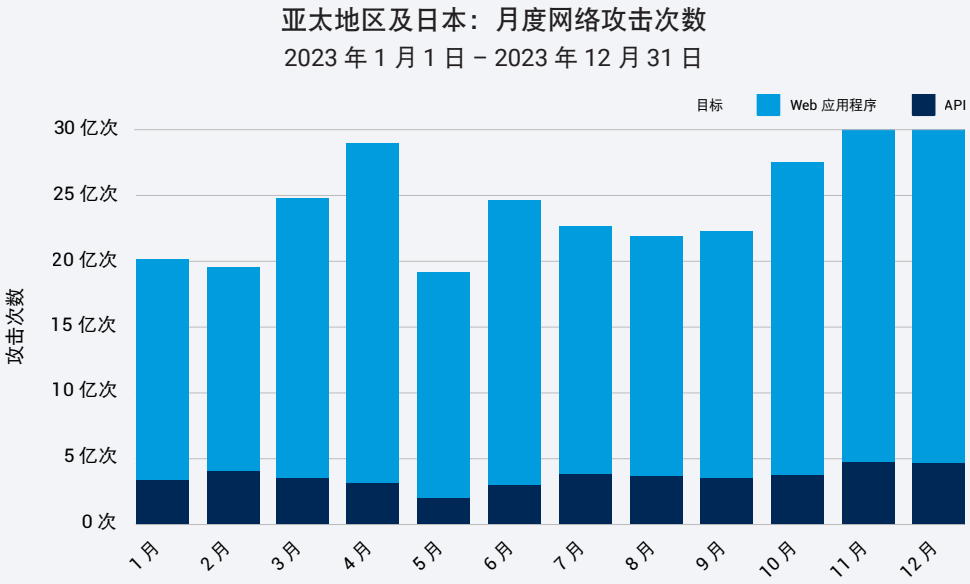
亚太地区及日本概况

《亚太地区及日本概况》是我们更全面的 API 安全性 SOTI 报告《潜伏在阴影之中：攻击趋势揭示了 API 威胁》（仅提供英文版）的姊妹篇。请阅读该报告，详细了解攻击者如何利用本期概况介绍中所描述的攻击媒介发起攻击，同时获取有关如何保障贵企业安全的建议以及对我们研究方法的深入说明和新的数据集。

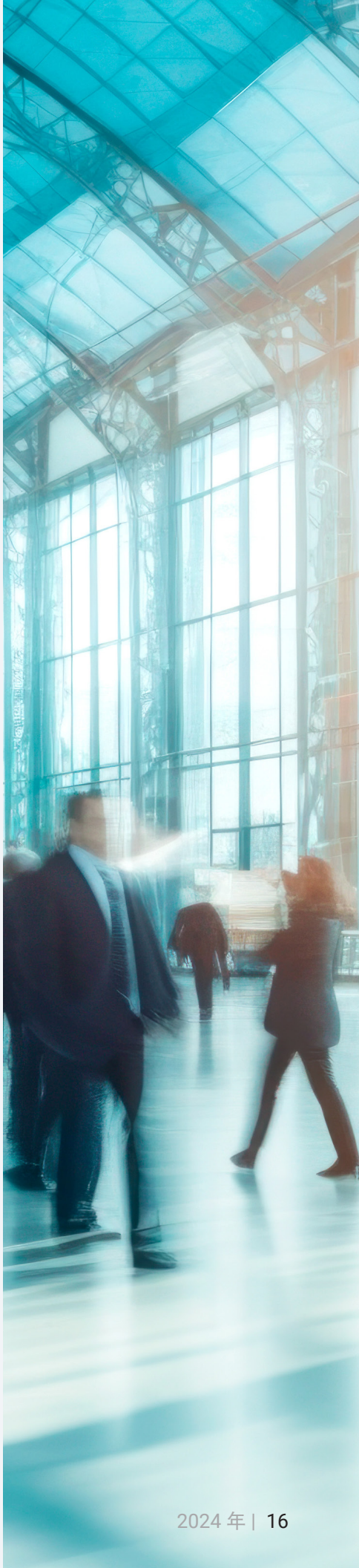
亚太地区及日本的 API 攻击值得关注

在利用专门跟踪 API 攻击流量的新数据集进行分析之后，Akamai 研究发现，亚太地区及日本 (APJ) 遭受的所有 Web 攻击中有 15.0% 是针对 API 发起的。在全球范围内，亚太地区及日本 (APJ) 受到的 API 攻击占比位列第三，仅次于欧洲、中东和非洲地区 (EMEA) 地区的 47.5% 和北美地区的 27.1%。

在 2023 年 1 月至 12 月的报告期间内，每个月针对 API 发起的 Web 攻击数量在 11% 至 21% 之间波动（APJ 图 1）。这一攻击百分比之所以低于其他地区，也许可部分归因于亚太地区及日本的开放 API 市场规模相比欧洲和北美较小，因而企业对 API 的采用率也较低。



