SOTI

第 10 卷，第 5 期

应对安全威胁狂潮

金融服务业的攻击趋势

Akamai

互联网现状/安全性

目录

前言

金融服务业不仅是全球经济的基石，也是经济增长和发展的命脉。金融服务涵盖众多不同的行业，例如商业银行、支付服务提供商、资产管理公司、投资银行和保险企业，整个业态不断发展演变。

技术进步持续重塑金融服务业的前景，催生了数字银行、智能投资理财顾问和加密资产等金融科技 (fintech) 领域的创新。全球金融科技公司的数量激增，走在最前列的是中美两国。截至 2024 年 1 月，全球最大的 10 家金融科技公司中，有 8 家位于这两个国家。这种技术上的转变还反映在无现金交易数量的增长上，而且此类交易仍有巨大增长潜力，尤其是在金融服务覆盖较为有限的地区。但漏洞与创新相伴而来。

网络犯罪分子无休止地尝试攻击金融机构，而攻击造成的影响远不止财务损失。诸如运营中断、声誉受损以及招致严厉的监管处罚等后果，会侵蚀金融服务业赖以生存的信任基础。当今的数字化转型速度一日千里，而网络威胁的复杂度也随之攀升，金融机构如何才能建立有效的防御措施？

这份《互联网现状》报告旨在帮助全球的金融服务专业人士（Akamai 客户、网络安全研究人员以及行业领导者等）应对日益复杂的威胁形势。作为网络犯罪分子的主要目标，金融服务业需要各方群策群力，以保障关键基础架构的安全、保护企业和客户、确保金融市场的稳定以及防止经济动荡。对于相关从业人员而言，要想领先攻击者一步，为行业关键资产建立强大防线，继续保持全球金融关系赖以存在的可信和可靠形象，请务必阅读本报告中的研究内容。

通过合规性、运营弹性和网络安全措施来强化金融服务

当今全球金融部门面临的关键挑战之一是必须增强合规性和运营弹性。随着监管形势的变化，金融机构必须主动进行调整，才能满足这些新的要求。例如，刚出台的《数字运营弹性法案》(DORA) 强调了企业有必要建立一个稳固框架，以便应对与信息和通信技术 (ICT) 相关的中断问题。DORA 将于 2025 年 1 月生效，该法案要求金融实体及其 ICT 第三方提供商制定全面的弹性策略，强制要求各公司增强安全措施和事件响应能力。

美国证券交易委员会的最新指南进一步扩大了对全面的网络安全方法的需求。现在，金融机构需要在其战略中融入运营弹性和灾难恢复措施，并高度重视网络风险的重要性。这涉及到深入了解重大威胁和事件会对财务稳定性和运营造成哪些影响。此外还要求及时披露重大网络安全事件，以及在年报中详细阐述风险管理策略，这体现了监管部门期望推动行业的模式转变。要想满足这些监管环境要求，金融机构需要与能够提供尖端安全解决方案和监测能力的公司建立合作关系。正如本研究所介绍，Akamai 可利用自身的专业知识来帮助金融服务企业，使之不仅能够实现合规性，还能面向严格的监管要求保持运营完整性。

考虑到这些发展情况，金融机构必须采用一种全面的方法来满足复杂的合规性和运营弹性要求。这包括识别可能会对投资者的决策过程造成显著影响的重大风险，并确定其优先级。金融机构必须将这些重大风险纳入风险管理框架中，并确保实施稳健的事件响应计划。金融机构通过采用多层深度防御战略，可以为高效地实现运营弹性铺平道路。这包括通过网络分段和微分段来减少攻击面，实施静态数据加密方法，强化服务器，以及结合使用 Web 应用程序防火墙与高级威胁监测系统。要想及时识别和缓解风险，持续监控和采用定期安全评估机制非常关键。

对于金融机构而言，根据最新的威胁情报和研究（例如，Akamai 的《互联网现状》(SOTI) 报告）来开展事件响应计划演习也非常重要。这些演习有助于构建一个模拟真实情况的场景，确保机构能够适应不断出现的新型工具、技术和程序。在越来越动荡的威胁形势下，要想确保运营弹性和维护客户信任关系，必须秉持这种积极主动的态度。随着金融服务业的发展，合规性、运营弹性和网络安全等各种要求交织在一起，不断影响该行业的未来。金融机构通过采用先进的安全措施并增强监测能力，能够从容应对复杂的监管要求并保障运营，从而维护对业务至关重要的信任关系。

Teresa Walsh
FS-ISAC 全球情报主管

关键见解

34%

金融服务机构遭受的第 3 层和第 4 层 DDoS 攻击事件百分比

金融服务业仍然是遭到第 3 层和第 4 层分布式拒绝服务 (DDoS) 攻击事件最多的行业。其后是游戏行业和高科技行业，分别占到 18% 和 15%。这种威胁类型的泛滥可能源于持续上演的地缘政治紧张局势，尤其是巴以冲突和俄乌战争，这些战争促使了全球黑客活动激增。

API 使用量增长引发了第 7 层 DDoS 攻击的攀升

虽然 Web 应用程序一直以来是网络攻击的主要目标，但在本报告所覆盖的期间内，针对 API 的第 7 层 DDoS 攻击出现了明显的高峰。这很大程度上是因为，为了满足不断变化的监管和合规性要求，金融服务业越来越多地采用 API。由于企业对 API 的依赖程度越来越高，攻击者也在调整攻击手段，这使得 API 安全成为了现代企业的头等大事。

流量激增突显了按频率和攻击量评估 DDoS 的必要性

金融服务业中的 DDoS 攻击揭示了一个关键见解：攻击事件频率并非始终与攻击强度存在对应关系。虽然一些月份的攻击次数很少，但对应的 Gbps 数据量表明流量大幅增加，这强调了在评估 DDoS 攻击影响时需要同时考虑攻击频率和攻击量。

36%

针对金融机构的可疑域的百分比

网络钓鱼攻击越来越多地针对金融服务客户，这加剧了身份盗窃和帐户接管的风险。这种攻击趋势使得金融机构需要接受监管部门更严格的审查，而数据泄露会引发客户的信任问题。

30%

跳转到网络钓鱼和品牌仿冒网站的页面访问量百分比

攻击者模仿合法的金融服务网站和应用程序，从而将流量成功地导向欺诈网站。他们利用网络钓鱼来持续攻击金融机构，以期获取这些企业掌握的大量敏感信息。

金融服务业仍是第 3 层和第 4 层 DDoS 攻击的最大目标

第 3 层和第 4 层分布式拒绝服务 (DDoS) 攻击以网络层和传输层为目标，这使得网络基础架构不堪重负并耗尽服务器资源和带宽。这种类型的攻击会发送海量流量，用以侵占网络容量，导致合法用户的性能下降。在所有行业中，金融服务业是第 3 层和第 4 层 DDoS 攻击的主要目标（图 1）。这一趋势由几个相互关联的因素所驱动，形成了非常适合攻击者利用的大量漏洞和机会。

