年度回顾

探索 2023 年网络趋势及未来

目录

实地案例

在编写这份《互联网现状》(SOTI) 报告时，我们改变了传统的年终回顾形式，不再逐一回顾今年发布的所有报告，而是重点讨论一个中心主题：今年您最关注的安全案例是哪个？我们邀请了 Akamai 安全情报组 (SIG) 的撰稿人和数据科学家，从我们过去 10 个月内收集的所有案例中任意选择一个进行年终评估。2023 年，我们在安全研究博客和 SOTI 报告中公布了许多值得关注的案例和新发现，只选择其中一个对他们来说肯定很困难。我们还请首席信息安全官 (CISO) 顾问和安全运营指挥中心 (SOCC) 副总裁评估了今年的攻击趋势，并总结了可以在 2024 年工作中加以利用的重要心得。

今年发生了很多网络安全事件，Akamai 也就此开展了大量的安全研究。不可否认，我们的安全专家在研究方面对业界做出了无可估量的贡献。在我们专门设立的安全中心，安全专业人员可以轻松获取可靠的资源，了解行业见解、防御策略和攻击趋势，从而更好地为企业构筑安全防线。他们还可以免费使用我们的 RPC 工具包和开源入侵模拟平台 Infection Monkey。Infection Monkey 好比在模仿恶意软件的行为，通过翻转位来传播和“加密”它可以访问的文件，让安全从业人员能够直观了解攻击者如何做到（或无法做到）在模拟环境中随处移动。在当前的威胁演变速度下，持续的测试很有必要。安全从业人员需要知道他们当下的网络状况，而不仅仅是上次渗透测试期间的情况。

如果要用一个词来概括 2023 年的形势，那就是“*转变*”。为了规避安全措施，攻击者改变了策略，试图寻找新的攻击面和未利用的目标，以期对各种规模和行业的企业造成严重破坏。安全防御人员也是如此，他们不断调整策略，并学习各种抵御攻击的新方法，希望能更好地保护企业。我们的解决方案、研究主题和工具也发生了转变，致力于为安全从业人员提供可行的见解和防御策略，因为他们和我们一样面临着相同的安全威胁。

祝阅读愉快！

医疗企业的软肋：医疗物联网的网络风险

我是 Badette Tribbey，SOTI 报告背后的案例编写人之一。我与安全专家和数据科学家合作，将技术发现和数据转化为有意义的见解。我讨厌数学，但我喜欢数字，因为它们能够揭示引人注目的攻击趋势。

我们今年讨论过一个最值得关注的话题：医疗物联网 (IoMT) 日益加剧的风险。这个话题与我们每个人都息息相关。在《钻过安全漏洞》和《勒索软件异常活跃》中，我们分析了医疗保健与生命科学领域的风险状况，以及该领域易受攻击的原因。其中一件事让我最有感触，那就是 MRI 设备、胰岛素泵和可穿戴设备等 IoMT 资产虽然给患者带来了福音，但却显著增加了医疗服务提供商的风险。由于医疗保健生态系统错综复杂，传统技术易受攻击，加上 IT 和网络安全人员配置问题，这些企业在周边网络的保护上已面临重重困难。此外，在这种环境中及时修补漏洞也是一项艰巨任务，因为其中存在多种系统或应用程序，更新也来自于不同的供应商，跟踪起来非常困难。

未经修补的 IoMT 设备是所有行业中最容易受到攻击的一种资产，它们可能会引发勒索软件攻击等危害性更大的威胁。随着 IoMT 呈指数级增长，API 的使用快速兴起，与此相关的漏洞也如雨后春笋般涌现，它们可能会成为攻击者攻破目标网络的立足点，也可能被滥用并导致数据泄露（图 1）。Cynerio 与 Ponemon Institute 合作对美国多家医院和医疗保健机构开展了一项研究，他们发布的联合报告表明，有一半以上的医院和医疗保健机构曾因 IoMT 设备的安全漏洞而遭受过网络攻击。

> “在这种（医疗保健）环境中及时修补漏洞也是一项艰巨任务，因为其中存在多种系统或应用程序，更新也来自于不同的供应商，跟踪起来非常困难。
>
> ——Badette Tribbey，Akamai 高级技术撰稿人

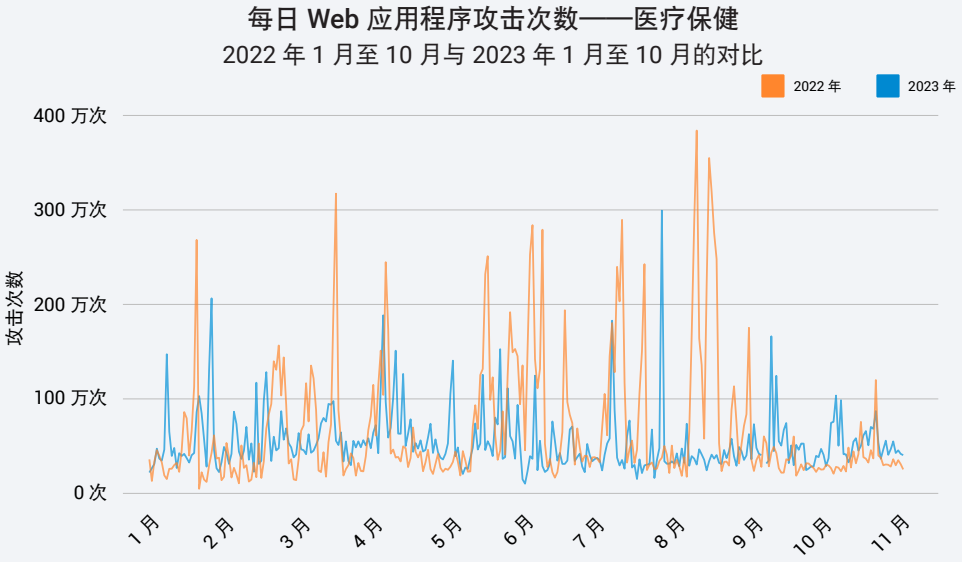


图 1：在 2022 年至 2023 年间，医疗保健 / 制药行业的 Web 应用程序和 API 攻击活动趋于稳定，并有零星的峰值。尽管攻击次数同比下降了 21%，但 2023 年每天的攻击次数中位数仍高于 2022 年。

医疗保健行业未来如何?