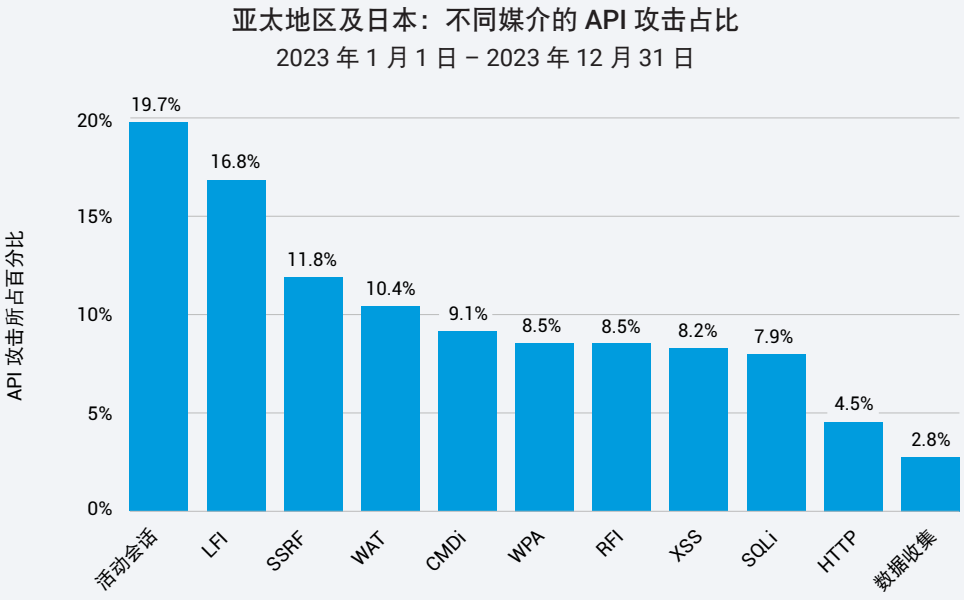
APJ 图 1：即使整体 Web 攻击数据有所增加，以 API 为目标的攻击数量仍然达到 15.0% 的平均占比



在亚太地区及日本，以 API 为目标的 Web 攻击占比最高的国家/地区依次为韩国 (47.9%)、印度尼西亚 (39.6%)、中国香港特别行政区 (38.7%)、马来西亚 (26.4%)、日本 (23.4%)、印度 (19.0%)、澳大利亚 (15.6%)、新加坡 (5.8%)、菲律宾 (5.5%) 和新西兰 (4.8%)。

API 成为攻击重灾区：流量分析

正如我们之前报告中关于整体 Web 攻击的分析所述，LFI 仍然是亚太地区及日本面临的主要 API 攻击媒介。但是，跨站点脚本攻击 (XSS) 和结构化查询语言注入 (SQLi) 相较 API 攻击的排名有所下降（APJ 图 2）。



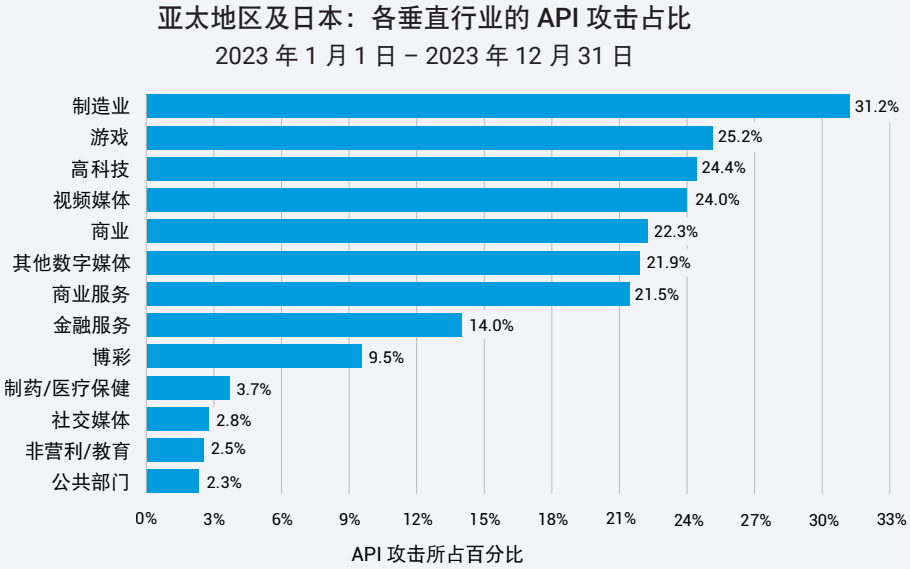
APJ 图 2：LFI 仍然是一种主要攻击媒介，而我们的新数据集也揭示了其他颇受青睐的 API 攻击手段

新的数据集能够帮助我们发现其他颇受青睐的 API 攻击媒介。例如，命令注入 (CMDi) 是一种很受欢迎的 API 攻击技术，而我们在 2023 年报告中讨论过的服务器端请求伪造 (SSRF) 现在也成为了最常用的攻击媒介之一。值得注意的是，活动会话会指出该会话期间的可疑行为，从而导致发生临时阻止。（如需查看攻击媒介定义的完整列表，请参阅全球报告结尾部分的附录。）