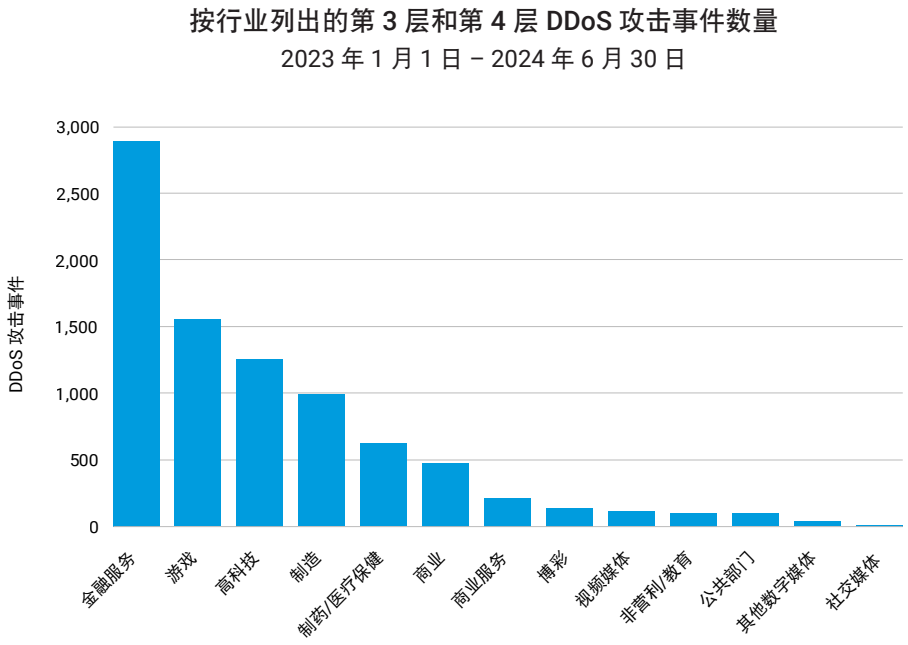


图 1：金融服务业遭受的第 3 层和第 4 层 DDoS 攻击事件数量遥遥领先于其他行业

地缘政治紧张局势是导致金融机构遭受的 DDoS 攻击数量上升的重要因素之一。旷日持久的俄乌战争和巴以冲突就与亲俄罗斯和亲巴勒斯坦的黑客行动的显著增长相互吻合。这些冲突对 DDoS 攻击的激增起了推波助澜的作用，尤其是针对与乌克兰有关联的欧洲银行的攻击。这些攻击的政治动机导致威胁形势愈发纷繁复杂。

金融机构由于涉及到高风险，尤其容易吸引 DDoS 攻击者。一旦攻击者成功造成业务中断，就会导致严重的财务影响、重大声誉损害以及用户丧失对全球金融体系的信任。由于可能造成广泛而深远的影响，金融服务业就成了那些寻求尽量造成巨大破坏或发表政治声明的犯罪分子的首要目标。

技术进步使得 DDoS 攻击者的攻击能力和规模都得到了大幅提升，攻击者现在可以部署虚拟机 (VM) 僵尸网络，利用大量 VM 和物联网 (IoT) 设备上的计算资源来更有效地开展攻击。此方法利用云服务的分布式特性，增加了抵御和跟踪攻击的难度。攻击者可以利用这些设备所具备的高带宽和大量计算资源，这样就能够通过各种策略，发起适应力强、强度高且经济高效的 DDoS 攻击。

金融服务业中的攻击面扩大，也是导致 DDoS 攻击数量增加的因素之一。数字服务和 API 使用的增长，使得攻击者可以找到更多的攻击点。这一转变增加了金融系统的复杂性，并引入了很多潜在的漏洞，让攻击者有机可乘。未明确记录的影子 API 尤其需要引起重视，因为信息安全团队不知道这些 API 的存在，通常也就未能进行保护。攻击者可以利用这些 API 泄露数据、绕过身份验证控制措施或执行破坏性行动。

监管压力也在无意中增长了金融机构面对 DDoS 攻击的漏洞。欧盟颁布了《第二号支付服务指令》(PSD2) 等法规，要求银行通过 API 向第三方提供商（例如金融科技公司）开放其系统。根据这一要求，虽然银行能够通过与金融科技平台、移动应用程序和其他平台相集成，来满足客户不断增长的期望，但也会增加安全风险以及扩大攻击面。而这些实体中另外使用的 API 又会造成更多可能被攻击者利用的潜在失陷点。

总而言之，这些因素导致了金融服务业一直是第 3 层和第 4 层 DDoS 攻击的首要目标。地缘政治动机、高价值目标、技术进步、不断扩大的数字产品应用和监管压力等多种因素结合起来，形成了一种针对金融机构的 DDoS 攻击不仅更加频繁，破坏性也可能会远超从前的环境。由于行业不断发展，在面对这些日益先进的持久威胁时，防御措施也必须随之发展。

