SOTI

第 10 卷，第 4 期

10 YEARS
OF SECURITY INSIGHT

现代应用程序架构面临威胁

亚太地区及日本概况

Akamai

互联网现状/安全性

目录

报告的关键见解

《亚太地区及日本概况》是我们更全面的安全应用程序 SOTI 报告《数字堡垒受到围攻：现代应用程序架构面临威胁》（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日益扩大的攻击面发起攻击，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说明。

概述

在过去二十年里，Web 应用程序在数量和功能上呈指数级增长，不仅简化了业务运营，改进了客户体验，还通过实时通信、数据分析和流程自动化等功能推动企业实现了增长。作为应用程序间通信基石的 API 也得到了蓬勃发展，现在有望迎来指数级增长。

应用程序几乎深入到了企业的方方面面，它们让数万亿的连接变得更容易，但也给攻击大开方便之门。在本期《亚太地区及日本概况》中，我们将以 2023 年 1 月到 2024 年 6 月为时间跨度，全面分析影响应用程序的各类威胁，包括网络攻击、分布式拒绝服务 (DDoS) 攻击以及对关键工作负载的威胁，并重点介绍它们对您的影响。

从 2023 年第一季度到 2024 年第一季度，亚太地区及日本 (APJ) 针对应用程序和 API 的网络攻击增长了 65% 并且愈演愈烈，于 2024 年 6 月达到 48 亿次攻击的峰值。在该地区中，金融服务和商业行业遭受的网络攻击最多，这与上一期报告的情况一致。

亚太地区及日本遭受的第 7 层 DDoS 攻击增长了五倍，在此期间的攻击总数达到了 5.1 万亿次，仅次于北美地区。社交媒体是受影响最大的行业，由于地缘政治事件和紧张局势，黑客行动和民族国家相关攻击者导致针对该行业的第 7 层 DDoS 攻击增加。

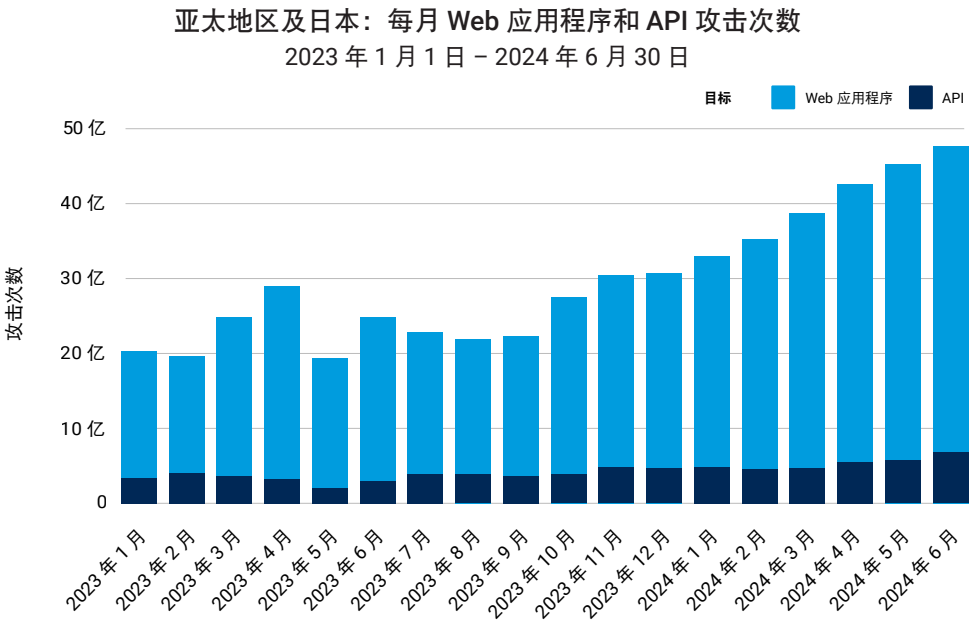
勒索软件和针对应用程序及它们之间内部工作负载的其他攻击成为一个日益尖锐的问题。各企业正在转向基于软件的微分段技术，以获取保护不断扩大的攻击面所需的监测能力和精细控制能力。