随着医疗保健行业不断扩大 IoMT 的使用范围，API 将继续在医疗服务的便利性方面发挥关键作用（例如远程医疗和远程患者监护），帮助该行业改善临床结果并提升财务业绩。由于健康档案和患者数据在暗网上价值很高，针对医疗保健行业的攻击可能会不减反增。

当我们将目光从当下转移到未来时，攻击者显然也会不断花样翻新，进一步扩大攻击范围并加大攻击的复杂性。未来可能会继续出现更多利用零日漏洞实施的技术攻击。此外，监管环境也在发生变化，包括但不限于 2022 年出台的《网络医疗安全保护和变革法案》(PATCH)。因此，我们需要确保我们的解决方案能够帮助企业满足大量即将出台的法规，包括隐私保护、信息披露、支付、数据主权和弹性方面的法规。最后，CISO 若是能将更多预算用于整合筛选供应商，并采用能够最大限度减少黑客入侵后的停留时间的解决方案，将更有可能瓦解攻击者的攻势。

揭露使用 JSON Web 令牌进行 API 识别的重大威胁

我是 Lance Rhodes，从 2023 年 3 月起在 Akamai 的 SIG 团队担任网络安全撰稿人。我做的很多工作就像是报告与博客之间的“联结纽带”，因为我一直负责博客文章和分段研究报告的发布和编写，以及 SOTI 报告内容和营销材料的撰写。我和团队在编写每月的内部和外部新闻稿以及安全会议陈述材料时，会将所有这些信息整合到一起。

说到今年我写过最令人激动的一篇博客文章，我认为是关于 JSON Web 令牌 (JWT) 的博文。这篇博文与应用程序和 API 的 SOTI 报告（《钻过安全漏洞》）有直接联系，文中详细阐述了 JWT（标准 API 识别方法之一）中失效的身份验证。我认为，能更深入地了解 JWT 很有意思。

今年初完成应用程序和 API 的 SOTI 报告后，我开始和 Nitzan Namer 一起撰写关于 JWT 的博文。这篇文章重点阐述了 JWT 作为攻击媒介会造成失效的用户身份验证，这是开放式 Web 应用程序安全项目 (OWASP) 十大 API 安全漏洞之一。SOTI 报告有一个部分专门讨论了这个问题，而博客文章则更深入地探讨了 JWT 结构，以及防止权限升级、数据泄露和帐户接管等严重威胁的最佳实践。

记得我和 Nitzan 说过，我们希望安全研究人员、技术从业人员以及 JWT 用户和管理员能够将这篇博文作为一种持续的资源加以利用。这篇文章的结构风格帮助我们实现了这个愿望 — 文章首先解释了 JWT 基本原理，然后介绍了六种案例场景，包括用实例阐述一些常见威胁，并指出应对每种威胁的最佳实践。基本原理部分解释了 JWT 如何通过发行令牌（其中包含的信息会作为 JSON 对象进行共享）来保护 API。每个令牌都经过编码（但未加密），并由标头、有效负载和验证签名（确认从服务器生成令牌以来数据未被更改）组成。

> 本博客文章更深入地探讨了 JWT 结构，以及防止权限升级、数据泄露和帐户接管等严重威胁的最佳实践。
>
> ——Lance Rhodes，
> Akamai 网络安全撰稿人

这六种案例场景是：

1. 允许服务器使用未经验证的令牌
2. 将同一私钥用于不同的应用程序
3. 使用弱签名算法
4. 选择较短并且/或者低熵的私钥
5. 在 JWT 的有效负载中存放敏感数据
6. 密钥混淆

JWT 是一种常见的验证形式；由于它造成的攻击面较大，并且很容易出错，所以恰当的安全措施至关重要。这些场景展示了 JWT 的一些常见威胁，但还有更多威胁存在，而且攻击手段也在不断演变。

JWT 既没有加密，在实施过程中也未考虑安全性

我从这篇博文中得出一个重要信息，那就是 JWT 既没有加密，在实施过程中也未考虑安全性。如此受欢迎的身份验证令牌竟然存在这样的漏洞，真是令人难以置信。JWT 之所以吸引人，一个方面在于它让人无需频繁登录便可使用许多 Web 应用程序和 API。SOTI 报告和 JWT 博客文章都分析了 Akamai 流量中的 JWT 算法，并确定对称算法是其最常见的算法，但对称算法在理论上安全性较低，而且保护效果也不如非对称算法。例如，报告和文章均显示有 54.8% 的 Akamai 客户使用 HS256 对称算法。

对称算法的使用之所以更常见，很可能是因为用户只需要一个密钥，而不对称算法则需要更多的计算资源。JSON Web 加密（JWT 的加密版本）也不常用。大多数公司都使用 JWT，这样选择是为了节省计算能力。

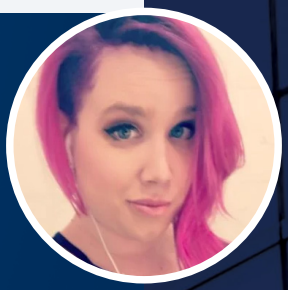
结论：比起安全性，人们更看重便利性、成本和速度。这是一个有益的提醒，让我们认识到安全研究人员和撰稿人的工作重要性。要想在效率和安全性之间取得令人满意的平衡，高质量的安全研究和实践很有必要。