攻击者可以利用这些设备所具备的高带宽和大量计算资源，这样就能够通过各种策略，发起适应力强、强度高且经济高效的 DDoS 攻击。

第 3 层和第 4 层 DDoS 攻击事件数量：起伏不定

尽管金融服务业遭遇了极为频繁的第 3 层和第 4 层 DDoS 攻击事件，但这些攻击的频率在全年中会出现波动（图 2）。

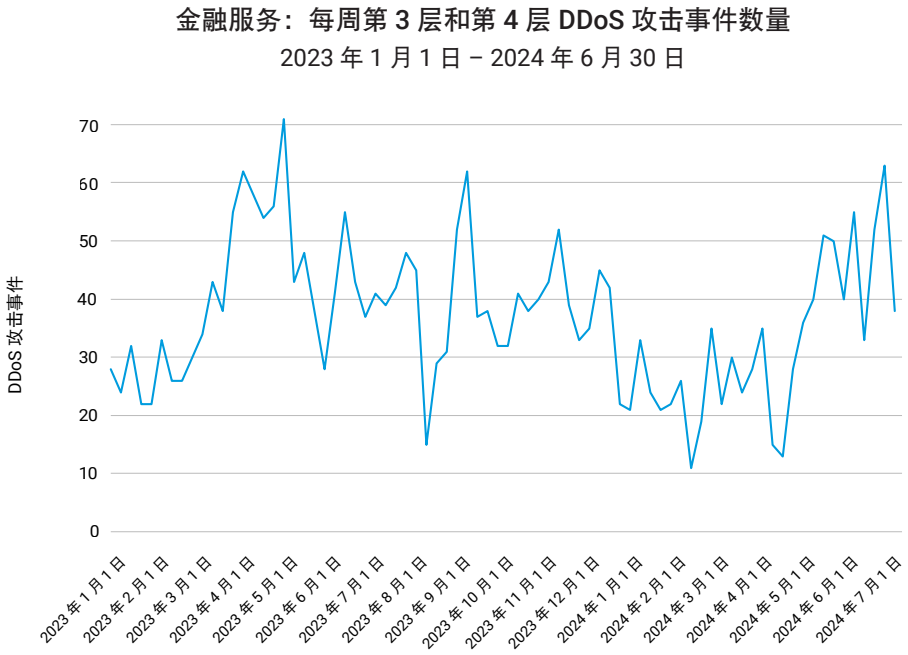


图 2：金融服务业中第 3 层和第 4 层 DDoS 攻击事件数量起伏不定的模式

在 2023 年 3 月/4 月、2023 年 8 月/9 月以及 2024 年 4 月/5 月期间，针对金融服务业的第 3 层和第 4 层 DDoS 攻击可能是由多种特定因素造成的。

每年开春的 3 月到 4 月，标志着美国所得税申报季的到来，对于 DDoS 攻击者来说，这是一个很有吸引力的时机。从 4 月 16 日开始，国家和区域性银行中帐户滥用情况出现了明显上升，这与许多银行开始报告第一季度收入的时间相吻合。在此期间，身份和访问管理 (IAM) 及网络提供商（如 Okta 和 Cisco 等）也报告称，针对线上服务的撞库攻击不仅有所增加，而且增幅巨大。

特别是在 2023 年 4 月，服务定位协议 (SLP) 高严重性漏洞 (CVE-2023-29552) 的发现很有可能造成了攻击活动的猛增。该漏洞可以放大网络层和应用层的 DDoS 攻击，据报道，影响了全球 2,000 多家企业和互联网上的 54,000 多个 SLP 实例。攻击者可以利用此漏洞，使用被入侵的实例来发起大规模的 DDoS 放大攻击。此漏洞的放大系数高达 2,200 倍，是有记录以来最严重的放大攻击之一。

回顾 2023 年 8 月/9 月这个时段，我们发现了一起重大事件。2023 年 9 月 5 日，Akamai 观察到并挫败了针对美国金融机构的有记录以来最大规模的 DDoS 攻击。此次攻击结合了 ACK、PUSH、RESET 和 SYN 泛洪攻击技术，峰值强度达到每秒 633.7 Gb (Gbps) 和每秒 5,510 万个数据包 (Mpps)。尽管攻击强度非常高，但持续时间很短，不到两分钟。

安全现状聚焦

第 3 层和第 4 层 DDoS 攻击强度：事件数与 Gbps

要想全面掌握 DDoS 攻击对金融服务业造成的威胁，了解其纯粹的复杂性和规模就显得极为重要。这些攻击并非简单的孤立事件，每次攻击通常都会涉及到多次大数据量的尝试，意图以每秒数个 Gb 的数据量及数百万个数据包来淹没网络。这些攻击不论是复杂程度、强度还是时间长度都在增长，攻击者会使用更多的不同技术，这进一步加剧了金融机构面临的风险（图 3）。

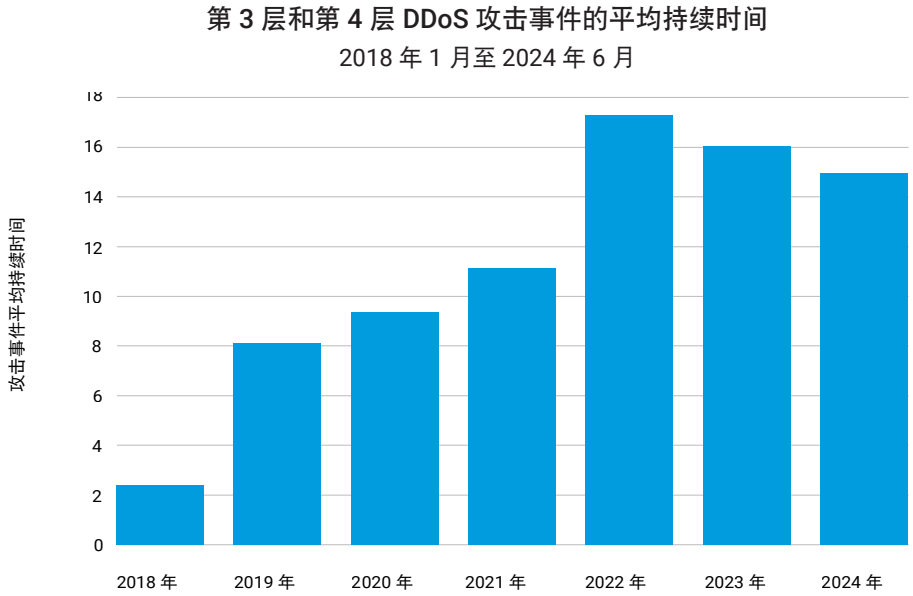


图 3：在全球范围内，第 3 层和第 4 层 DDoS 攻击的时间长度呈增长趋势

此外，在将金融服务业中第 3 层和第 4 层 DDoS 攻击事件的数量图表与相应的 DDoS Gbps 数据量进行对比时，您会注意到一个显著的差异（图 4）。Gbps 图表中显示的急剧增长在攻击事件数量图表中并未体现出来。这种差异强调了一个重要概念：有的月份虽然攻击事件的数量相对较少，但以 Gbps 计量的话，DDoS 流量却可能依然很高。