我们的研究还表明，爬虫程序请求是一个值得关注的领域。在同样的 12 个月报告期内，超过 2 万亿次的可疑爬虫程序请求中有 40% 以 API 作为攻击目标。

API 攻击遍布各行各业

在报告期内，Akamai 研究人员发现，制造业受到的以 API 为目标的整体 Web 攻击占比最高，达到 31.2%，随后依次是游戏行业 (25.2%)、高科技行业 (24.4%)、视频媒体行业 (24.0%) 和商业 (22.3%)（APJ 图 3）。



APJ 图 3：制造业遭受的 API 攻击占比最高，部分原因在于这一关键基础设施行业通过 API 建立的连接越来越多，并且供应链中断的可能性也较高

亚太地区及日本概况的相关结论

从安全和风险管理的角度来看，API 的防护迫在眉睫。此外，除了现行的法律法规之外，新推进的改革也要求网络安全立法跟上威胁形势的变化步伐，这都使保护 API 变得势在必行。

例如，印度正在起草《数字印度法案》，该法案将是对《信息技术法案》的一次重大修订，第一项举措就是于 2023 年 8 月通过了《数字个人数据保护法案》。澳大利亚于 2023 年 11 月 23 日发布了《2023-2030 年澳大利亚网络安全战略》，其中一个重点就是确保技术安全、增强对数字产品和软件的信任。此外，在即将发布的《支付卡行业数据安全标准》(PCI DSS) 4.0 版的第 6 节中，特别包含了关于在系统和软件的开发及维护中使用 API 的标准，以降低违规风险。

随着 API 越来越广泛地用于交换敏感财务信息，监管机构也正在制定相关举措和政策以加强 API 的网络安全标准。了解最佳实践和指导原则非常重要，这样您就可以将 API 纳入到自己的安全计划中，从而提高监测能力、加强防御措施并遵循合规要求。

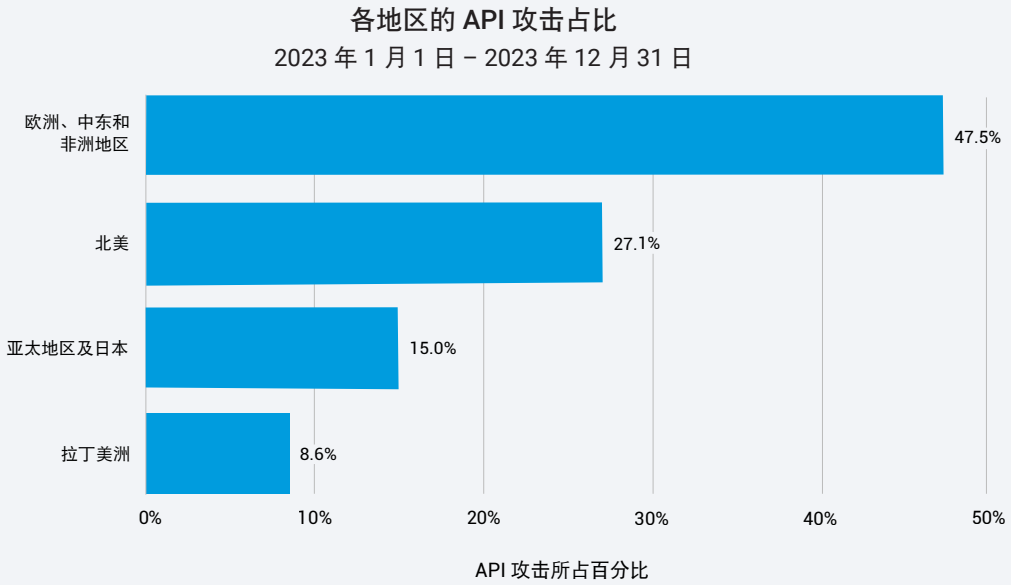
如需了解更多信息，请参阅全球 API 安全性 SOTI 报告《潜伏在阴影之中：攻击趋势揭示了 API 威胁》。

欧洲、中东和非洲地区概况

《欧洲、中东和非洲地区概况》是我们更全面的 API 安全性 SOTI 报告《潜伏在阴影之中：攻击趋势揭示了 API 威胁》（仅提供英文版）的姊妹篇。请阅读该报告，详细了解攻击者如何利用本期概况介绍中所描述的攻击媒介发起攻击，同时获取有关如何保障贵企业安全的建议以及对我们研究方法的深入说明和新的数据集。

欧洲、中东和非洲地区盛行的 API 攻击

在利用专门跟踪 API 攻击流量的新数据集进行分析之后，Akamai 研究发现，全球范围内欧洲、中东和非洲地区 (EMEA) 地区遭受的 API 攻击占比最高 (47.5%)，远高于排名第二的北美地区 (27.1%)（欧洲、中东和非洲，图 1）。此数据基于每个地区的 Web 攻击总数，并表明欧洲、中东和非洲地区的 API 比其他地区面临更多危险。