如此受欢迎的身份验证令牌竟然存在这样的漏洞，真是令人难以置信。

——Lance Rhodes，
Akamai 网络安全撰稿人

Outlook 绕过漏洞

大家好！希望你们今天过得愉快！我叫 Tricia Howard，在 SIG 负责博客相关的工作。技术评论是一项需要挖掘事实真相的工作，我的合作对象包括我们的研究人员、企业传播团队和法律部门等，我们致力于及时有效地发布这些文章。我的工作有一点非常吸引人，那就是我可以夸奖我们的研究人员，因为他们的工作确实做得很出色！



在我今年写过的所有文章中，这篇写起来可能最难落笔。但我们团队过去 12 个月完成了大量优质的研究，我怎么可能只喜欢其中一项？如果必须要选择一项，我会选择 Ben Barnea 对也许已广为人知的 Outlook 绕过漏洞的研究。Ben 是我认识的一名出色研究人员，他只用了一个斜线号便让整个补丁失去作用。我知道这听起来很夸张，甚至不可能——但事实如此，他做到了。

原始漏洞允许未经授权的攻击者发送带有自定义通知声音的 Outlook 邀请。这种声音同时也是一种攻击路径，可将客户端连接到攻击者的服务器，导致 NTLM 凭据泄露。这是一个严重漏洞，攻击者可以利用它来暴力破解用户凭据，或者执行中继攻击。当然，所有这些活动都可能导致权限升级，而我们都知道结果会是什么。最糟糕的是，这是一个零点击漏洞，也就是说不需要用户执行任何操作便可触发攻击。这背后需要强大的实力，也说明它非常危险，尤其我们了解到这种攻击来源于俄罗斯，并且已经四处蔓延，渗透到了欧洲的很多政府机构。

漏洞补丁已在三月份发布。该补丁使得攻击者无法再使用 *PidLidReminderFileParameter*，因而也就无法指定自定义路径（连接到攻击者的服务器）。而且，该补丁利用了 *MapURLtoZone* 功能来检查路径是否尝试连接到互联网。如果路径尝试连接到互联网，则会播放传统的通知声音，从而消除了自定义通知的文件路径选项。从理论上讲，这取消了远程攻击者利用此漏洞的选项，因为要想在攻击者和受害者之间建立连接，最终都得向互联网发出请求。

攻破补丁

接下来，事情开始变得有趣了，我认为这确实很有意思。作为一名出色的研究人员，Ben 想要验证这个漏洞是否真的无法再被利用。这样说可能过于简单，但 *MapURLtoZone* 本质上只有两个选项：允许或拒绝。具体取决于是否向互联网发出请求。在大多数情况下，该补丁都发挥了预期的作用。即使路径看似是指向本地，*MapURLtoZone* 也会在它试图访问互联网时识别出来并加以阻止。

> 网络安全人员每天有很多工作要做，他们没必要为新的零点击权限升级漏洞而担忧。
>
> ——Tricia Howard，
> Akamai 高级技术撰稿人

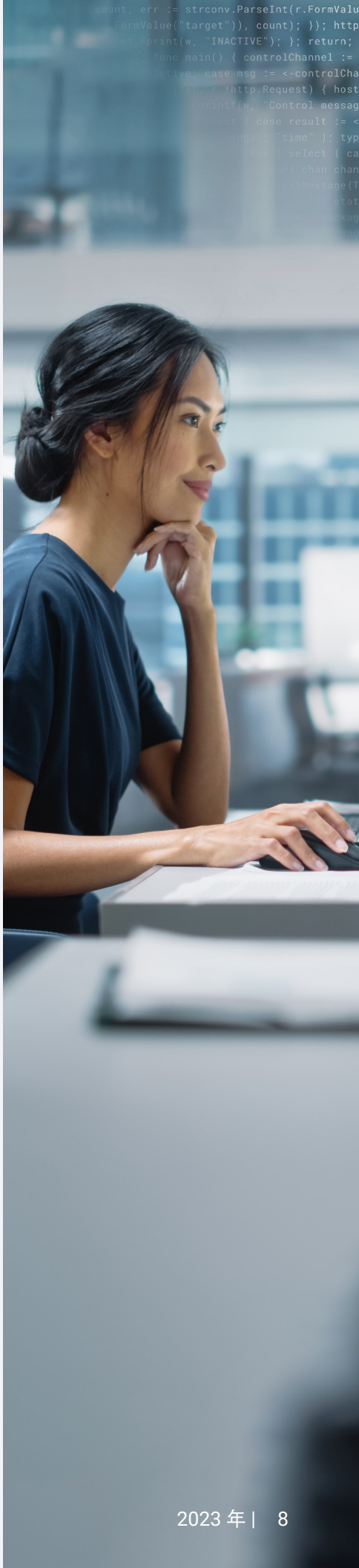
Ben 决定在路径名末尾添加“/”来验证一下。哪怕您给 *MapURLtoZone* 提供了不合常规的内容，它也得决定是允许还是拒绝。添加的斜线未被识别出来，而是返回了 0，函数将其视作本地路径并予以信任。然后，通过利用 *CreateFile* 指定自定义路径，便能够按照预期方式执行其余部分的漏洞。

就这么简单！只是添加了一个不起眼的斜线号，针对**关键**漏洞设计的整个补丁就突然变得不再有效了。网络安全专业人员为了消除威胁，可能花费了几天、几周甚至几个月的时间和精力来开发这个补丁，却被简单的一个斜线号就攻破了。

原始攻击十分复杂，在阻止时确实很耗神费力，就像在与攻击者下一局漫长的象棋比赛一样，难度直逼国际象棋大师马格努斯·卡尔森的级别。但我们只用了一个斜线号就导致补丁失去作用，不难想象攻击者最终也会找到绕过补丁的办法。幸好 Ben 打破常规发现了这个漏洞，避免了它被攻击者利用。

为什么说发现这些漏洞的研究人员是维护网络安全的生力军，原因就在于此。网络安全人员每天有很多工作要做，他们没必要为新的零点击权限升级漏洞而担忧。安全研究人员正在为世界带来切实的改变，特别是随着我们的日常生活越来越离不开技术和互联网，这种改变愈加重要。

我很自豪能够成为这个优秀团队的一员，与这些“大神们”一起工作。我想对所有读过我们博客、推文和 SOTI 报告的人说一声谢谢！也想对 Akamai SIG 内部和外部的研究人员说：感谢你们付出的所有努力！让我们一起期待明年更精彩的故事!