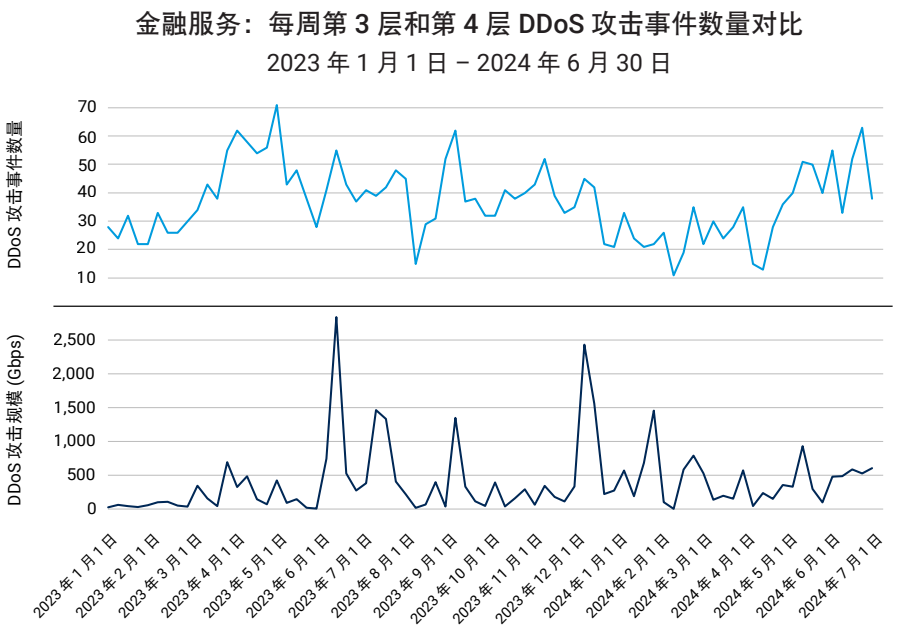


图 4：金融服务业第 3 层和第 4 层 DDoS 攻击事件数量与其 Gbps 指标的对比

此观察结果突显了一个问题：仅仅依靠攻击事件的频率进行衡量，会严重低估威胁的真正严重程度。务必要同时考虑每次攻击中流量的数据量和强度。少量高强度的 DDoS 攻击所造成的损害可能会远高于大量小规模的攻击事件，因此必须对每个威胁进行全面评估。

倾向于单一化：金融服务业中的单媒介第 3 层和第 4 层 DDoS 攻击

网络犯罪分子在尝试破坏系统或者获取未经授权的访问时，通常采用的策略是针对应用层或网络层的多媒介攻击。但是，在主要以金融服务业为目标的攻击者中，对于第 3 层和第 4 层 DDoS 攻击，似乎会更频繁地使用单媒介攻击（图 5）。

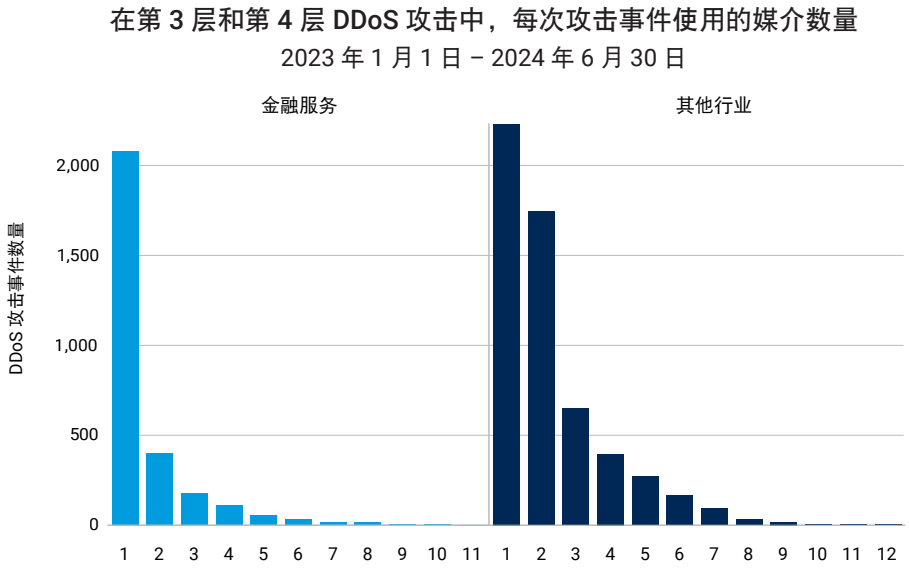


图 5：在针对金融服务业的第 3 层和第 4 层 DDoS 攻击中，更为广泛地使用了单媒介攻击

针对第 3 层和第 4 层的单媒介 DDoS 攻击所需资源更少，而且单媒介攻击本身非常高效，尤其是当金融服务机构采用了强大的防御措施来抵御更复杂的攻击时。与多媒介攻击相比，单媒介攻击执行起来更简单，需要的配合也更少。在第 3 层和第 4 层中，金融机构也可能存在一些明确的已知漏洞，单媒介攻击可以有效地利用这些漏洞，又避免了安全措施检测到利用其他攻击媒介的风险。

这种针对金融服务业的单媒介攻击偏好，对网络安全团队带来了独特的挑战。虽然您仍然必须高度重视复杂的多媒介攻击，但确保任何防御措施都能够承受第 3 层和第 4 层的针对性单媒介攻击也至关重要。

针对 API 的第 7 层 DDoS 攻击数攀升

应用层（第 7 层）DDoS 攻击也称为 HTTP 或 Web 流量层攻击，在针对金融服务业的攻击者中，这种攻击方法越来越盛行，现已成为了一种首选攻击方法。这些攻击专门集火于应用程序中大量使用资源的组件，这样就能有效地阻止合法用户的访问。第 3 层和第 4 层 DDoS 攻击通常可以利用防火墙和网络保护措施来加以缓解，第 7 层攻击则不同，这种攻击会伪装成合法用户来绕开防御措施，针对的是特定应用程序页面或搜索功能，其目的是彻底耗尽应用程序服务器的资源。

虽然金融服务业遇到的攻击更多针对的是 Web 应用程序而非 API，但我们已经观察到专门针对 API 的第 7 层 DDoS 攻击量在急剧增长（图 6）。相比其他行业的整体 API 攻击模式，这些攻击高峰更为明显且更多样化。