Web 应用程序和 API：安全风险的温床

随着各企业争相部署应用程序以改进客户体验和推动业务发展，Web 应用程序和 API 攻击也随之出现激增。攻击者将利用这个不断扩大的攻击面（例如，代码编写质量不佳和存在设计缺陷以及数年前的旧漏洞的 Web 应用程序）。此外，API 经济的快速发展也为网络犯罪分子提供了利用漏洞和滥用业务逻辑的更多机会。

通过数字了解攻击趋势

在 2024 年的第一期 SOTI 报告中，我们探讨了 2023 年在整体 Web 应用程序攻击背景下的 API 攻击趋势。通过回顾过去 18 个月（从 2023 年 1 月到 2024 年 6 月）的数据，Akamai 研究人员发现亚太地区及日本每月的 Web 应用程序和 API 攻击次数于 2024 年 6 月创下了 18 个月以来的新高，达到 48 亿次的峰值。这表示从 2023 年第一季度到 2024 年第一季度该地区的网络攻击增长 65%，并在随后的季度继续保持增长。针对 API 的攻击小幅增加，于期末达到 6.7 亿次（亚太地区及日本图 1）。



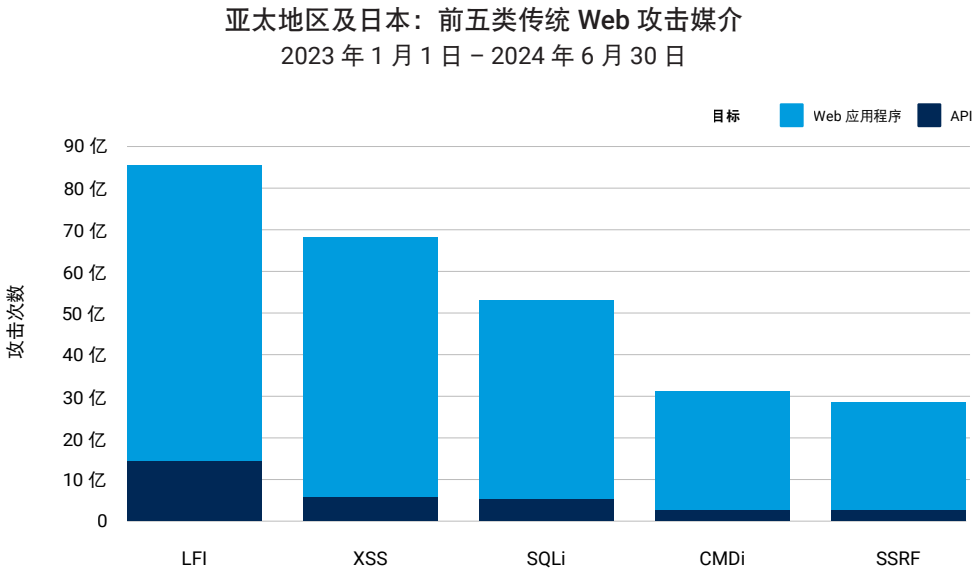
亚太地区及日本图 1：Web 应用程序和 API 攻击次数年同比增长 65%

在亚太地区及日本中，澳大利亚（146 亿次）、印度（120 亿次）和新加坡（107 亿次）在此期间遭受的 Web 应用程序和 API 攻击最多，紧随其后的是中国大陆（43 亿次）、日本（40 亿次）、新西兰（21 亿次）、韩国（16 亿次）和中国香港特别行政区（15 亿次）。

Akamai 还跟踪了多种网络攻击媒介。在本期报告中，我们将重点介绍前五类基于传统攻击媒介的攻击方法。

Akamai 研究人员发现，亚太地区及日本的每月 Web 应用程序和 API 攻击次数在 2024 年 6 月创下了 18 个月的新高，达到了 48 亿次的峰值。

