SOTI

第 10 卷，第 6 期

10 YEARS
OF SECURITY INSIGHT

显微镜下的医疗保健行业

针对应用程序和 API 的猛烈攻击

Akamai

互联网现状/安全性

目录

从漏洞到监测能力，揭示医疗保健行业的网络安全状况

医疗保健行业的安全现状可以归结为一个词：“漏洞百出”。为了应对此状况，“监测能力”成为 2024 年医疗保健行业关注的重要主题。日益增加的平台、第三方软件以及大规模的数据交换需求都在促使企业提升监测能力，然而，医疗保健企业的技术现代化速度如此之快，以致于很多企业难以真正地全面监测自己的生态系统。一些合规措施让情况变得更加复杂，它们一方面要求企业共享更多信息，一方面又要求施加更严格的控制。虽然从逻辑上讲，这是为了消除数据护城河及网络垄断而采取的必然之举，但它增加了技术复杂性因素。除了个别顶尖企业外，业内大多数企业当前的安全防护能力可能都不足以应对这些因素。

这使得攻击者蠢蠢欲动。随着医疗保健行业的各个领域都在开放系统来交换社会中最敏感的信息，我们正在将新系统和新标准与数十年的传统基础架构混搭在一起。因此，这些传统基础架构不仅本身可能会产生的大量技术债务，还为恶意攻击者提供了一个发动攻击的“温床”。

因此，医疗保健企业遭受一轮又一轮的网络安全攻击是意料之中的结果。特别是在美国，多年以来，很多医疗保健企业一直将网络安全视为招标和供应商评估过程中走过场的内容。企业通常只是要求供应商符合 HITRUST 和 HIPAA 标准以及通过 SOC 2 认证，然后借助业务合作伙伴协议将风险转嫁给这些供应商，而不会在内部培养专业人才。虽然这是一个不错的开端，但是我们仍然看到接连不断的头条新闻，大肆宣扬医疗保健行业的重大财务问题、运营故障，甚至更糟糕的内容——对患者安全的威胁。我们下面的说法可能会惹恼一些人，但是，当排名前 1,000 的医院和医疗系统中有四分之一到二分之一的机构使用同一份基于电子表格的“安全检查清单”来审批和考核供应商时，这个行业确实出现问题了。

值得关注的是，医疗支付方面临的暴露风险比以往任何时候都要高，并且合规措施要求他们脱离以往的本地、批处理系统，以符合现代生态系统基于 API 的数据要求。虽然这种现代化让医疗支付方能够访问多年以来他们一直梦寐以求的临床数据，但开放式交换是一种新的业务开展方式，会带来新型风险。由于掌握着财务数据和临床数据，医疗支付方必须保护自己的基础架构，并在遵守每项新的合规要求时，审慎地提升安全态势。

结论：这些市场变革还会持续下去。医疗保健行业无法退回到不需要 API 和云计算的时代。虽然对变革带来的安全问题表示担忧是难免的，不过，对于一个历来受到数据孤岛问题困扰的行业来说，能够重视开放式数据交换就是巨大的进步。

Untangle Health 副总裁
Neil Jennings

Untangle Health 首席执行官
Chris Notaro

简介

医疗保健行业在网络安全方面存在一些独特的挑战。

- 其中的利害关系可能关乎生死。
- 这个行业所持有的信息在价值上高于其他所有行业。
- 基础架构既包含传统系统，也包含医疗物联网 (IoMT) 设备。
- 这些系统盘根错节，并且常常相互依存。
- 合规性要求极为苛刻。

在本期的《互联网现状》(SOTI) 报告中，我们将分析与医疗保健生态系统所面临风险相关的威胁数据和趋势。对此行业影响最大的两种威胁分别是 Web 应用程序和 API 攻击以及分布式拒绝服务 (DDoS) 攻击。

此外，医疗保健生态系统中的企业（医疗支付方、医疗服务提供商以及制药和生命科学公司）还分别面临不同的挑战，在制定安全策略时需要考虑到这些挑战。

保险公司或医疗支付方可以广泛获取临床数据和财务数据来确定是否符合理赔条件、承保范围以及进行付款，同时也是整个行业中数据共享的重要枢纽。

制药和生命科学企业发现，攻击者开始瞄准企业采用的创新技术，包括使用人工智能和机器学习来分析各种应用程序的大量数据集，这让他们站在创新与风险的十字路口，难以做出抉择。

医疗保健服务提供商的资金主要用于远程医疗等临床创新和蓬勃发展的 IoMT 技术，只有较少的资金被投入到更传统的功能上，例如对企业恢复能力至关重要且不断演变的网络安全方法。

推动互操作性可以实现更好的患者预后并提升财务业绩，但也会带来 Web 应用程序和 API 攻击风险。

从历史角度看，医疗保健生态系统多年来一直是攻击者觊觎的目标。2024 年，医疗保健行业连续 13 年成为所有行业中数据泄露损失最高的行业，平均损失达到 977 万美元，远高于排名第二的金融服务行业（608 万美元）。