欧洲、中东和非洲地区，图 1：欧洲、中东和非洲地区的 API 遭受的 Web 攻击显著高于任何其他地区

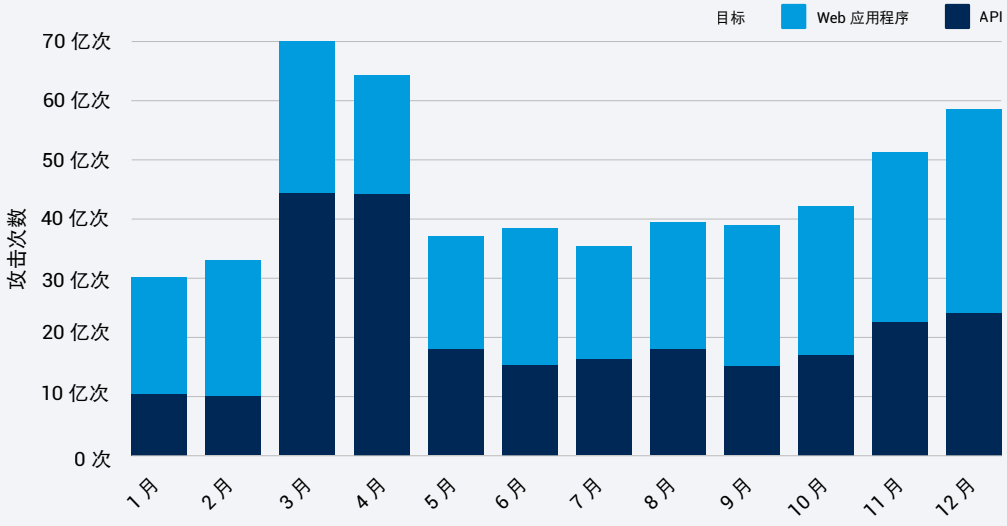
欧洲、中东和非洲地区的攻击占比之所以相对较高（与其他地区的攻击占比进行比较时），也许一部分原因在于这个地区的开放 API 市场规模相比北美和亚太地区较大，这反映出此地区的 API 采用率更高，而另一部分原因在于开放银行业务和支付卡行业数据安全标准 (PCI DSS) 4.0 版，它们促进了 API 的使用并且会带来全球报告中所讨论的安全风险。

在欧洲、中东和非洲地区，以 API 为目标的 Web 攻击占比最高的几个地区依次是西班牙 (94.8%)、葡萄牙 (84.5%)、荷兰 (71.9%) 和以色列 (67.1%)。这并不是说这些国家的 Web 攻击总数比欧洲、中东和非洲地区的其他国家更高，而是说由于攻击者重点关注此攻击媒介，这些国家面临的 API 滥用风险更加集中。

2023 年 1 月到 12 月的报告期内的月度趋势表明，以 API 为目标的 Web 攻击在欧洲、中东和非洲地区的增长相当稳定，从 1 月份的 34% 增长到年底的 41%（欧洲、中东和非洲地区，图 2）。例外情况出现在 3 月和 4 月，当时 Akamai 研究人员发现 API 攻击数量激增，因为在 API 攻击集中度很高的西班牙，商业行业遭遇了大规模的集中攻击。此激增情况表明了攻击者在地区和行业之间转移注意力的速度有多快，因此值得跟踪更广泛的趋势。

欧洲、中东和非洲地区：月度网络攻击次数

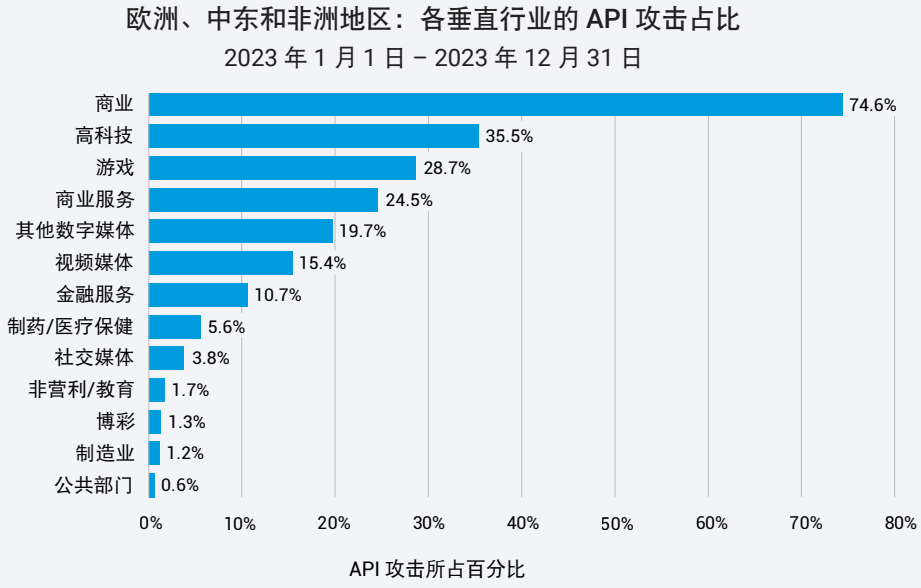
2023 年 1 月 1 日 – 2023 年 12 月 31 日



欧洲、中东和非洲地区，图 2：3 月和 4 月出现例外情况，当时的 API 攻击数量激增，而整个 2023 年 API 攻击数量呈现缓慢增长，到年底在全部攻击中的占比增长至 41%