新数据和新兴威胁：敲响 Magecart 攻击的警钟

我是 Chelsea Tuttle，已经在 Akamai 工作了将近八年。作为一名数据科学家，我在过去四年里负责 SOTI 报告中的数据部分，大部分时间都在清理、研究和分析数据并进行数据可视化。除了关注数据，我还与 SOTI 报告的撰写人密切合作，帮助传达数据背后的案例。鉴于大数据的复杂性和报告历史数据的益处，我们通常不会添加新的数据集，但今年却这样做了！回顾 2023 年，我要首推与这个新数据集有关的案例，因为我很喜欢这项举措所带来的学习机会。

我们在工作中常常专注于报告网络中发生攻击的次数，而忽略了其他数据，这些数据可能是保护潜在漏洞和阻止攻击的重要机会。今年我们在 SOTI 报告中添加的一个数据集就很特别，因为它突显了潜在的漏洞区域，而不是关注攻击次数。该数据集来源于 Akamai Client-Side Protection & Compliance 的观察结果，这个敏锐的工具每天都会对数十亿个网页脚本进行检测。我们密切关注的其中一个潜在漏洞区域是跨网站使用的第一方和第三方脚本数量。虽然使用第一方脚本并不能保证安全，使用第三方脚本也不是必然存在漏洞，但对其他方越信任（例如让第三方托管网页脚本），安全风险就越高。随着第三方脚本在各行各业的使用越来越普遍，便利性与安全性的矛盾也日渐突出，Akamai 正努力寻求二者的平衡。

从我们 2023 年 6 月发布的 SOTI 报告——《商业行业的威胁趋势分析》中可以看到，Akamai 今年的一个重点研究领域是最近的 Magecart 式 Web 数据窃取攻击；具体而言，我们观察到 Magecart 攻击正在持续入侵数字商务行业。攻击者使用恶意 JavaScript 代码注入的手段，试图从数字商务网站的购物车窃取敏感用户凭据，例如信用卡信息。这种类型的攻击对于攻击者来说往往很容易，但给消费者带来了巨大的风险，同时也变得越来越难以检测。这些 Magecart（或 Web 数据窃取）攻击通常在网站用户或所有者没有意识到的情况下发生，攻击者通常会选择那些使用易受攻击或过时的软件的数字商务网站。

> 随着第三方脚本在各行各业的使用越来越普遍，便利性与安全性的矛盾也日渐突出，Akamai 正努力寻求二者的平衡。
>
> ——Chelsea Tuttle，
> Akamai 高级数据科学家

Magecart 的新变体

在 Akamai 研究人员近期发现的 Magecart 攻击活动中，我们可以看到很多 Magecart 变体。我们在 2023 年 6 月的 SOTI 报告中重点分析了 Magecart 客户端攻击，并指出来自开源库的第三方脚本中存在被利用的漏洞，这些漏洞可能会引发供应链攻击。在撰写 SOTI 报告后不久，我们发布了一篇博客文章，介绍 Akamai 研究人员发现的新型 Magecart 攻击活动，这种攻击通过滥用合法网站来攻击其他目标。在这种攻击活动中，本质上有两组受害网站：被劫持用于托管的合法网站，充当攻击者控制的服务器；易受攻击的商业网站，这些网站会遭受客户端 Web 数据窃取攻击。第二篇博客文章在 8 月发布，阐述了 Akamai 研究人员发现的另一种新型 Magento 攻击活动，攻击者通过不易察觉的服务器端模板注入手段，利用数字商务网站收集受害者的付款信息。

Akamai SIG 最新发布的 Magecart 博客文章介绍了一种新的混淆技术，攻击者通过操纵网站的默认 404 错误页面来隐藏恶意代码。Akamai 研究人员发现这种新的攻击活动包含另外两种高级隐藏技术，这表明攻击者在不断改变策略，以延长攻击链并避开检测。

2023 年即将结束，回想起新数据和新兴威胁在研究和报告方面存在的价值，我不禁也期待着 2024 年将会获得的新数据和学习机会。

Akamai 研究人员发现了一种新型 Magecart 攻击活动，这种攻击通过滥用合法网站来攻击其他目标

值得注意的区域攻击趋势

我是 Charlotte Pelliccia，我在 2023 年加入了 SOTI 团队，负责编写亚太和日本 (APJ) 地区以及欧洲、中东和非洲 (EMEA) 地区的案例。APJ 和 EMEA 地区简报是我们全球 SOTI 报告的补充。在此，我将回顾 2023 年我们所报告的一些重要攻击趋势，并更新年初发布的简报数据。

Web 应用程序和 API 攻击 — 情况最严重的两个行业

正如我们最新的金融服务业和商业行业 SOTI 报告所述，金融服务业仍然是亚太地区及日本遭受 Web 应用程序和 API 攻击最严重的垂直行业，商业行业次之。从我们 2023 年 6 月发布报告以来，针对金融服务业发起的攻击已超过 45 亿次（相比之前的 37 亿次增加了 22%）。此外，从我们 2023 年 3 月发布报告以来，商业行业遭受的攻击从 12 亿次攀升到了 19 亿次，增加了 58%。各子行业发生攻击的比例保持相对稳定（图 2）。