API 是影响医疗保健行业中所有子垂直行业的主要技术之一。API 使得在医疗服务提供商、医疗支付方、患者和其他第三方（例如电子健康记录系统、医疗设备公司和健康信息交换机构）之间共享数据成为可能。推动互操作性可以实现更好的患者预后并提升财务业绩，但也会带来 Web 应用程序和 API 攻击风险。

对于应用层，另一种常见风险是 DDoS 攻击。在欧洲、中东和非洲 (EMEA) 地区，它们是攻击者当前的首选武器，其可能的原因在于该地区的地缘政治发展和亲俄黑客组织。但是，实施 DDoS 攻击的团伙数量如此之多，他们采用的策略、技术和过程如此的变化多端，没有任何国家或地区能够免受攻击。

关键见解

41%

医疗保健生态系统中针对医疗支付方企业的 API 攻击所占百分比

医疗保健生态系统中的 API 攻击一直有增无减，特别是医疗支付方和保险公司因掌握着受保护的健康信息 (PHI)、索赔数据以及财务信息等大量数据，更是成为重点攻击对象。

API 蔓延构成了重大风险，例如对数据的未授权访问

API 蔓延，也就是企业内 API 不受监管的扩散，会因为企业缺乏监测能力以及它们游离在安全控制措施之外而造成严重的安全漏洞。因此，API 蔓延会扩大企业的攻击面并带来未经授权访问敏感数据等风险。

88%

EMEA 地区针对制药企业的第 7 层 DDoS 攻击所占百分比

EMEA 地区的制药公司遭遇的第 7 层 DDoS 攻击最多，紧随其后的是北美和亚太地区及日本 (APJ)。深入研究 2024 年上半年的数据可以发现，针对 EMEA 和北美地区的攻击数量有望超过 2023 年每个地区的总和。

2100 万

针对医疗保健服务提供商的 Web 应用程序和 API 攻击的月度平均数

推进数据互操作性以及其他合规性要求促使对 Web 应用程序和 API 的使用越来越多，而这会给医疗服务提供商和患者带来安全风险。

4.15 亿

针对医疗保健服务提供商的第 7 层 DDoS 攻击的月度平均数

在黑客行动主义和当前地缘政治气氛紧张的驱动下，医疗保健行业遭受的 DDoS 攻击呈现激增态势。这些攻击可能导致停电和服务中断，威胁患者预后。2023 年，Killnet 发动了一次主要针对医疗服务提供商的大规模 DDoS 攻击活动。

医疗支付方面临 API 滥用的高风险

医疗支付方在医疗保健生态系统中大量使用 API 来收集和处理数据，虽然这可以带来巨大的好处，但也需要做出取舍——特别是重要的合规性要求和安全风险。网络犯罪分子和数据聚合商会对这些能力进行攻击和滥用，从而可能导致安全和隐私问题。

对于医疗支付方来说，通过 API 实施的攻击也可能会导致服务中断，从而影响医保的投保登记和理赔操作，导致成本高昂的停机事件，并损害品牌声誉。举例来说，2024 年 2 月发生的系统性攻击就是一次令人头疼的攻击事件，它严重阻碍了全美药房处理支付订单。

API 攻击趋势

Akamai 研究发现，从 2023 年 1 月到 2024 年 6 月，针对医疗保健生态系统的 API 攻击中 41% 攻击的目标都是医疗支付方企业。这表明，医疗支付方面临更集中的 API 滥用攻击风险，这与医疗支付方在维持医疗保健系统运转方面的重要性保持一致，因为截至 2022 年，美国医疗保健总支出中约有 67% 的部分通过医疗支付方支付。

我们在其他受监管的行业中也看到了类似的趋势，尤其是那些掌握着支付系统的行业。例如，金融行业在进一步深化其数字化转型，并且已在其业务模式中使用集成度更高的 API。开放银行业务正在推动 API 的使用并带来了更多安全风险。因此，金融行业正面临着更加集中的以 API 为重点目标的攻击，这与我们 API 安全性 SOTI 报告的发现结果一致。

在仔细研究医疗支付方 API 攻击数据后，Akamai 研究人员发现从 2023 年 1 月到 2024 年 6 月的 18 个月里攻击活动的数量出现多次波动，尤其是每季度都会出现波动。每个季度总体呈上升趋势可能反映了各系统会在季度末进行数据同步，以对预测数据和实际数据进行对帐的实际情况，但 2023 年第 4 季度出现整体增长可能是攻击者针对年度投保登记期发动攻击，以扰乱相关操作所致（图 1）。