API 攻击遍布各行各业

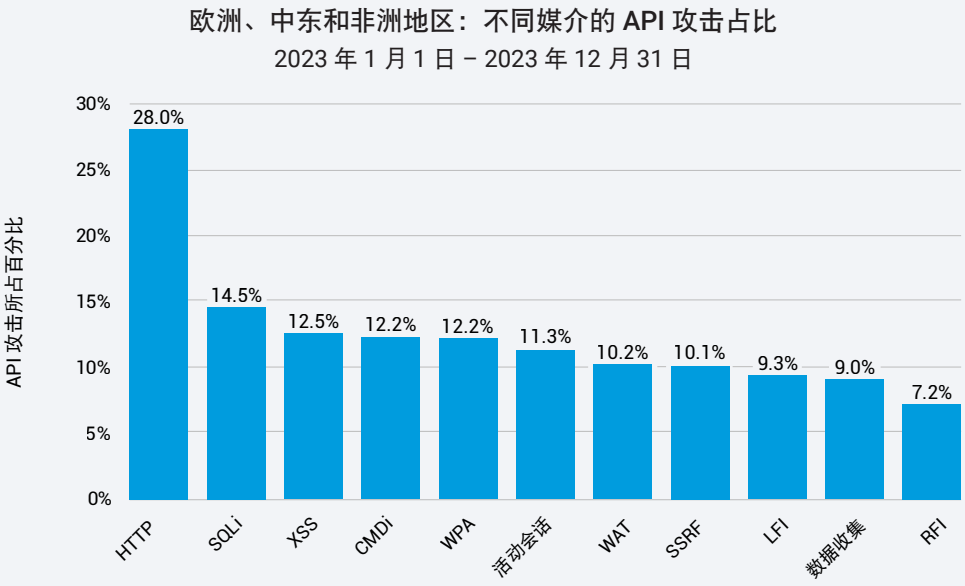
在报告期内，Akamai 研究人员发现，在影响企业的全部 Web 攻击中，商业行业遭受的 API 攻击占比最高 (74.6%)，超过了位居第二的高科技行业 (35.5%) 的两倍。紧随其后的分别是游戏行业 (28.7%)、商务服务行业 (24.5%) 和其他数字媒体行业 (19.7%)（欧洲、中东和非洲地区，图 3）。



欧洲、中东和非洲地区，图 3：商业垂直行业的 API 攻击占比最高，部分原因在于其生态系统的复杂性、其对 API 的高度依赖性以及此行业中的企业拥有的高价值数据

API 成为攻击重灾区：流量分析

与全球趋势一致的是，过去 12 个月里，HTTP 协议 (HTTP) 和结构化查询语言注入 (SQLi) 已成为攻击者对欧洲、中东和非洲地区的 API 发动攻击的主要方式，而对于本地文件包含 (LFI)，虽然它仍然在 Web 应用程序攻击中占据主导地位，但在本列表中的排名进一步下降（欧洲、中东和非洲地区，图 4）。



欧洲、中东和非洲地区，图 4：HTTP、SQLi 和 XSS 是与 API 攻击相关度最高的三种攻击媒介；对于 API 攻击来说，LFI 不再是主要的攻击媒介，但攻击者仍然会在针对 Web 应用程序的攻击中积极使用该媒介

在欧洲、中东和非洲地区，跨站点脚本攻击 (XSS) 仍然是攻击者青睐的一种技术，即便对于 API 攻击也是如此，并且命令注入 (CMDi) 也是主要攻击媒介之一。利用新数据集，我们能够监控 API 中的更多攻击媒介。例如，我们在 2023 年报告中讨论过的服务器端请求伪造 (SSRF) 是现在新出现的一种攻击媒介。（如需了解攻击媒介定义，请参阅全球报告结尾部分附录。）

我们的研究还表明，爬虫程序请求是一个值得关注的领域。在同样的 12 个月报告期内，将近 4 万亿次的可疑爬虫程序请求中有 40% 以 API 作为攻击目标。

欧洲、中东和非洲地区概况的相关结论

从安全和风险管理的角度来看，API 的防护迫在眉睫。此外，除了现行的法律法规之外，新推进的改革也要求网络安全立法跟上威胁形势的变化步伐，这都使保护 API 变得势在必行。