金融服务：每天第 7 层 DDoS 攻击数量

2023 年 1 月 1 日 – 2024 年 6 月 30 日

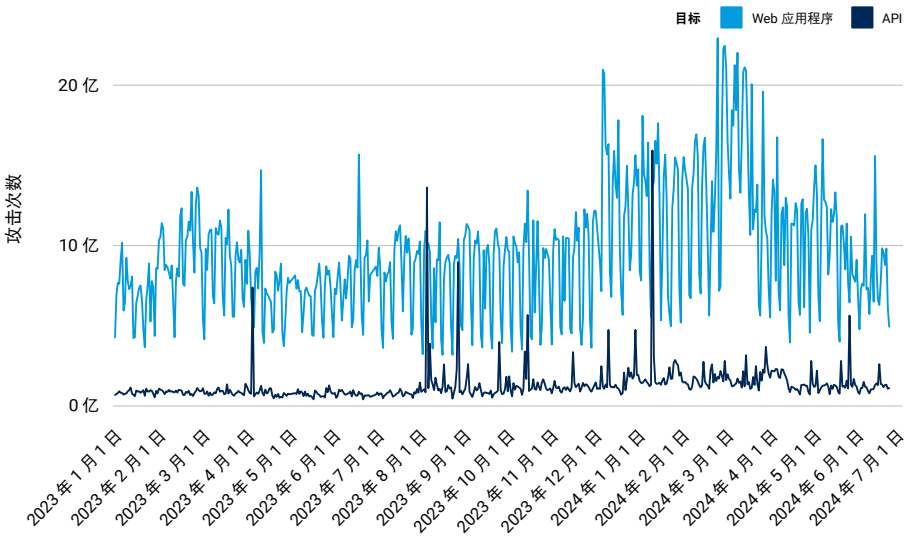


图 6：在金融服务业遭受的第 7 层 DDoS 攻击中，
针对 Web 应用程序的攻击模式与针对 API 的攻击模式存在显著差异

在 2023 年 4 月、2023 年 8 月和 2024 年 1 月间，这些急剧增长尤为明显。我们认为，造成这些高峰的因素，与影响第 3 层和第 4 层攻击数量的因素相似，此外还有一些特定于第 7 层的因素。

攻击者不断寻找可以利用的新漏洞，而一旦发现了这样的漏洞，就可能会导致攻击频率突然上升。例如，HTTP/2 快速重置漏洞 (CVE-2023-44487) 在 2023 年 8 月被首次发现，这个漏洞能够实现极为高效的第 7 层 DDoS 攻击。此漏洞使得攻击者可以利用似乎无害的逻辑，将多个请求捆绑成一个流，从而导致服务器和应用程序资源不堪重负。这也造成了迄今为止有记录的最大规模的第 7 层 DDoS 攻击。

此外，在针对金融机构的网络犯罪分子中，季节性的 DDoS 攻击仍是一种常用策略，在纳税季和节假日期间，这种攻击都会显著增长。2024 年 1 月，伴随红火的假日购物季而来的是攻击态势显著升温，这表明攻击者准备在线上交易火爆之际伺机而动。

金融服务业中的勒索软件和黑客行动

金融服务业常常会成为采用高度复杂技术的攻击者的目标，比如说勒索软件组织。这些组织采用各种技术来渗透金融机构，窃取敏感信息并勒索大额赎金。虽然这些行动的动机主要是为了谋财，但也可能会有地缘政治背景因素掺杂其中，因而会针对一些可能有政治关系的金融机构。俄罗斯的 REvil（即 Sodinokibi）的勒索软件组织就属于这种情况。BlackCat (ALPHV) 也以这种方式参与其中，从针对一家知名银行的攻击中就可以看出。

一些组织以攻击包括金融机构在内的大型企业而闻名，LockBit 仍是其中最为活跃的组织之一。该组织尽管近期遭到执法部门的严厉打击，依然活动猖獗。欧洲刑警组织与欧洲司法合作单位共同成立首个针对网络犯罪团伙的国际特别行动组并开展代号为 Operation Cronos 的清剿行动，然而，LockBit 通过建立新的基础架构，再次死灰复燃。2024 年 2 月，在执法部门的行动查封了该勒索软件团体仅仅几天后，该组织便带着新的基础架构和一个暗网泄密网站重新出山。LockBit 宣称，作为对 Operation Cronos 的回应，该组织将增加对政府网络的攻击作为反击方式。

勒索组织 CL0P 同样活动猖獗，该组织以利用企业（包括金融机构）广泛使用的文件传输软件中的漏洞而闻名。零日漏洞 CVE-2023-34362 便是其中一个知名案例，受影响的是 MOVEit Transfer 软件，该漏洞通过 SQL 注入来渗透 MOVEit Transfer Web 应用程序。至少 15 家银行和信用社确认 MOVEit 造成了数据泄露。CL0P 还会通过其他技术（包括网络钓鱼）来获得初始访问权限，并继续以勒索软件即服务 (RaaS) 模型运行。最近，该组织在针对金融机构等目标时，实现了手法的演变，采用的是四重勒索。除了三重勒索采用的技术之外，四重勒索还包括发消息骚扰被攻击企业的业务合作伙伴、员工、客户、高层人员和媒体，告诉他们这家企业被黑了。这种伎俩导致了支付的平均赎金金额增加。

还有一些针对金融机构但并未归类为勒索软件组织的激进黑客攻击者，包括 Anonymous Sudan、KillNet 和 NoName057(16) 等。他们都因与俄乌战争相关的活动而知名，而且 Anonymous Sudan 还被指曾牵涉到与哈以战争相关的网络攻击中。去年，这些组织伙同其他多个网络攻击组织，利用俄乌战争带来的混乱，将注意力转向了关键的银行基础架构。

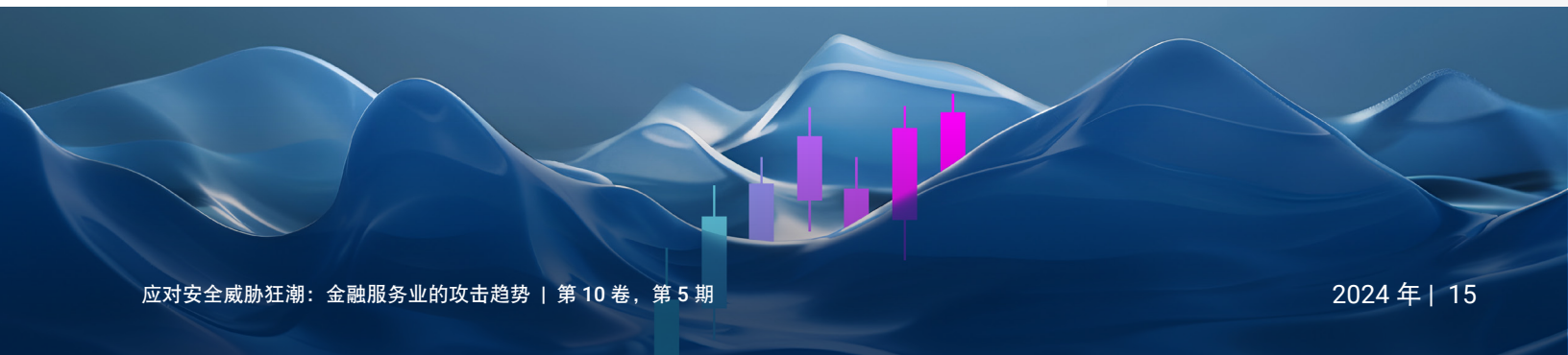
还有其他许多相当活跃的攻击者同样以攻击金融服务业而闻名，但未被归类为勒索软件组织，例如 Lazarus Group、MoneyTaker、Carbanak/FIN7、Cobalt 和 APT41。