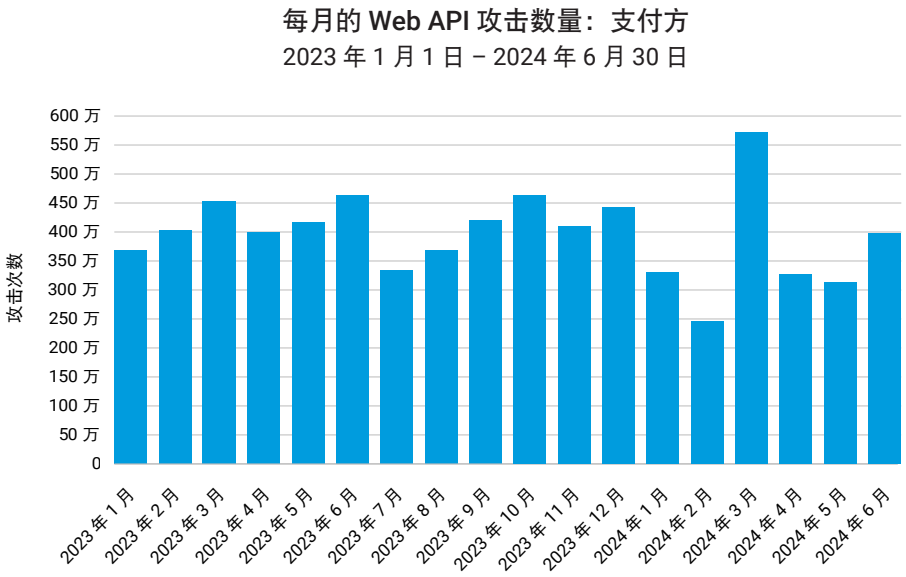


图 1：每个季度针对 API 的 Web 攻击数量呈上升趋势，2023 年第 4 季度出现整体增长

所有行业中的 API 滥用和重大安全挑战

虽然医疗保健行业面临很多独有的 API 安全挑战，不过，对于所有行业说，API 基础知识都是一样的，我们也有必要回顾一下所有行业都需要抵御的技术风险。首先，我们应专注于应对 OWASP 十大 API 安全风险所强调的风险。另外还需要确保开发人员和 IT 人员了解被我们列为态势问题和运行时问题的一些更常见的漏洞。

- **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有助于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。常见态势问题包括影子端点和 URL 中的敏感数据。
- **运行时问题**是需要紧急回应的主动威胁或行为。与其他类型的安全告警相比，这些关键告警更细致，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。常见运行时问题包括未经身份验证的资源访问尝试和数据抓取。

同样重要的是，回顾并审视 API 所带来的三个更为普遍的挑战，以确保您的安全计划涵盖 API 滥用和利用。

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 一般是在转型过程中引入，或者嵌入于新产品之中，因此许多 API 没有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值？您是否确定了可疑活动的构成要素？

以上问题的答案构成了您的团队应了解内容的基础。总体目标应该是具有开展调查的可见性和能力，并建立能够快速抵御威胁的流程。不管是面向患者的 API，还是内部 API，都是如此。

API 往往是复杂数字化转型项目的组成部分，因此它们可能不会受到医疗保健企业的关注，而安全计划受到的关注甚至更少。

更高的性能可能会带来更大的风险

患者希望所有的应用程序都能提供同等水准的用户体验，因而，性能正在成为一个更严重的问题。这意味着需要保护医疗保健生态系统免受拒绝服务攻击以及滥用攻击。此外，医疗服务提供商还需要遵守针对透明度的监管要求，这些要求促使他们必须及时提供信息。

API 蔓延可能会导致监测能力下降，甚至会随着攻击面的扩大而更加模糊。API 往往是复杂数字化转型项目的组成部分，因此它们可能不会受到医疗保健企业的关注，而安全计划受到的关注甚至更少。

医疗支付方在日常业务活动中涉及的各类医疗和财务数据既受到严格监管，又容易成为网络犯罪分子的目标，因此，其面临的挑战更加复杂。

针对生命科学企业的 DDoS 攻击的数量日益增加

在新冠疫情期间，疫苗开发研究、试验数据、制造、生产和发布都成为了攻击者的目标，因此对制药网络安全的关注变得尤为突出。现在，医疗保健被美国列为关键基础设施，而两党的最新拨款提高了对关键基础设施行业恢复能力的要求。原因很明确：

- 全球范围内的国际紧张局势持续加剧，以及地缘政治气氛对接受普华永道第 25 届全球首席执行官年度调查的受访高管产生了很大的影响。几乎有三分之一的受访高管表示地缘政治冲突会威胁其公司的增长，并且超过三分之二的受访高管表示这是导致供应链中断的一个预期因素。
- 本地化采购和加强区块链技术的使用等方法可以帮助制药公司提升恢复能力并改善临床和业务影响。
- Akamai 获取的生命科学行业的全球数据表明，DDoS 攻击数量以及实施这些攻击的团伙数量只增不减；此行业需要具备的正是恢复能力。