例如，欧盟的《通用数据保护条例》(GDPR) 注重对个人数据的保护，而现在 API 在如何使用和共享此类数据方面处于重要位置。此外，新的《网络和信息安全指令》(NIS2) 专门要求制定强有力的 API 安全计划。欧盟之外的国家/地区（例如，沙特阿拉伯）已出台类似于 GDPR 的数据保护法律，它们规定了处理个人数据的实体的相关义务。此外，在即将发布的《支付卡行业数据安全标准》(PCI DSS) 4.0 版的第 6 节中，特别包含了关于在系统和软件的开发及维护中使用 API 的标准，以降低数据泄露风险。

随着监管机构制定相关举措和政策以加强 API 的网络安全标准，必须了解最佳实践和指导原则，这样您就可以将 API 纳入到自己的安全计划中，从而加深了解、加强防御措施并遵循合规要求。

如需了解更多信息，请参阅全球 API 安全性 SOTI 报告《潜伏在阴影之中：攻击趋势揭示了 API 威胁》。

提升监测能力：企业 API 资产一年回顾

在本报告的开头，我们提到了缺乏对 API 的监测能力所带来的危险，并强调了企业通过安全告警获得的一些见解。在本部分中，我们将展示采用强有力的 API 安全计划如何让您实现不同层次的监测能力，包括：

- **发现**——了解企业内部的 API 清单
- **风险审计**——了解发现的每个 API 的风险状况
- **行为检测**——了解正常使用与异常滥用的区别，以检查每个 API 上的主动威胁
- **调查和威胁搜寻**——了解由专业人工威胁搜寻人员发现的潜伏在 API 资产内部的威胁

这些监测能力层次不是 API 特有的，但我们发现，由于 API 的快速部署，很多 API 的网络安全完善程度都比不上更成熟的 IT 基础架构。问题是很多 API 都包含可以被利用的敏感数据。与我们合作的企业会对其 API 足迹应用更复杂的 API 安全实践，当这些企业更详细地了解其 API 活动并开始查看态势告警和运行时告警时，他们通常会遵循一种通用模式。

1. **通过监测能力找到 API**

   “您无法保护自己看不到的东西”是一句古老的谚语，但它同样适用于现在的 API。对于很多提升其 API 活动监测能力的企业来说，最大的意外发现之一是自己的环境中竟然存在如此之多正在运行而未被发觉的影子端点。当恶意 API 或僵尸 API 被发现时，安全团队都会心怀感激之情，因为这让他们发现了隐藏的威胁。通常，API 安全完善之旅的第一步是系统性地发现这些影子 API，并确保每个此类 API 已停用或者进行了正式的文档记录，而且已纳入企业的 API 安全控制措施之中。这有助于直接降低意外 API 滥用的风险并减少其他威胁。通常，我们会在部署 API 安全工具时看到告警数量激增，但随着时间推移，会出现更多的非受管或未授权 API，于是我们便开始发现流程中的漏洞。

2. 做到有条不紊

解决影子 API 的问题后，在对经批准 API 的清单进行合理规划和整理方面仍然有工作要做。这包括按开发、测试和生产等宽泛类别进行细分，以及建立层次结构来确保安全告警和分析有适当的上下文，以便团队了解与 API 相关的风险。

对每个 API 进行文档记录是提升监测能力过程的下一步。利用文档，安全团队可以更高效地应对态势告警，因为文档可以将告警带入上下文中，并使告警与他们对应用程序、API 和业务流程的思考方式保持一致。只有制定了活动程度的基准，才能轻松地判断哪些是可疑的活动。

3. 强化 API 态势

企业收到的第一波态势和运行时告警往往会告知一组对其 API 实施的高优先级更改。例如，安全团队通常会查看其最常见的告警类型，并确定相关策略和优先级以降低风险。这包括更正 API 代码中的缺陷并解决配置错误问题，以及在吸取经验教训的基础上实施预防未来漏洞的流程。这将有助于划分渗透测试验证计划的优先顺序，并且可能会告知管理层必要的编码最佳实践，以避免今后出现漏洞。

4. 加强威胁检测和响应

虽然前三个步骤通常会使 API 安全告警的总数呈现总体下降趋势，但随着时间推移，我们偶尔也会看到此数量出现激增。这些激增可能是内部驱动因素引起的，例如对业务模式的广泛更改、获得新功能，或者 API 足迹的增加带来新的漏洞或恶意系统。此外，激增也可能是外部因素引起的，包括攻击者进行的攻击尝试。高效的企业会针对这些激增制定计划，并在出现激增时采取明确的响应程序，将风险和告警数量降至正常水平。他们也会采取措施来持续缩短对主动 API 威胁进行响应、调查、限制以及从中恢复所需要的时间。这可能需要新的技能，具体取决于 API 环境。

5. 制定更强的防御策略

   随着企业增强其防御性 API 安全措施，下一个阶段是采取进攻性方法来实施 API 威胁发现和抵御，以完善防御性措施。这包括制定正式的 API 威胁搜寻准则和节奏，目的是在可能的威胁升级为被动情况之前尽早识别它们。这可能难以实现，因为它需要高度专业化的人才以及将资源与中断驱动型任务相隔离的能力。出于此原因，一些企业会聘请第三方服务提供商（包括 Akamai）来实现此重要功能。