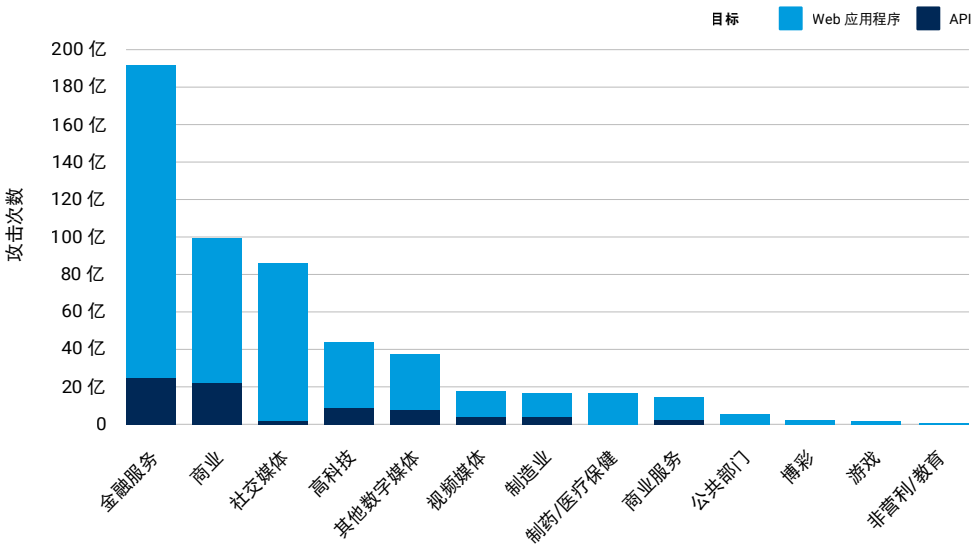
与上一期报告一致的是，本地文件包含 (LFI) 仍然是攻击者首选的攻击媒介，但跨站点脚本攻击 (XSS) 和结构化查询语言注入 (SQLi) 等其他攻击媒介继续构成风险（亚太地区及日本图 2）。



亚太地区及日本图 2：LFI、XSS 和 SQLi 正在推动 Web 应用程序和 API 攻击的增长

攻击者很少使用 LFI 和 XSS 等传统攻击手段来访问预定目标的数据。此外，LFI 让攻击者能够在预定目标中建立立足点并实现远程代码执行，从而破坏安全机制。

从行业角度来看，受 Web 应用程序和 API 攻击影响最大的五个行业与上一期报告中的情况一致，金融服务和商业行业首当其冲。在具体研究 API 攻击时，我们发现与 API 安全性 SOTI 报告相比，针对游戏行业的攻击次数大幅下降（亚太地区及日本图 3）。这一变化并不意味着游戏行业不再是攻击者的攻击重点。游戏仍然是遭受第 3 层和第 4 层 DDoS 攻击最多的行业之一，您可以在本期报告的后续部分中看到与此相关的内容。