EMEA 地区的制药企业成为应用层 DDoS 攻击的目标

Akamai 研究发现，从 2023 年 1 月到 2024 年 6 月，所有以制药企业为目标的应用层（第 7 层）DDoS 攻击中有 88% 针对的是 EMEA 地区，而针对北美地区和 APJ 地区的此类攻击分别占 7% 和 5%。在研究 2024 年上半年的数据后，我们可以看到 EMEA 和北美地区的攻击集中度呈上升趋势，并且有望超过 2023 年每个地区的攻击数量总和（图 2）。

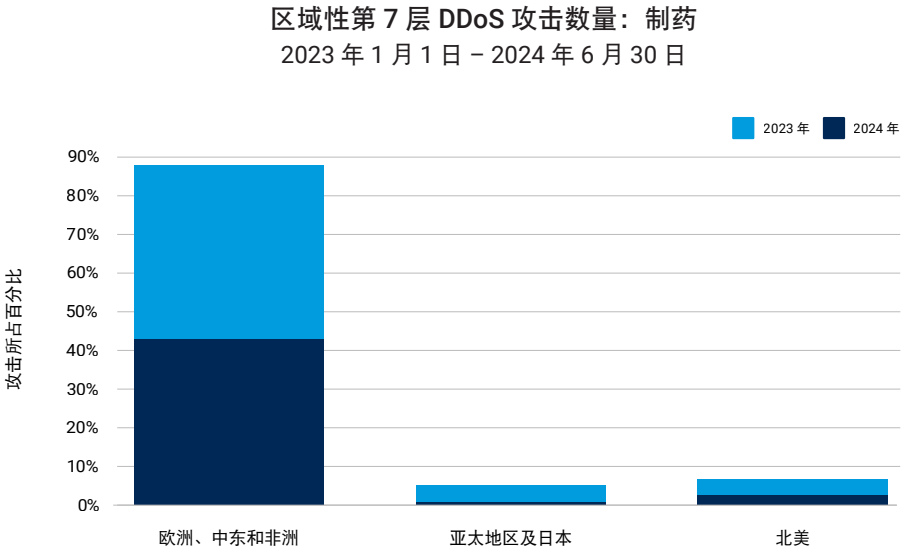


图 2：2023 年到 2024 年 EMEA 地区的第 7 层 DDoS 攻击持续集中并于 2024 年上半年出现激增，而北美地区的攻击也在增加

传统的第 3 层和第 4 层 DDoS 攻击以让网络和传输层基础架构不堪重负为目的，而第 7 层 DDoS 攻击与这两种攻击有所不同，它们以特定的应用程序功能或应用程序服务器本身为目标。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。

第 7 层 DDoS 攻击以应用级资源（如 CPU 和资源）为目标，因此被攻击的目标应用程序或服务虽然仍然可用，但可能会变得运行缓慢或完全无响应。

欧盟医疗保健和生命科学行业遭受的 DDoS 攻击增加

《ENISA 2023 Threat Landscape: Health Sector》报告指出，欧盟医疗保健和生命科学行业遭受的 DDoS 攻击不断增加。值得注意的是，该报告中网络事件的 “热点” 国家（尤其是法国、德国和荷兰）与 2022 年欧盟前 1,000 家公司中的制药和生物技术公司的地理集中度呈正相关。

ENISA（欧盟网络安全局）将 DDoS 攻击的增长归因于地缘政治风险加剧和亲俄黑客组织（如 Killnet）。

美国生命科学企业成为下一个目标

Killnet 首先攻击了欧洲的医院，然后将目标转向美国几乎每个州的医院。虽然这些针对医院的网络攻击占据了最多的头条新闻，但美国卫生与公众服务部 (HHS) 2023 年 4 月的一份报告指出，成为 Killnet 的 DDoS 攻击目标的企业中，制药和生物技术公司所占比例实际上是最高的。

鉴于美国在全球生命科学领域的市场份额 (50%) 高于 EMEA (34%)，因此可以合理地预计，针对美国制药公司的 DDoS 攻击威胁还会加剧。

但是，没有国家或地区能够免受攻击。作为全球最大仿制药生产国和出口国之一的印度，去年发生了一起 17 TB 公司数据遭到泄露的事件，因此蒙受了巨大损失。勒索软件团伙和攻击者 ALPHV/BlackCat 声称对另一起勒索软件攻击负责，该攻击涉及供应商、客户的敏感信息以及 1,500 名美国员工的文件。

哪些攻击者正在使用何种策略?