考虑到这些攻击者会持续带来威胁，因此金融机构务必要随时掌握最新的威胁形势，并更好地了解攻击者的动机和技术，以便制定更有效的防御策略。请查看本报告后面的“抵御措施”，了解建议采取的安全防护措施。

近期在中东金融机构中爆发的 DDoS 黑客行动

受地缘政治紧张局势的推动，中东金融服务业最近经历了复杂和持续的 DDoS 攻击激增。这一趋势在欧洲、中东和非洲 (EMEA) 地区尤为普遍，这表明出于政治动机针对金融机构进行 DDoS 攻击的威胁在上升。

体现这种趋势的一个知名案例发生在本年初，一家亲巴勒斯坦的黑客组织 BlackMeta（也称为 DarkMeta）针对阿拉伯联合酋长国 (UAE) 的一家金融机构，发起了为期 6 天的第 7 层 DDoS 攻击。此次攻击使用了 InfraShutdown，这是一项租用型 DDoS 服务，突显出这些攻击工具的获取越来越容易。BlackMeta 自 2023 年 11 月以来便一直活跃，在以色列、UAE 和美国都有针对企业发起攻击的历史。



此次针对这家阿联酋金融机构发起的攻击具有持续时间长且强度高的特点。攻击持续了大约 100 小时，Web 请求波动持续时间在 4 到 20 小时之间，平均每秒有 450 万个请求。此次攻击使得该银行七成的时间处于受攻击状态，造成严重服务中断。BlackMeta 针对该银行发起的行动是抗议巴勒斯坦人和穆斯林所遭受的不公正待遇的更广泛行动中的一环，所用的手法与 Anonymous Sudan 相似。

幸运的是，这家金融机构的抵御措施阻止了攻击造成巨大破坏，但这一事件突显了政治因素造成的网络攻击数量日益增长的趋势。该事件还突显出，租用型 DDoS 服务越来越易于获得，这降低了黑客组织发起大规模攻击的门槛。这种发展趋势强调了实施强有力的安全措施以防范大规模持久威胁的必要性。

近期另一起疑似出于政治动机的 DDoS 攻击发生在 2024 年 7 月 15 日，目标是以色列的一家大型金融服务公司。这场大规模的攻击源自一个全球分布式僵尸网络，持续了近 24 小时，峰值流量达到 798 Gbps。Akamai 成功抵御了此次第 3 层和第 4 层 DDoS 攻击，攻击中采用了 DNS 反射和 UDP 泛洪等多种媒介。

此次攻击期间最密集的 3 小时时段中，Akamai 阻止了大约 389 TB 的恶意流量，在攻击的整个持续期间，总共阻止了大约 419 TB 的流量。在同一天，以色列的其他金融机构出现了停机，表明这是一次协同攻击，进一步突显了高级 DDoS 攻击带来的威胁日益严重。

值得一提的是，此资源丰富的攻击者在此前的 90 天内曾针对该金融服务客户发起 27 次攻击。自 2023 年第 4 季度以来，该客户便反复受到 DDoS 攻击，这一时间与哈以战争发生的时间相吻合。Akamai 的国际 DDoS 威胁情报团队报告称，2024 年，以色列的机构和企业经历了前所未有数量的 DDoS 攻击。这种持续而激进的行动说明了这些威胁的规模和强度越来越大，表明攻击者不仅资源越来越多，而且攻击时间也越来越长。

假冒知名机构：金融服务中的品牌滥用

金融服务机构纷纷采用数字优先的方法来改善客户体验、运营效率、创新能力、整体收入和知名度，网络攻击者则通过品牌仿冒骗局，来利用企业与客户之间的固有信任关系。图 7 显示了模仿知名金融机构的欺诈网站示例。虽然网络钓鱼和品牌仿冒方法很常见，但数量惊人的欺诈网站以及攻击者在先前的仿冒网站下线后创建新域名的速度之快，尤其令人担忧。这种快速激增对金融服务领域造成了不断增长且永无休止的威胁。