亚太地区及日本图 3：网络犯罪分子继续明确地将金融服务行业作为攻击目标

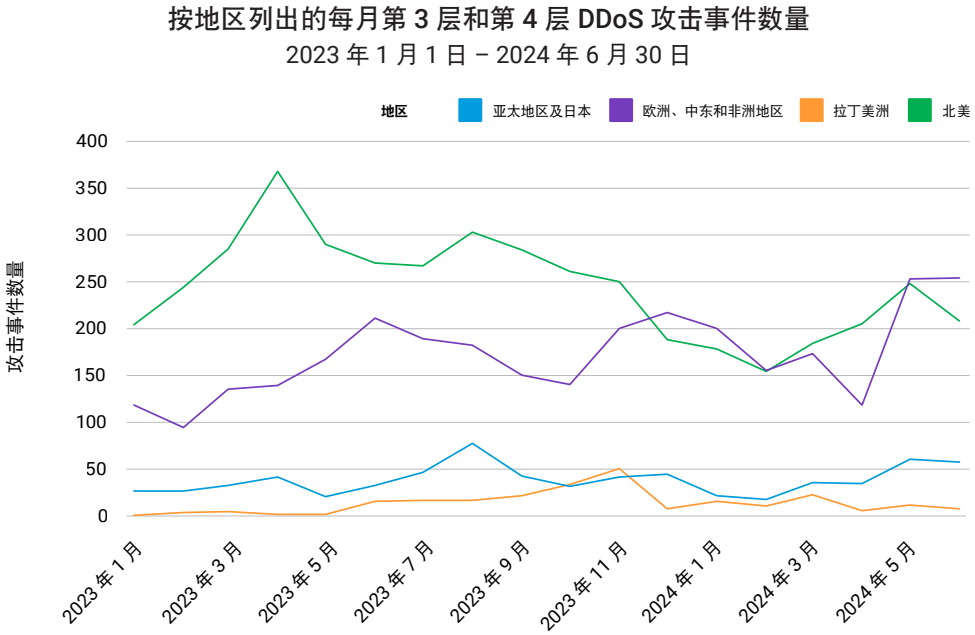
DDoS 攻击威胁应用程序正常运行时间

随着攻击面继续扩大，影响应用程序的 DDoS 攻击类型也在不断增加。正如我们在全球 SOTI 报告中详细介绍的那样，传统第 3 层和第 4 层 DDoS 攻击已存在了很长时间，其目的是导致网络或应用程序服务器容量不堪重负。应用层（第 7 层）DDoS 攻击会利用漏洞以及应用层中业务逻辑的漏洞和/或缺陷。即使只利用相对少量的恶意流量，它们也能够造成严重损害。无论攻击媒介如何，成功实施的 DDoS 攻击所带来的影响便是应用程序停机。

我们的最新研究表明，第 3 层、第 4 层以及第 7 层 DDoS 攻击会持续威胁为应用程序提供支持的基础架构以及应用程序本身。

基础架构 DDoS 攻击

在从 2023 年 1 月到 2024 年 6 月的 18 个月报告期内，Akamai 研究人员发现，亚太地区及日本遭受的第 3 层和第 4 层 DDoS 攻击事件比其他地区都要少。但是，我们可以看到自 2024 年 2 月以来攻击事件有所增加（亚太地区及日本图 4）。



亚太地区及日本图 4：亚太地区及日本的第 3 层和第 4 层 DDoS 攻击事件数量少于其他地区，但该数量 2024 年呈上升趋势

受影响最大的地区是中国台湾 (409)，紧随其后的是澳大利亚 (105)、巴基斯坦 (51)、中国香港特别行政区 (49)、日本 (38) 以及新加坡 (29)。本节以及下一节关于应用层攻击的内容表明，DDoS 攻击正在成为亚太地区及日本攻击者首选的网络武器，这主要是受地缘政治动荡和紧张局势的影响，民族国家相关攻击者和黑客都越来越多地参与其中。