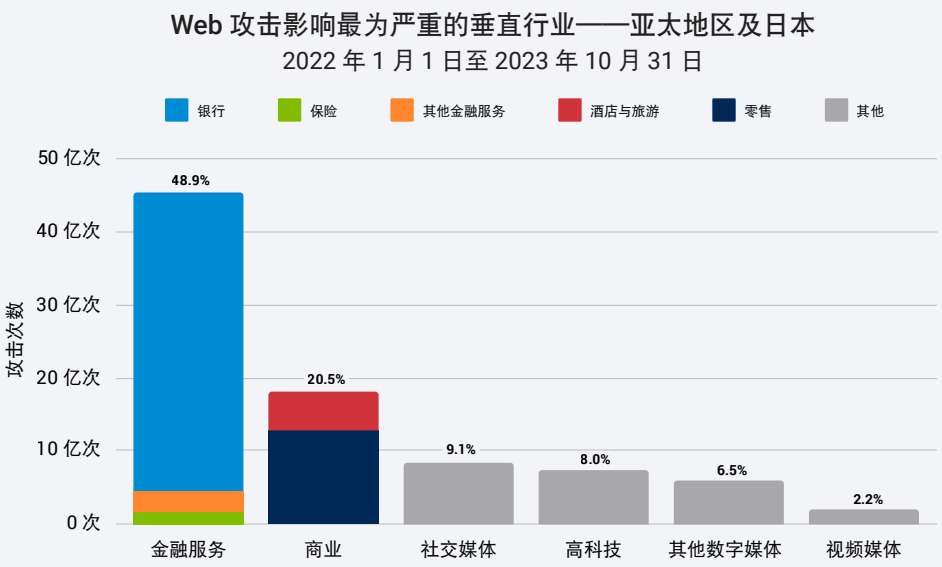


图 2：截止 2023 年 10 月 APJ 地区各行业的网络攻击情况

> 清晰了解区域攻击趋势，对于帮助企业更好地理解其风险并调整其工具和最佳实践至关重要。
>
> ——Charlotte Pelliccia，Akamai 网络安全撰稿人

与此同时，在欧洲、中东和非洲地区，商业行业仍然是遭受 Web 应用程序和 API 攻击最严重的行业，自我们 2023 年 3 月发布报告以来，攻击次数现在已突破 65 亿次（比先前的 46 亿次增加了 41%）。从 2023 年 6 月发布报告以来，尽管制造业从第四位上升至第三位，取代了金融服务业，但金融服务业遭受的攻击仍从 10 亿次增加到了 17 亿次，攀升了 70%。在该区域内，各子垂直行业遭受攻击的比例同样保持相对稳定（图 3）。

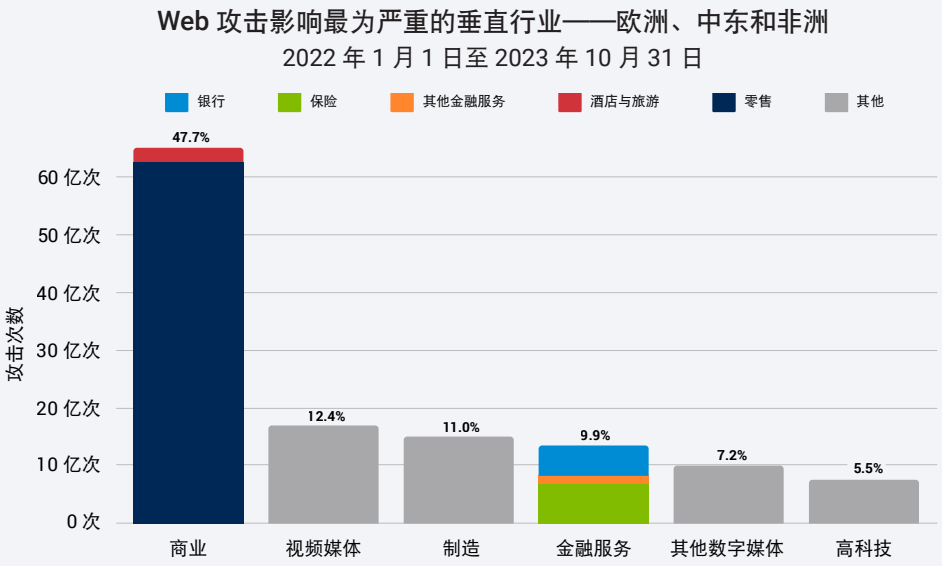


图 3：截至 2023 年 10 月 EMEA 地区各行业的网络攻击情况

恶意爬虫程序成为攻击者的首选武器

亚太地区及日本遭受的恶意爬虫程序攻击次数仅次于北美，这和我们之前的报告中所述的情况一致。2022 年 1 月到 2023 年 10 月期间，亚太地区及日本遭受攻击最多的三个垂直行业分别是商业行业 (27.4%)、视频媒体行业 (15.0%) 和金融服务业 (14.3%)。在欧洲、中东和非洲地区，半数 (50.1%) 的恶意爬虫程序攻击发生在商业行业，紧随其后的是其他数字媒体行业 (15.3%) 和视频媒体行业 (12.2%)（图 4）。