ENISA 报告指出，ALPHV/BlackCat 是针对 EMEA 地区生命科学行业的主要攻击者团伙之一，他们也是今年早些时候重创美国供应链的罪魁祸首。

和 Killnet 一样，该报告中提到的 Anonymous Sudan 也出于政治动机而发动攻击；该犯罪组织最初以医疗服务提供商群体为目标，但现在其目标变得更广，已包括医疗保健生态系统的其他部分。

这种扩展使得最近的事态发展变得更加令人担忧，比如 Anonymous Sudan 声称对最近针对 OpenAI 的 DDoS 攻击负责。该团伙声称使用了 Skynet 僵尸网络，此僵尸网络最近加入了对第 7 层 DDoS 攻击的支持，以导致应用程序不堪重负和产生错误。

高风险需要采取保守方法

制药公司长期以来一直是医疗保健行业中积极应用人工智能 (AI) 技术（尤其是机器学习 (ML) 技术）的佼佼者，并从利用 AI 技术对各种应用程序的大量数据集进行分析中受益匪浅。这些好处包括提早发现疾病、更快地发现药物以及改进药物生产。但是，与拥抱数字化转型的其他行业（如金融服务业）一样，生命科学行业也处在创新与风险的十字路口。

成为 Killnet 的 DDoS 攻击目标的企业中，制药和生物技术公司所占比例实际上是最高的。

制药公司正在表明立场。在研究其他受监管行业如何应对第 7 层 DDoS 攻击后，Akamai 研究人员发现，在所应用的 “拒绝” 与 “告警” 操作的比例方面，制药公司的策略比较保守，对异常活动的拒绝比例较高（图 3）。

按子垂直行业列出的针对第 7 层 DDoS 应用的操作
2023 年 1 月 1 日 – 2024 年 6 月 30 日

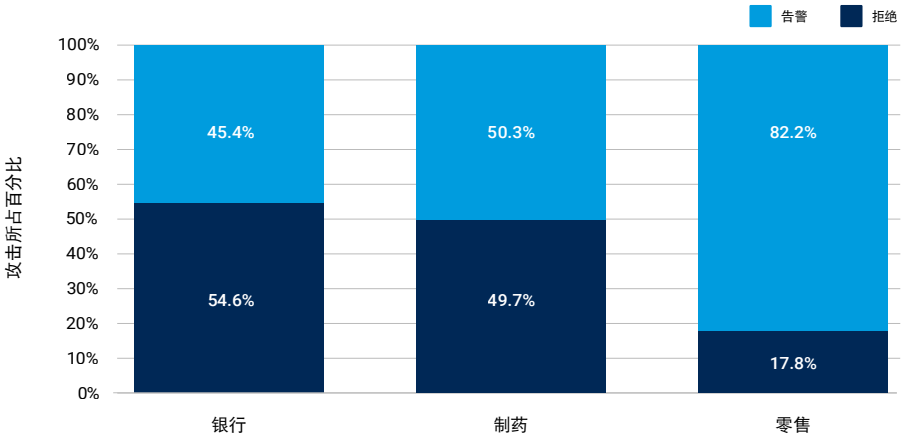


图 3：与告警操作相比，制药和生命科学公司的拒绝操作比例较高

自我们首次报告 2023 年 1 月至 2024 年 3 月的拒绝与告警统计数据以来，该比率上升了超过 4 个百分点，拒绝操作所占比例从 45.5% 增加至 49.7%——短时间内出现了显著增加。

金融服务业和银行业等其他行业也采取了与之类似的保守策略；银行业和生命科学行业都被视为关键基础设施并因此受到严格监管，这导致出现了很多相似之处。

此外，对于制药企业来说， DDoS 攻击一旦得逞，就会带来非常严重的后果，可能导致患者无法及时获取维持生命的药物，生命安全受到威胁。所以，他们往往倾向于应用拒绝操作，然后再对活动进行调查。

相比之下，零售行业采取的立场不那么激进，留出了更多时间来接收告警并评估异常活动，然后再采取行动。但是，如果有新的法规出台，特别是与 AI/ML 技术应用相关的法规，我们可能会看到零售商转为更频繁地采取拒绝操作。

Akamai 研究人员发现，在所应用的 “拒绝” 与 “告警” 操作的比例方面，制药公司的策略比较保守，对异常活动的拒绝比例相对较高。

医疗保健服务提供商受到围攻

健康信息共享和分析中心的首席安全官援引 HHS 于 2023 年 12 月发布的数据泄露分析报告称，平均每小时有 3,604 条患者记录遭到泄露并上报给 HHS。

针对医疗服务提供商和医院的网络攻击次数持续激增。由 Web 应用程序和强制使用 API 推动的连接性和互操作性可能会使医疗服务提供商和患者面临风险。传统技术中未修补的漏洞和所带来的技术债务是一项代价高昂的挑战，勒索软件团伙会利用该挑战来获取利益。