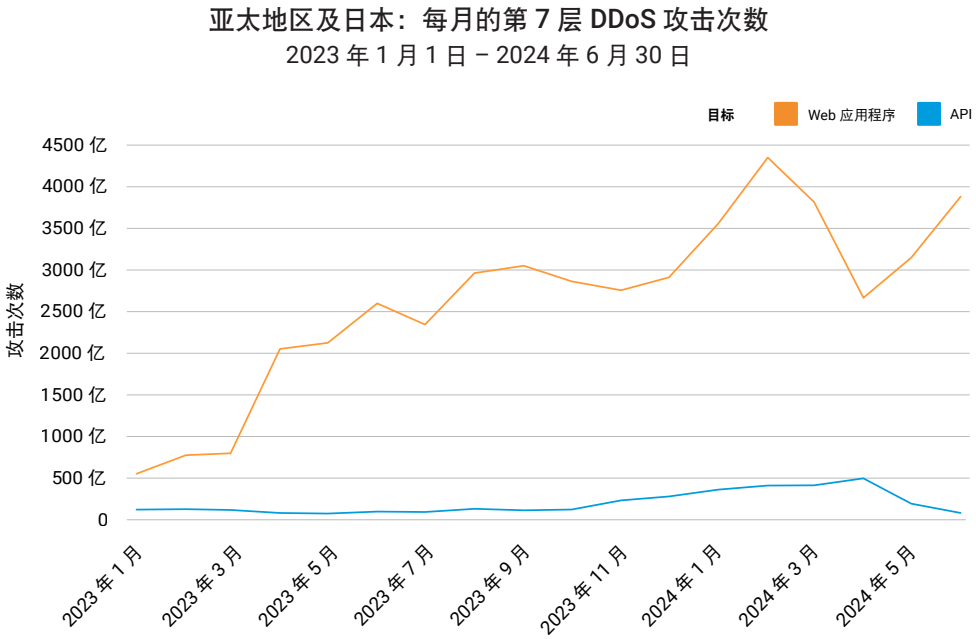
从行业角度看，商业 (207) 和游戏 (158) 行业遭受的第 3 层和第 4 层 DDoS 攻击事件最多，紧随其后的是金融服务行业 (120)、视频媒体行业 (91) 和高科技行业 (63)。

应用层 DDoS 攻击

除了第 3 层和第 4 层 DDoS 攻击之外，该地区还遭受了定向应用层（第 7 层）DDoS 攻击。在从 2023 年 1 月到 2024 年 6 月的 18 个月报告期内，Akamai 研究人员发现，亚太地区及日本遭受的第 7 层 DDoS 攻击次数为 5.1 万亿次，排名第二，仅次于北美地区的 8.7 万亿次。

在从 2023 年 1 月到 2024 年 6 月的 18 个月报告期内，Akamai 研究人员发现，亚太地区及日本遭受的第 7 层 DDoS 攻击次数为 5.1 万亿次，排名第二，仅次于北美地区的 8.7 万亿次。

在深入研究这些数据后，我们看到报告期内每月的第 7 层 DDoS 攻击量大幅增长，从 2023 年 1 月的 700 亿次攻击激增到 2024 年 6 月的 3990 亿次攻击，增长了五倍多。此外，虽然亚太地区及日本中不到 10% 的第 7 层 DDoS 攻击以 API 为目标（亚太地区及日本图 5），但该风险呈上升趋势。这是一个不断变化的形势，并且随着该地区 API 采用率的不断上升，所面临的风险也会随之增加。