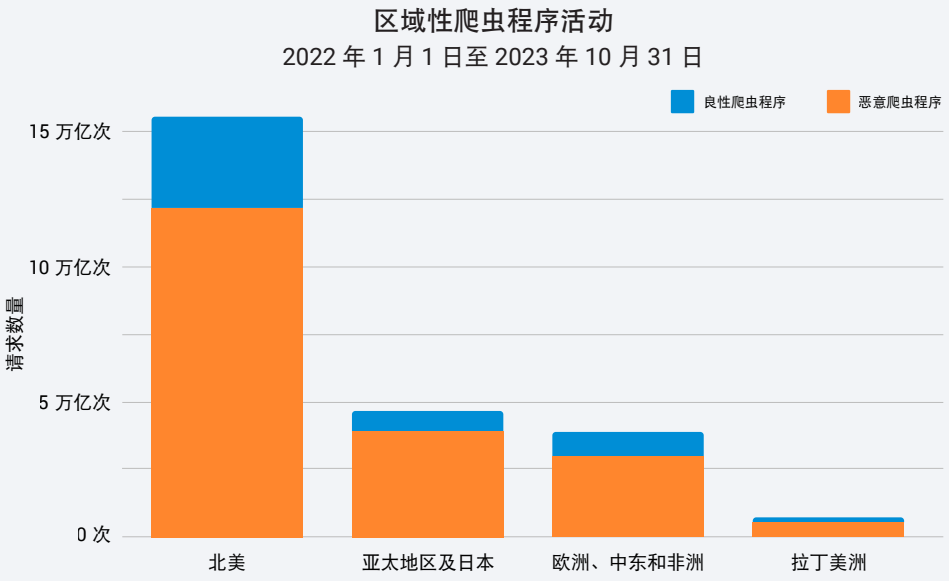


图 4：恶意爬虫程序的使用在所有地区都很普遍，远超过良性爬虫程序的使用

请参阅下面的文章，了解我们的 SOCC 对爬虫程序和 DDoS 攻击变化趋势的分析见解。

欧洲、中东和非洲地区处于 DDoS 攻击区域转变的十字路口

我们在 2023 年的报告中明确指出，攻击者已将目光瞄准欧洲、中东和非洲地区，这部分原因在于当前的地缘政治环境。举一个典型例子：EMEA 地区金融服务业、博彩业和制造业发生分布式拒绝服务 (DDoS) 攻击事件的次数超过了其他所有地区的总和（图 5）。

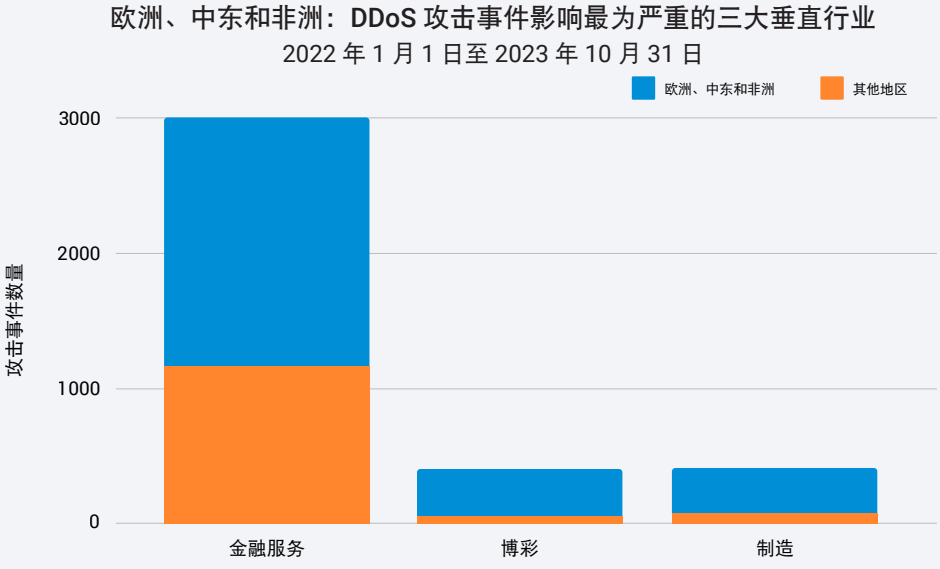


图 5： EMEA 地区这些行业发生的 DDoS 攻击事件超过了其他所有地区的总和

展望未来

只要攻击者实施的网络攻击、爬虫程序攻击和 DDoS 攻击得逞，我们就可以合理预见到这些攻击方法仍然是攻击者的首选武器。事实上，这三种媒介已经在演化，以维持或聚集力量。Web 应用程序零日攻击正在与勒索软件攻击相结合（例如 CL0P 等勒索软件团伙采用的攻击手段），并开始纳入 DDoS 攻击，以形成三重勒索策略。利用爬虫程序进行 Web 抓取已成为几乎所有的航空公司重大活动或机票销售的新常态。以 API 业务逻辑为导向的 API 攻击不断涌现。

为应对这种局面，全球各地各行业的监管监督和报告义务不断加重，因为没有哪个地区或行业可以幸免。这样做的目的是使网络安全法规与不断变化的威胁态势保持同步。企业需要对履行报告义务始终保持警醒，并准备好采取多层防御措施来降低风险。

把脉全球网络安全大势：来自我们安全运营指挥中心的见解

我是全球安全运营副总裁 Roger Barranco。我在 Akamai 工作十几年了，负责公司的托管安全运营业务，我们在全球设有六个 SOCC，并有一支出色的团队提供支持。我的职业生涯始于网络安全，我被这个领域所吸引是因为这是一个非常有意思且不断变化的市场——2023 年就是一个很好的例子。

Akamai SOCC 从未如此忙碌——到 2023 年底，我们完成的安全工单将比去年增加约 30%。在为客户提供托管安全服务的过程中，我们总结了以下这些重要见解，供各行企业在 2024 年参考借鉴。