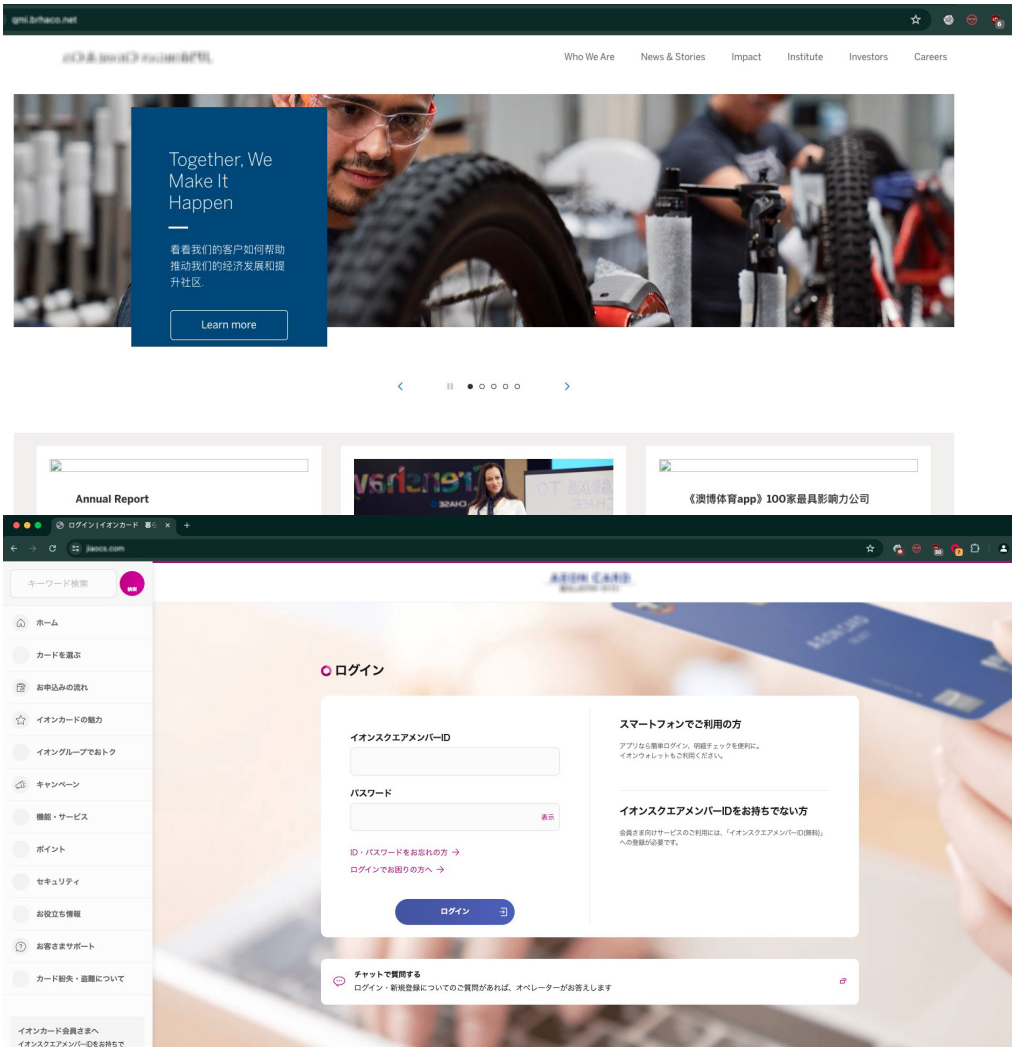


图 7：模仿知名金融机构的欺诈性网络钓鱼网站示例

网络钓鱼即服务平台和工具包的出现，极大地改变了品牌滥用的形势。这些资源降低了网络犯罪分子的入行门槛，使得针对金融服务机构及其客户的网络钓鱼攻击的规模日趋庞大，情况日益严重。从这个角度来看，国际反网络钓鱼工作组在 2023 年记录了近 500 万次网络钓鱼攻击，将这一年称为“有史以来网络钓鱼攻击最泛滥的一年”。

品牌滥用可能会推动风险升级，例如身份盗窃和帐户滥用。攻击者通常会在暗网上兜售客户信息，或者利用这些信息来接管帐户。从安全的角度来看，提前干预对于预防品牌攻击非常重要。通过在攻击生命周期的早期阶段进行阻止，您可以防止攻击者收集凭据用于恶意用途。

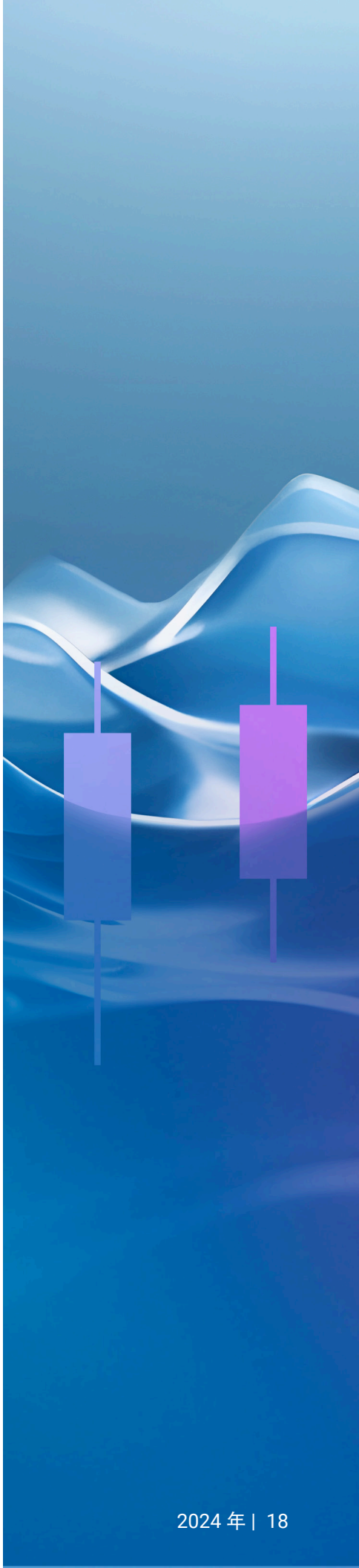
品牌滥用的涉及面很广，远不止直接造成的安全问题。企业会由于多种原因遭受重大财务损失，例如声誉受损、合规性和法律问题，甚至是假冒产品造成的销售损失。在当今的数字化环境中，需要尽早检测到品牌仿冒攻击，这对于维护客户信任和业务连续性至关重要。

欺骗点：深入了解仿冒攻击

安全团队面临着艰巨的挑战，需要防范各种在线平台上可能出现的品牌滥用情况，这使得保护数字资产成了一项艰巨的任务，因为合法用户和攻击者都能访问数字资产。攻击者通常会抓取面向公众的资产内容（例如网上银行门户），用于创建自己的仿冒网站，并注册具有相似拼写的域名来欺骗没有起疑心的用户。此外，网络攻击者发起的行动涉及网络钓鱼电子邮件、社交媒体帖子和其他数字化渠道，以引诱潜在受害者访问其恶意网站或虚假应用程序。

在本报告中，我们分析了过去 12 个月内，在活跃的域上观察到的品牌仿冒和网络钓鱼活动，以深入分析各个行业中品牌仿冒的盛行情况，并重点考察金融服务业。Akamai 提供了全面的监测能力和专有解决方案，使得我们能够：

- 跟踪流经网络钓鱼和品牌仿冒网站的流量，包括在线市场
- 确定活跃的恶意域数量
- 评估恶意域的严重性评分



在 Akamai 监控的所有可疑网站中，金融服务业是被仿冒比例最高的行业 (36.25%)（图 8）。这一发现进一步突显了金融服务业易于遭受品牌仿冒和滥用的攻击。位居二三位的分别是商业 (26.41%) 和商业服务 (18.90%) 行业中的企业。