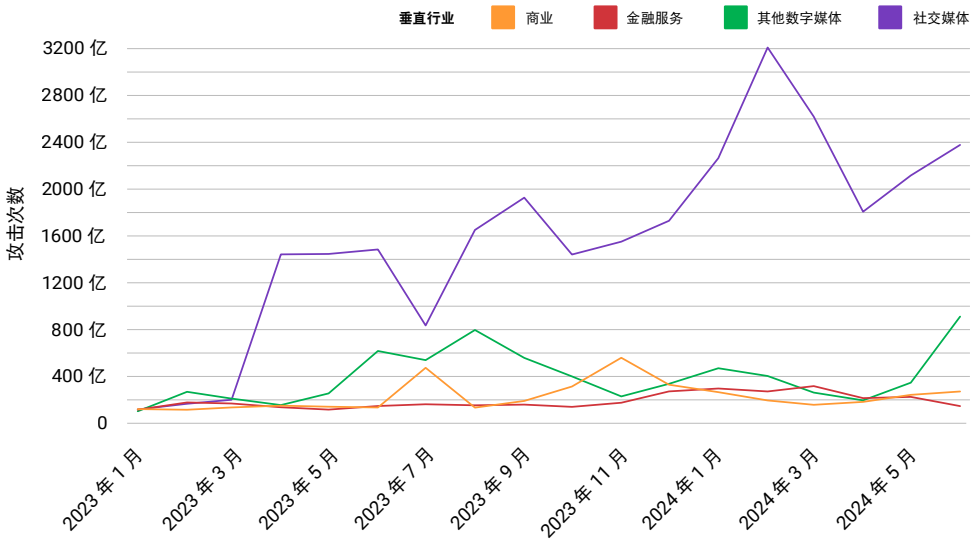


亚太地区及日本图 5：从 2023 年 1 月到 2024 年 6 月，第 7 层 DDoS 攻击增长了五倍

其中，新加坡受到的攻击最为密集，达到 2.9 万亿次，其次是印度（9590 亿次）、韩国（5440 亿次）、印度尼西亚（2600 亿次）、中国大陆（1880 亿次）、日本（830 亿次）、澳大利亚（740 亿次）以及中国台湾（500 亿次）。

按垂直行业查看趋势可以发现，第 7 层 DDoS 攻击活动的增加主要原因在于针对社交媒体行业的攻击尝试（亚太地区及日本图 6）。

亚太地区及日本：按垂直行业列出的每月第 7 层 DDoS 攻击次数
2023 年 1 月 1 日 – 2024 年 6 月 30 日



亚太地区及日本图 6：针对社交媒体的攻击有所增加，这与全球宏观趋势一致，并且与世界范围内更广泛的军事冲突以及受到大量媒体关注的选举事件相关

众所周知，社交媒体平台会因为地缘政治动荡而收到大量攻击流量，亚太地区及日本也未能幸免。正如我们在全球 SOTI 报告中详细介绍的那样，此攻击活动中出现了大量虚假的亲俄社交媒体帐户和欺骗性新闻网站，其目的是炒热制造分裂的政治话题。这些攻击还与全球持续的地缘政治动荡相关。受到大量媒体关注的大规模选举活动以及总统/国家或地区领导事务往往会导致各个地区发生出于政治动机的网络攻击（包括 DDoS 攻击），因为攻击者试图利用紧张的政治气氛来实现他们的目的。与持续的俄乌战争及以色列-哈马斯战争相关的黑客行动也可能导致攻击增加。

人工智能 (AI) 工具的兴起使一些令人信以为真的虚假内容变得更加容易传播，并且社交媒体平台是一个巨大的传播渠道，里面充斥着各种各样的内容。再加上 2024 年是亚太地区及日本和美国的大选年，因此我们很可能会继续看到攻击者对所有地区的社交媒体平台发动攻击。

本期报告中的攻击趋势数据提醒我们，攻击者会不遗余力地去追求破坏和经济利益，他们能够在不同的行业、地域及攻击手段之间快速转换重点。因此，所有企业都必须保持警惕，并确保采用适当的防御措施来防范各种类型的攻击，从而避免自己的应用程序出现停机。

攻击者以应用程序工作负载为目标

人们通常会在网络安全的背景下讨论 Zero Trust。但是，Web 应用程序与它们之间的内部工作负载也可能会面临勒索软件等威胁，这些威胁会寻找任何入口点和途径来达到其预定目标。

正如全球报告中详细介绍的那样，无论在云端、本地还是混合环境中，要让应用程序正常工作，每个单独的工作负载都必须无缝运行。工作负载在网络中移动时会穿过多个安全管辖区，并且每个新的管辖区都会为入侵者增加一个潜在的入口点。要增强整体安全态势，保护这个扩大的攻击面至关重要，但也会让安全团队本就困难重重的工作变得更加棘手。

通过基于硬件的传统方法实施 Zero Trust 框架不仅需要耗费大量的资源和时间，而且必须停机。此外，真正的 Zero Trust 实施需要进行微分段来防范勒索软件或针对工作负载本身的攻击。

基于软件的微分段可以快速、轻松地实施和操作，因此它甚至可以作为可行的事件响应措施，并作为一项控制措施来隔离关键系统以支持合规性。由于微分段具备这些优势，企业越来越多地在其动态数据中心、云端和混合云环境中采用此方法来检测和抵御受到危害的工作负载或容器。