黑客组织针对医院发起的持续 DDoS 攻击威胁和地缘政治气氛都会中断患者护理。所有这些都会导致 PHI 数据泄露；对客户护理产生不利影响；有时还会导致患者安全问题。

攻击重创医疗服务提供商企业

Akamai 研究发现，从 2023 年 1 月到 2024 年 6 月的 18 个月里，针对医疗服务提供商企业的 Web 应用程序和 API 攻击持续稳定增长（图 4）。随着网络犯罪分子利用不断发展的护理模式、交付方法和创新系统中的新漏洞和屡试不爽的固有漏洞来攻击并滥用 Web 应用程序及 API，这种趋势可能会继续增长，但也会有所波动。

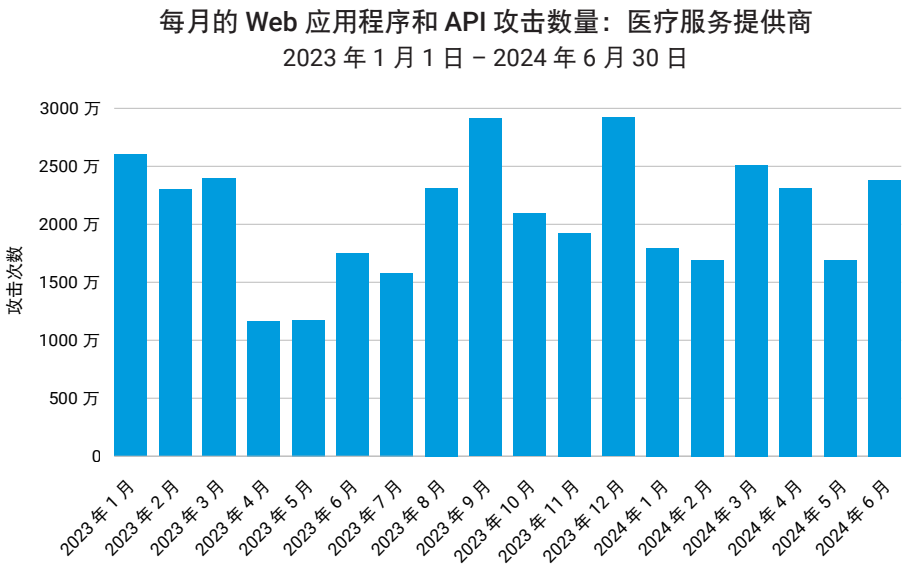
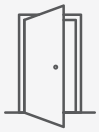


图 4：全球每月针对医疗服务提供商企业的 Web 应用程序和 API 攻击数量平均为 2100 万次（注意：一位客户的数据有偏差，因此为了保证报告数据准确，我们已将其删除）



传统技术中未修补的漏洞和所带来的技术负担是一项代价高昂的挑战，勒索软件团伙会利用该挑战来获取利益。

利用 Web 应用程序和 API，通过数据共享和互操作性实现护理协调，可以获得更好的临床和财务结果。但是，这也会让医疗保健行业面临重大风险，因为我们尚未充分了解 API 的安全影响。

在最佳护理协调与漏洞带来的风险之间取得平衡

由于提供商掌握着大量的患者记录和系统连接点，医疗保健服务需要优化护理协调，同时还需要实施控制措施来提供监测能力，以主动抵御漏洞带来的风险。在部署新技术和基础架构（如 API）时，往往很难保证这种平衡。

Akamai 研究人员还研究了上述 18 个月时间里针对医疗服务提供商企业的第 7 层 DDoS 攻击，并发现 2023 年 1 月之后，服务中断数量呈现较为稳定的节奏（图 5）。我们可以将此情况部分归因于亲俄黑客组织 Killnet 针对医疗保健行业发起全球性 DDoS 攻击活动，并以美国的医疗服务提供商企业为重点。在此期间，网络犯罪分子持续利用以应用程序功能或应用程序本身为目标的 DDoS 攻击，为患者护理带来了风险。