图 5 中的匿名示例说明了我们的一位企业客户因此所获得的好处。在 1 月和 2 月，由于该企业采取了一些措施来消除影子 API、开展整顿并对其 API 安全态势进行一些初步改进，威胁风险开始下降。在对 API 资产进行更改时，我们观察到态势告警偶尔会出现峰值。通过其 API 监测能力，该客户快速解决了可能的漏洞，没有让它们继续存在。

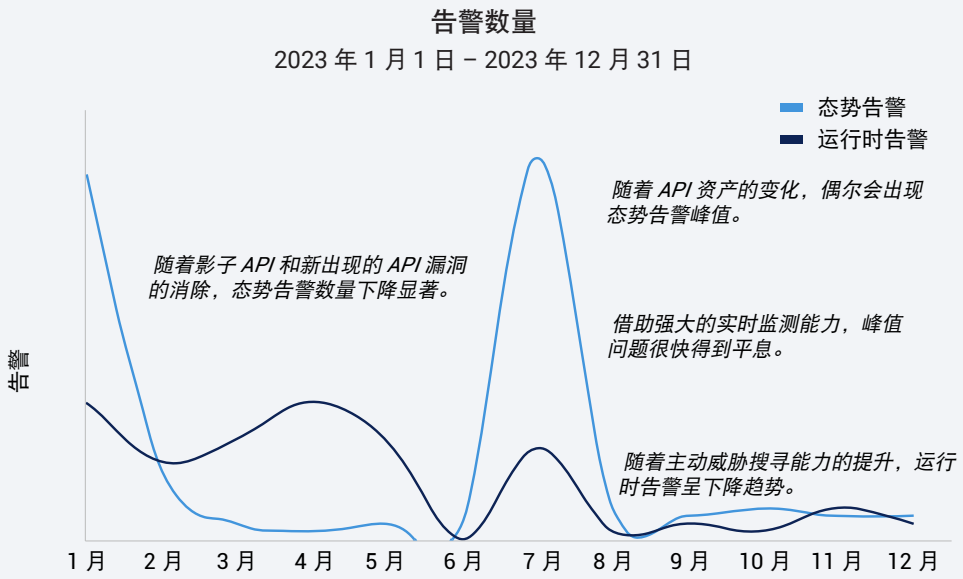


图 5：企业在拥有对 API 环境的监测能力后，API 资产的波动情况便会一目了然，而且告警数量也显著减少

运行时告警数量的可预测性较低，因为它是由外部因素驱动的。但是，也能观察到该数量普遍下降，因为该企业增强了其整体安全态势并提升了主动威胁搜寻能力。

我们的结论是，保护 API 不只是 IT 团队的责任。这可能需要新的工具和技能，具体取决于数据敏感度所决定的潜在 API 风险暴露情况。随着新工具的部署，API 防御也成为了负责人需要关注的领域。他们应当针对该领域考虑技能组合和人员需要，并且在很多情况下应当考虑重新分配工程时间或转向托管服务。总体而言，需要跟踪和分析网络安全针对 API 提供支持的工作量，以找出效率低下的情况。

保护 API 领域

API 是众多公司正在构建的很多新功能的基础。但在大多数情况下，这些公司要么没有在规划过程中尽早考虑 API 安全，要么其 API 安全水平跟不上新技术的快速部署步伐。因此，在探讨如何制定有效的安全计划时，我们会引用我们很喜欢的网络安全专家灰胡子 Bruce Schneier 的一句话：“当危险来临时，你可能会猝不及防。所以，你唯一能做的就是及早检测和从容应对”。这一理念应当促使我们专注于培养更强的环境感知能力。我们应确保将所有 API 纳入我们的安全计划中，并确保我们主动对其进行攻击、漏洞和滥用监控。我们的渗透测试和红队应该测试身份验证和公开数据的态势，以及 JSON 属性和抓取等运行时问题。这些测试应构建为紫队演习，在这些演习中，安全信息和事件管理团队以及安全运营中心需要验证他们是否检测到攻击并且是否实施了最新流程来减轻相关影响。我们在本报告中回顾的案例分析（会员欺诈和盗刷攻击等）是用于测试计划的理想模板。

我们应当使用与编码实践相关的 OWASP 指导来阻止常见攻击。这些主动控制措施以及围绕发现、强化、检测和响应制定有效流程的行动号召，都是制定季度行动计划的重要基础。

我们还必须考虑合规问题。虽然现在 API 方面的法律/法规不多，但我们应当利用很多最佳实践和标准来确保我们正在采取正确的措施来保护自己的客户。GDPR 等现行法规包括与 API 相关的规定，PCI DSS v4.0 等新标准也提到了 API，并且 ANSI 等组织将发布相关指导原则。