保护应用程序工作负载方面的实际经验教训

在本节中，我们将介绍来自亚太地区及日本的两个案例研究，举例说明企业如何保护关键工作负载并推进 Zero Trust。

亚太地区及日本案例研究 1：某社交网络需要一种方法来确保客户通信安全，该平台提供消息传递、游戏和社交媒体等服务以及金融服务购买功能。防止黑客获取客户对话并横向移动到其他网络和数据库是首席信息安全官的首要任务。客户使用了多种不同的操作系统和应用程序，因此无法知道哪台设备容易受到攻击。利用精细的分段策略来隔离设备和网络是该公司维持通信所需信任的基本方式。

亚太地区及日本案例研究 2：某业务遍布全球的优秀 IT 分销商为金融服务行业的大量客户提供服务。保护对银行业务运营至关重要的支付服务器极其重要。在微分段领域拥有深厚的专业知识，让该公司可以在一些极为复杂的环境中大规模部署并启用网络监测和极其精细的治理控制措施，从而能够在客户信任和 Zero Trust 能力优势的基础上加快发展速度。

工作负载在网络中移动时会穿过多个安全管辖区，并且每个新的管辖区都会为入侵者增加一个潜在的入口点。

结论

在本期《亚太地区及日本概况》中，我们尝试全面分析攻击者针对您的应用程序和 API 发起攻击的不同方式。从安全和风险管理角度来看，企业必须了解并防范应用程序和 API、基础架构及关键工作负载所面临的威胁。此外，现有的法律和即将落地的法律改革也让确保应用程序安全变得至关重要。

亚太地区及日本不断变化的形势包括新加坡近期对其网络安全法案的修订、日本对国家网络安全事件准备和战略中心法律的更新、《支付卡行业数据安全标准 v4.0》以及其他新的立法措施（例如，印度对《信息技术法案》的全面修订，《数字个人数据保护法案》的通过为此修订工作拉开了序幕，以及《2023–2030 澳大利亚网络安全战略》等）。此外，欧洲的开放银行指令正在推动欧洲、中东和非洲对 API 的使用，并可能扩展到更多地区，而亚太地区和日本对 API 的应用可能有机会更胜一筹。

对于企业来说，应用程序比以往更加重要，但同时也更容易受到攻击。凭借应对不断扩大的攻击面挑战的能力和最佳实践，企业可以随时随地保护其构建的应用程序，而不会影响性能或客户体验。

如需了解更多信息，请参阅全球安全应用程序 SOTI 报告《数字堡垒受到围攻：现代应用程序架构面临威胁》。

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。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。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 Connected Cloud 上检测到的安全事件。Akamai Connected 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。

该数据涵盖了从 2023 年 1 月 1 日到 2024 年 6 月 30 日的 18 个月的时间段。

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 应用程序攻击数据集已收到一些更新。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《SOTI/安全性》发展的这一里程碑。

DDoS（第 3 层和第 4 层）

Akamai Prolexic Routed 专为保护企业免受 DDoS 攻击以及其他有害流量或恶意流量的影响而打造，旨在避免这些威胁侵扰应用程序、数据中心和面向云和混合互联网的基础架构（不论是公有还是私有），包括所有端口和协议。Akamai 安全运营指挥中心 (SOCC) 的专家可定制主动缓解控制措施，以便即时检测和阻止攻击，并对其余流量进行实时分析，以根据需要确定进一步的缓解措施。系统会对这些被抵御的攻击进行整理并分组为攻击事件，并且所有关联的数据都由 SOCC 记录以进行分析。

该数据涵盖了从 2023 年 1 月 1 日到 2024 年 6 月 30 日的 18 个月的时间段。

致谢名单

研究总监
Mitch Mayne

编辑与创作
Tricia Howard
Charlotte Pelliccia
Lance Rhodes
Badette Tribbey
Maria Vlasak

审稿和主题撰稿
Sven Dummer
Reuben Koh
Tony Lauro
Richard Meeus
Menacham Perlman
Sandeep Rath
Steve Winterfeld

数据分析
Chelsea Tuttle

推广材料
Barney Beal

营销与发布
Georgina Morales
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

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 针对应用程序和 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。