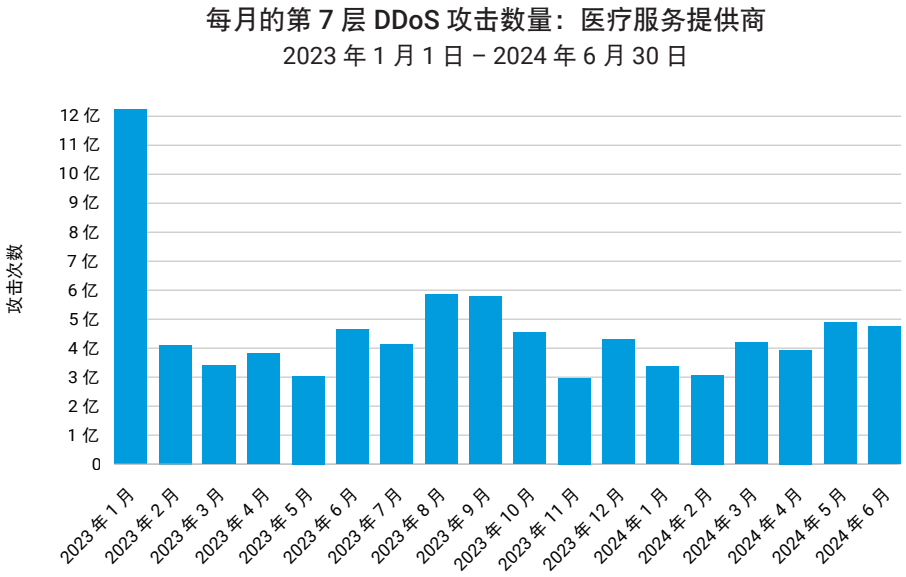


图 5：除了 1 月份出现一个孤立峰值之外，全球针对医疗服务提供商企业的每月第 7 层 DDoS 攻击数量的平均值为 4.15 亿次

针对医疗保健行业的 DDoS 攻击在规模和速度上都创下了新纪录

由地缘政治发展和黑客组织造成的 DDoS 攻击活动增加已导致出现可能威胁患者预后的服务中断。整个医疗保健生态系统也受到了影响——在 2023 年 Killnet 发起的大规模 DDoS 攻击中，医疗服务提供商企业成为遭受攻击最为频繁的目标。HC3 警告称，即便只是数小时的医疗保健服务中断，也会影响从常规手术到重症手术的一系列日常手术，并且可能造成严重的后果。

随着更多医疗保健交互通过应用程序实现，及时获取信息和护理对患者的体验越来越重要。因此，确保您实施了相应的保护措施和流程同样至关重要。

多阵线攻击阻碍了医疗护理的配合

除了 DDoS 攻击之外，医疗服务提供商还面临着其他的常见攻击类型。限制访问医疗保健记录并强迫救护车改道的勒索软件攻击突显出一个事实：如果无法访问患者的病史，医疗保健服务提供商就无法相互配合。恢复纸质记录会扰乱对患者护理操作的跟踪、关键部门之间的沟通以及所有订购服务。

当敏感数据受影响时，医疗服务提供商企业还必须应对数据泄露的影响。常见软件工具中的漏洞利用让未经授权的攻击者可以访问从 PHI 到健康保险和医疗信息等各种数据。

患者保护必须包括数据保护

对患者的保证应包括能够保护和控制对患者数据的访问权限。传统上，医疗保健网络安全预算和人员配置都很有限，这给数据保护带来挑战。但是，随着针对医疗保健服务提供商群体的网络攻击不断成为头条新闻，这些群体需要继续改善外包保护合作伙伴关系并扩大网络保险覆盖范围。

随着医疗保健服务提供商受益于美国政府关于加强关键基础设施部门恢复能力的新政策，加强保护的势头会继续增强。

在 2023 年 Killnet 发起的大规模 DDoS 攻击中，医疗服务提供商企业是最常见的目标。

合规考虑因素

监管环境对透明度的要求越来越高，这推动了 API 的使用。合规措施对医疗服务提供商和医疗支付方提出了广泛的数据共享要求。此数据共享旨在促进临床数据与财务数据互为所用，虽然这对各方来说一直都是大难题，却也是有效实施价值医疗 (VBC) 的必经之路。

向 VBC（即，在考虑成本的情况下提供医疗服务）转型这个示例很好地体现了现在需要共享的信息的数量和种类。长期以来，医疗支付方一直拥有对患者和服务提供商财务数据的访问权限。但是，更多的 VBC 数据点（例如，服药依从性和入院人数）需要一个不仅更具创新性而且更具互操作性的连续体，而且还需要一种共享这些数据的方法。API 是数据管道。

最近颁布的《CMS 互操作性和患者访问最终规则》要求医疗支付方维护三种主要类别的 API，以保持医疗支付方、医疗服务提供商与患者之间的信息畅通：

1. 患者访问 API：这将允许成员更方便地访问自己的医疗数据，还有可能提升成员的满意度。

2. 医疗服务提供商目录 API：这允许相关成员根据自己所在的位置和医疗专业来搜索医疗保健服务提供商，从而提高医疗服务可及性。

3. 医疗支付方-医疗服务提供商 API 和医疗支付方-医疗支付方 API：这可帮助填补和缩小患者护理缺口，并且有可能减少重复和昂贵的服务。

并且，即将出台的 CMS 互操作性和事先授权最终规则将要求受影响的医疗支付方采用一个额外的事先授权 API。

此外，合规措施也通过快速医疗保健互操作性资源 (FHIR) 标准规定了 API 的格式。这些要求和标准将在提升安全性的同时简化和优化系统之间的互操作性。FHIR 希望相关企业实施一个包括 Web 应用程序防火墙、身份验证、加密、隐私保护和微分段等基本功能的安全计划。