本报告的依据包括我们已抵御的威胁流量，以及我们从客户身上学习到的最佳实践。此外，在我们与客户进行沟通互动时，客户不断告诉我们安全控制措施在少数平台上的整合价值、灵活的人员解决方案对于满足转型目标的必要性，以及监测能力对决策和性能评估的重要意义。我们希望这份报告中的数据能够提供相关见解和可见性，帮助您更新自己的计划并开发最佳实践来保护您的客户。

敬请访问我们的安全研究中心，随时了解我们的最新研究资讯。

方法

Web 应用程序和爬虫程序攻击

这些数据表示通过我们的 Web 应用程序防火墙 (WAF) 和爬虫程序管理工具观察到的流量的应用层告警数量。如果在针对受保护的网站、应用程序或 API 的访问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。如果在针对受保护的网站、应用程序或 API 的访问请求中检测到爬虫程序负载，系统就会触发爬虫程序告警。恶意和良性爬虫程序都可能触发此类爬虫程序警报。警报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 Connected Cloud 上检测到的安全事件。Akamai Connected Cloud 是一个全球性网络，在 130 多个国家/地区拥有 4,000 多台边缘服务器。我们的安全团队使用这些数据（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。

该报告中的数据涵盖了从 2023 年 1 月 1 日到 2023 年 12 月 31 日的 12 个月时间段。

2024 年数据更新

值此 10 周年庆之际，我们很高兴地宣布对数据集做出的一些更新！我们的 Web 应用程序和爬虫程序攻击数据集已经进行了数次升级。每种数据的收集方式都进行了革新、精简和优化。我们的见解在广度和深度上都得到了扩展。另外，我们还增加了其他攻击媒介（例如 SSRF）的分类。以 API 端点为目标的攻击识别也已加入到每个数据集。我们很高兴在本期报告中强调其中的部分新改进，并且期待在今年及以后继续分享这些更新，与读者一起庆祝《互联网现状/安全性》发展的这一里程碑。

Akamai API Security 见解

特别感谢 Akamai API Security 解决方案工程团队，他们在帮助了解 API 风险方面做出了具有现实意义的贡献，并且还有可能通过我们的 API Security 告警发挥重大影响。

附录

攻击媒介	定义
活动会话	已为客户端标记出攻击流量，并且重复请求将在会话持续期间被阻止
命令注入 (CMDi)	攻击者在现有命令中注入新的项目，以修改解释并使其偏离预期，转向他们选择的行动
跨站点脚本攻击 (XSS)	攻击者在内容中嵌入恶意脚本，以便在向 Web 浏览器提供内容时，使目标软件以用户的权限级别执行脚本
数据收集	攻击者利用攻击目标在设计或配置以及通信上存在的弱点，使其披露比预期更多的信息；此类攻击的目的通常是收集数据以准备实施另一种类型的攻击，但获取信息的访问权也有可能是攻击者的最终目标
HTTP 协议 (HTTP)	攻击者利用客户端与服务器之间的通信协议中存在的弱点，企图执行非预期的操作；对不同协议类型的攻击可能存在不同的最终攻击目标
本地文件包含 (LFI)	攻击者操纵对目标软件的输入，企图获取文件系统中原本不可访问的区域的访问权，或者可能试图对其进行修改

攻击媒介	定义
远程文件包含 (RFI)	攻击者加载并执行远程任意代码，随后劫持目标应用程序并迫使其执行自己的指令
服务器端请求伪造 (SSRF)	攻击者滥用服务器的功能，企图读取或更新内部资源
结构化查询语言注入 (SQLi)	攻击者伪造输入字符串，以便当目标软件打算基于用户输入构建 SQL 语句时，使生成的 SQL 语句执行攻击者想要的操作；成功的注入攻击可能会导致信息泄露，并且能够在数据库中添加或修改数据
Web 攻击工具 (WAT)	攻击者主动探测目标，企图获取可能被用于实现恶意目标的信息；通过此类探测行为，攻击者能够从目标获得信息，帮助其针对目标的安全性、配置或潜在漏洞进行推断
Web 平台攻击 (WPA)	以软件平台（云、Web 或应用层）为目标进行的攻击；此类攻击并未纳入其他的攻击组别当中

Akamai

致谢名单

编辑与创作

Badette Tribbey——总编辑
Charlotte Pelliccia——主笔人（地区）

编辑人员

James Casey
Edward Roberts
Steve Winterfeld

审稿和主题撰稿

Tom Emmons
Reuben Koh
Rob Lester
Richard Meeus
Abigail Ojeda
Menachem Perlman
Yariv Shivek

数据分析

Chelsea Tuttle

营销与发布

Georgina Morales Hampe
Emily Spinks

进一步阅读《互联网现状/安全性》报告

《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

进一步查看 Akamai 威胁研究

请前往以下网址，了解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

访问此报告中的数据

查看本报告中引用的图片和图表的高画质版本。这些图片可供免费使用和引用，但必须注明转载来源，并保留 Akamai 徽标。
akamai.com/sotidata

进一步探索 Akamai 解决方案

如需详细了解 Akamai 针对 API 攻击推出的解决方案，请访问我们的**“应用程序和 API 安全”页面**。

Akamai

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 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 3 月。