DDoS 攻击花样翻新

虽然从历史上看，遭受攻击的客户数量逐年增加，但如今的攻击方法已经不同往日。首先，受到攻击的客户资产类型和体量发生了变化。例如，攻击者不再对相同或相似的端点发起 10 次攻击，而是会对客户网络空间中的不同 IP 发动 100 次攻击。而且这些攻击不仅针对第 3 层，还同时针对第 7 层。此外，针对 DNS 的攻击急剧增加，其中大部分是有效查询攻击，很容易拖垮客户的 DNS 基础架构。仅仅是几兆不必要的 DNS 流量，就可能给企业带来巨大的压力。令人担忧的是，Mirai 活动也开始死灰复燃，这种攻击因利用物联网的力量造成大规模破坏而臭名昭著。

在当前的威胁态势下，只是在边缘部署强大的防备力量并不足以应对攻击。企业需要强大的云安全服务来承担该工作负载，从而维持防护状态并为每个端点实施独特的保护。从平台和服务的角度来讲，这都是 Akamai 的优势所在。我们可以采用多层安全措施来防御全方位的网络攻击。而且，我们的实践专家可以分析不同客户的细微差别和趋势，采取极具个性化的方式进行监控和抵御，从而防止恶意入侵，同时又能允许符合预期的干净流量通过。

> Akamai SOCC 从未如此忙碌——到 2023 年底，我们完成的安全工单将比去年增加约 30%。
>
> ——Roger Barranco，Akamai 全球安全运营副总裁

抵御爬虫程序是一场残酷的战争

撞库攻击很令人头疼，因为很难区分不必要的流量和必要的流量，而且客户的后端千差万别，需要采取的抵御措施也可能截然不同。此外，撞库攻击者往往技术高超还非常警觉，因为这种攻击一旦得逞，攻击者就可以轻松获利。这些爬虫程序攻击十分危险，并会造成高昂的成本，因此拥有撞库防御解决方案非常重要，特别是在恶意爬虫程序使用量持续攀升的金融服务业和商业行业。

EMEA 地区仍是攻击者的目标

自俄乌冲突以来，EMEA 地区（特别是欧洲）取代了美国，成为网络攻击最严重的地区，各行各业都遭受了不同类型的攻击，尤其是 DDoS 攻击。这种转变凸显了一个事实：许多攻击者都是民族国家或对民族国家抱有同情者，而且他们对欧洲的关注并未减弱。

攻击者越来越成熟

过去，脚本小子是网络安全的主要威胁。他们利用常见的工具发起攻击，寄希望于好运降临；或者以每小时 10 美元的价格租用 DDoS 僵尸网络，试图击败视频游戏竞争对手。但这样的时代早已不复存在。现在，攻击者已变得更加老练，他们会密切关注特定的目标，规划自己的策略，有时甚至提前一年进行侦察，并利用在此过程中发现的潜在弱点精心策划攻击。由于攻击者已经提前做好了准备，如今攻击活动的持续时间会变得更长，不再像过去那些年一样常常只持续几分钟。

> 由于攻击者已经提前做好了准备，如今攻击活动的持续时间会变得更长，不再像过去那些年一样常常只持续几分钟。
>
> ——Roger Barranco，
> Akamai 全球安全运营副总裁

保持网络与运营相协调的最佳实践

尽管面临这些挑战，但客户可以参照这里的两项最佳实践以保持网络与运营相协调，让 Akamai 成为他们网络团队的外援，从而提高网络安全保护措施的有效性。首先，客户在平静期就应该与 SOCC 合作，预先建立防御体系，而不是等到攻击发生时再来亡羊补牢。这样就可以提前阻止攻击而避免影响生产。此外，客户将收到后续跟进报告，详细说明被阻止的攻击情况。

其次，客户应该主动做好运营准备工作，并制定备份计划。例如，他们应确保自己知道在测试期间如何进出不同的平台。如果存在运营问题，五分钟的攻击可能就会造成客户停工一小时，所以除了做好准备应对单纯的网络问题之外，在运营方面做好准备也同样重要。

今年的情况凸显出网络安全不断变化的态势，我们预计这种变化会继续存在。好消息是，这里的见解可以帮助客户领先一步，在 2024 年做足自我保护。

CISO 顾问分享让他豁然开朗的时刻及更多体会

我叫 Steve Winterfeld，是 Akamai 的 CISO 顾问。我曾经担任 Nordstrom 银行的 CISO，以及 Charles Schwab 的事件响应和威胁情报总监。我的职责是确保我们的合作伙伴成功保证其客户的安全，并且确定我们应集中自身能力对哪些领域进行攻坚。

今年出现了一些令我惊讶的趋势，还有一些已被数据证实的规律，我们可以参照这些来更新我们的策略。今年最让我关注的九个案例中包含了豁然开朗的时刻、意料之中的消息和难以改变的局面。

豁然开朗的时刻

- 总共有 10% 到 16% 的企业每季度至少遭遇了一次针对其网络的命令和控制 (C2) 流量攻击。此外，有 26% 的受感染设备访问了与初始访问代理相关的域。
- 就勒索软件威胁态势而言，过去六个月内攻击手段出现了令人担忧的转变，零日漏洞和一日漏洞滥用猖獗。
- Akamai 的研究发现，相比其他类型的攻击者，多个勒索软件团伙在发起初次攻击后的三个月内对受害者发起后续攻击的可能性要高出近 6 倍。

意料之中的消息

- 以 API 业务逻辑为导向的 API 攻击非常复杂，很难检测和抵御。因此，也就很难在单独的请求中加以确定。
- 企业需要确保遵守《支付卡行业数据安全标准》(PCI DSS) v4.0 中的新要求和《数字运营弹性法案》(DORA) 的规定。

> 这些见解是很好的指南，可以帮助您对安全计划进行模拟演练，了解哪里有多余的工具或需要填补的缺口。
>
> ——Steve Winterfeld，Akamai CISO 顾问