虽然要求医疗服务提供商比以往共享更多的数据，并以标准格式进行共享，以便能够及时地连接到患者所选的健康应用程序，但 FHIR 标准的目的是减轻管理负担并提高透明度。因此，患者可以期待获得更高水平的服务。

此外，数据交换的延迟可能会导致负面（并且往往代价高昂）的医疗影响，包括受到信息阻塞处罚。因此，最近实现云现代化的医疗服务提供商正在迅速推出新格式的面向外部的 API，以遵守这些新的合规措施。

除了面临以 API 为重点目标的攻击风险之外，DDoS 和勒索软件等可用性攻击继续对所有行业产生重大影响，并且医疗保健行业是可能会受到严重影响的行业之一。旨在应对这些类型攻击的法规往往注重恢复能力。例如，美国卫生和人类服务部 (HHS) 发布了《医疗保健行业 DDoS 攻击防护指南》。此外，非营利的医疗保健信息共享和分析中心发布了一份关于医疗保健行业恢复能力问题的白皮书《Resilience is in our DNA》。

积极行动：抵御措施建议

API 安全比以往更加重要，这是我们从风险管理和合规角度得出的结论。但是，由于 API 蔓延，医疗保健 API 的识别、分类和保护变得越来越具有挑战性。此外，医疗保健服务企业必须抵御威胁服务可用性的 DDoS 攻击。

您无法抵御自己不知道的攻击。因此，您首先需要发现所有资产，以便将它们纳入自己的安全计划中。然后，您需要了解存在哪些漏洞，并对性能和安全方面发生的情况具有态势感知能力。最后，您需要通过自动化和传统的渗透测试来验证自己系统的安全性。

满足以下 API 和 DDoS 防护策略里程碑可帮助您实现更强大的安全计划。

五个 API 保护策略里程碑

采用强有力的 API 安全计划可帮助您增强对所有 API 的监测能力并了解您面临的风险，让您可以加强相关保护措施。

1. 可通过系统性地发现恶意或影子 API 来消除基础架构盲点，并确保每一个恶意或影子 API 都被停用或纳入 API 安全控制措施中。

2. 分析常见告警类型并更正 API 代码中的缺陷，解决错误配置问题，以及在吸取经验教训的基础上实施预防未来漏洞的流程，以此确定并增强风险态势。

3. 了解正常行为并根据 API 安全告警的激增来识别潜在滥用问题，以此增强威胁检测和响应能力。然后，采用明确定义的响应程序，将风险和告警量降低到正常水平。

4. 与提供培训和专业知识的供应商合作。他们应该提供从基于项目的支持到完全托管式服务的一系列服务，以帮助正确配置和管理复杂的集成网络安全解决方案。

采用强有力的 API 安全计划可帮助您增强对所有 API 的监测能力并了解您面临的风险，让您可以加强相关保护措施。

5. 通过制定正式的 API 威胁搜寻准则来建立更强的防御措施，目的是及早发现可能的威胁，以避免升级为更加被动的情况。

四个 DDoS 防护策略里程碑

随着针对第 7 层网页和 API、第 3 层和第 4 层基础架构以及 DNS 系统的 DDoS 攻击数量创下新纪录，确保服务和功能的可用性至关重要。现在，这意味着需要采取能够应对最新攻击的规模、范围和速度的主动保护措施。

1. 采用能够提供监测能力并对攻击作出快速响应的系统。这应当涵盖第 7 层、第 3 层和第 4 层以及 DNS 基础架构。

2. 使用混合 DDoS 抵御平台作为本地 DDoS 防护的备份，防止攻击造成本地设备过载。

3. 与医疗服务提供商合作或使用让您可以轻松管理策略和维护 IP 允许列表的系统，这些系统可实时提供具有实用价值的分析，帮助您构建主动安全态势。

4. 通过测试来验证您的告警、保护功能和危机管理流程，并确保您的所有基础架构都受到了相应的保护。

如需了解详细信息，请阅读我们最新的研究内容或访问我们的博客。

随着针对第 7 层网页和 API、第 3 层和第 4 层基础架构以及 DNS 系统的 DDoS 攻击数量创下新纪录，确保服务和功能的可用性至关重要。

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 应用程序和爬虫程序攻击数据集已经进行了数次更新。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《SOTI/安全性》发展的这一里程碑。

致谢名单

研究总监
Mitch Mayne

编辑与创作
Neil Jennings
Chris Notaro
Charlotte Pelliccia
Badette Tribbey
Maria Vlasak
Steve Winterfeld

审稿和主题撰稿
Claire Broome
Shane Keats

数据分析
Chelsea Tuttle

推广材料
Barney Beal

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

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 为抵御针对医疗保健行业的威胁而提供的解决方案，请访问我们的医疗保健和生命科学页面。