难以改变的局面

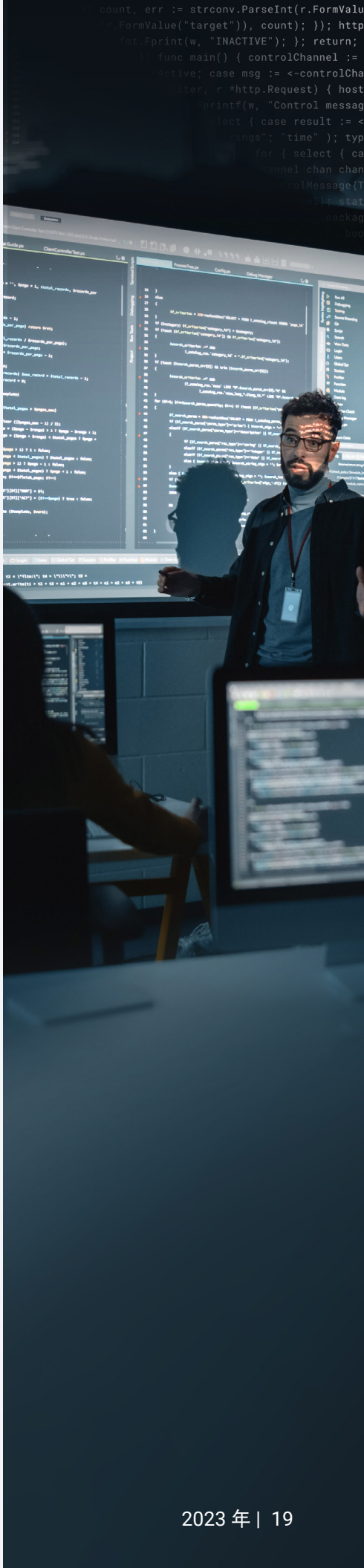
- 爬虫程序和 API 攻击的数量持续增长，DDoS 攻击不断刷新记录。
- 金融服务业、高科技行业和商业行业往往是受攻击最严重的行业。
- 本地文件包含 (LFI) 是攻击者最常利用的攻击手段。
- DDoS 攻击最多的地区正从北美转向欧洲。

引人深思的一个重要发现是，已证实 C2 通信中出现了入侵迹象。尤其令人不安的是，在恶意软件已经成功侵入系统并建立通信之后，首次检测的频率仍然很高。这说明了在预防措施与快速检测之间达到平衡的重要性，这样才能尽可能降低影响。

最让我惊讶的案例涉及到攻击手段从利用社会工程学转变为利用零日漏洞。在过去几年里，我感觉我们的技术防御越来越强，我需要做的是借助培训和监督来强化员工队伍。但是今年出现了向零日攻击转变的趋势，所以我需要认真考虑明年的资源如何部署。

在企业已经遭受勒索软件攻击或者正从攻击中恢复时，如果再次发生攻击，也许就会出现失衡的情况。 我们很容易过度关注眼前的危机，因而不惜调取负责持续性防御监控的资源。这种失衡可以让我们清楚地认识到，任何时候也不能卸下防御！

这些见解是很好的指南，可以帮助您对安全计划进行模拟演练，了解哪里有多余的工具或需要填补的缺口。您可以依照这些指南进行练习，以便更新行动手册/流程，并且引导培训、增强渗透测试计划或者支持风险组合评估。网络安全需要团队合作，所以这些见解对于推动与内部合作伙伴（例如法律或 IT 团队）和供应商的讨论也很有作用。同样，美国国家标准与技术研究院 (NIST)、MITRE ATT&CK 知识库和 OWASP 十大安全风险等参考框架/工具都是很好的资源。



展望未来

未来无法预测，但可以预见的是，DDoS 和 API 攻击将在 2024 年占据主导地位。网络攻击者仍致力于建立更大规模的僵尸网络大军并开发新的攻击技术，再加上民族国家的影响，将导致 DDoS 继续增长。这个因素与勒索软件的演变结合在一起，将成为推动立法和提高弹性的源动力。

转型需求继续推动着 API 在大多数行业的广泛实施。这种快速扩张将在无意中导致更大的攻击面和更多漏洞，以及影子 API、僵尸 API 和 API 滥用。针对 Web 应用程序和 API 的攻击预计会显著增长。这种增长源于 LFI 等标准攻击，以及服务器端请求伪造 (SSRF) 和服务器端模板注入 (SSTI) 等新型攻击手段，这将使可以检测横向移动并减轻影响的工具成为必备条件。

最后，除了一些特定的行业和地区之外，我们认为技能熟练的网络安全专业人员总体上会出现短缺。机器学习和大型语言模型人工智能会缓解一部分压力，但总体而言，我们将很难找到并留住需要的人才。这将促使我们与供应商合作，按需配置工作人员，或寻求非必要功能的托管服务。

至于 Akamai SIG，我们会继续针对普遍存在的威胁和即将出现的新型安全风险发出警报。我们将通过我们的平台和渠道与网络安全领域的伙伴开展合作，以加强威胁情报工作。2024 年是我们发布 SOTI 报告的第 10 年！我们很高兴可以利用新的数据集、视觉辅助工具和重要见解来继续完善我们的报告，这将能够为安全专业人员提供支持，帮助他们保护好各自所在的企业。

我们期待明年可以分享更多的研究见解。最后，祝大家安全无忧！

致谢名单

编辑与创作

Roger Barranco
Tricia Howard
Charlotte Pelliccia
Lance Rhodes
Badette Tribbey
Chelsea Tuttle
Steve Winterfeld

审稿和主题撰稿

Kimberly Gomez
Reuben Koh
Emily Lyons
Richard Meeus
Carley Thornell

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 为抵御威胁提供的解决方案，请访问我们的**安全解决方案页面**。