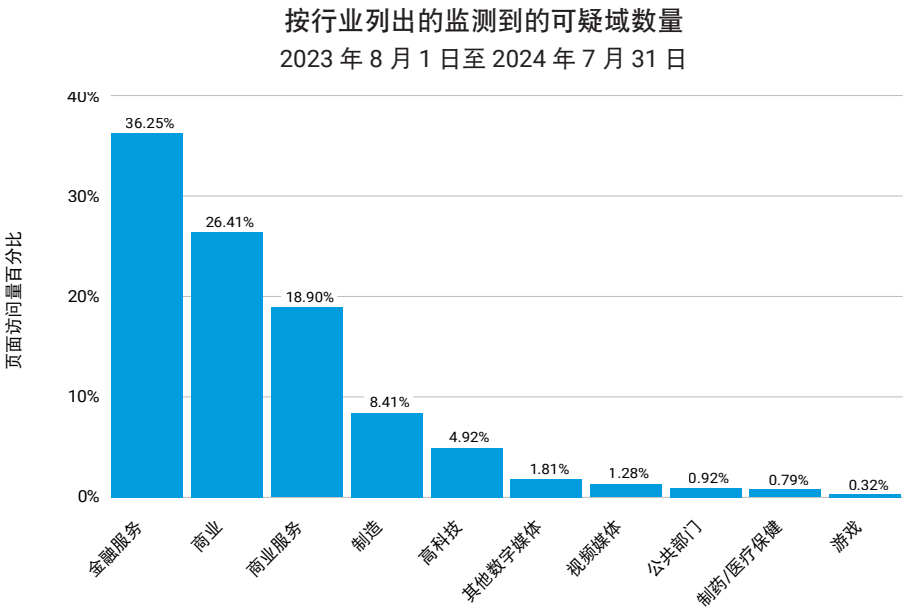


图 8：在网络钓鱼和/或品牌仿冒域中，金融服务业占到了 36.3%

金融服务业之所以成为品牌仿冒攻击的主要目标，是因为该行业拥有大量敏感且极具价值的数据，例如银行凭据和个人身份信息 (PII)。利用从假冒银行网站获得的信息，网络犯罪分子可以轻松地访问银行帐户，继而将帐户搜刮得一干二净。与此类似，攻击者还可以获取其他高价值的财务信息，例如电子钱包和加密货币帐户的凭据（在暗网上售价为 120 美元到 400 美元之间），从而转走帐户中的所有有价物或者在暗网上售卖这些信息。此类骗局具有高额回报，使得金融服务业成为了品牌滥用和网络钓鱼攻击的首要目标。

同样地，电子商务和网上购物的盛行为窃取凭据和其他个人信息带来机会，商企成为了有利可图的品牌滥用目标。制造公司和提供服务的第三方供应商同样容易遭受品牌滥用的攻击。虽然数字化推动了整体业务的强劲增长，但对于许多企业而言，数字化环境已经成为了一个易受攻击的软肋，导致品牌仿冒攻击和网络钓鱼尝试出现了激增。

[品牌仿冒] 骗局带来的高额回报，使得金融服务业成为了品牌滥用和网络钓鱼攻击的首要目标。

企业必须保持警惕并实施安全措施，才能在这种快速发展的数字环境中保护品牌和客户。这包括持续监控品牌滥用情况，对假冒网站采取快速下线措施，以及教育客户识别可能的假冒尝试。通过重视这些工作，企业在面对日益复杂的威胁环境时，可以更好地保护自己的声誉和客户的信任。

品牌滥用瞄准金融服务业

为了全面了解品牌仿冒和网络钓鱼的影响，我们还分析了可疑网站的页面访问量。我们的调查结果显示，伪装成金融机构的网站获得了 30% 的访问量，其后是冒充商务公司的网站，访问量占到了 20%（图 9）。无论我们是按请求数还是按域来衡量，金融服务业和商业均稳居被冒充的前两位。这种一致的结果突显了这些行业的现状，也就是成为品牌滥用和仿冒攻击的首要目标，而且有着充分的理由。

金融服务涵盖各种各样的被攻击目标，从具备完善机制的银行到安全资源有限的小型机构，无不面临高度的攻击风险。与金融服务业一样，商业是另一个需要接受合规性部门（例如，支付卡行业安全标准委员会）进行类似审查的行业，该行业由于拥有的大量客户信息，同样面临着重大风险。

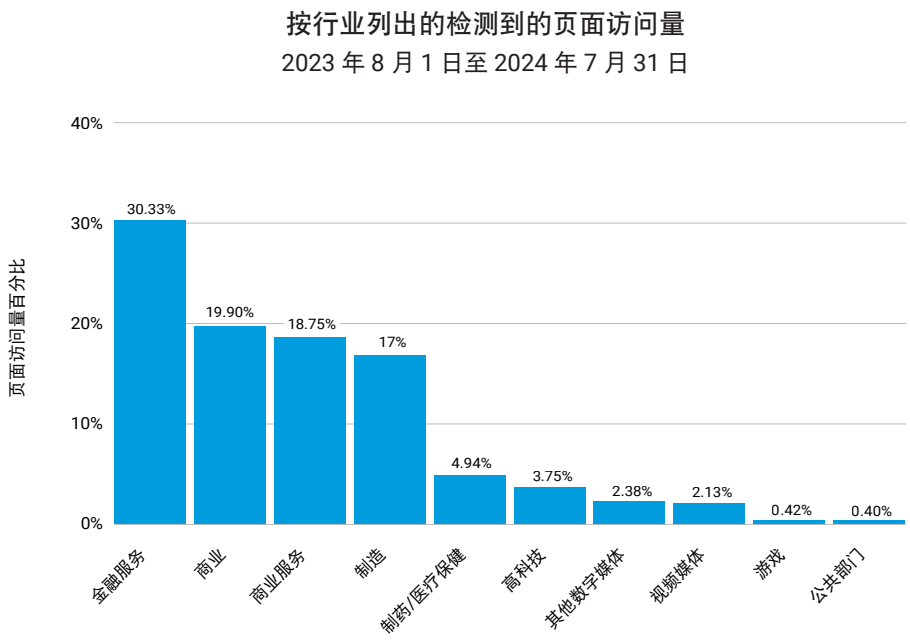


图 9：在报告期间（2023 年 8 月至 2024 年 7 月），超过 30% 的页面访问量指向了仿冒合法金融服务网站的可疑网站

有趣的是，我们观察到，对于不同的行业，在域仿冒排名与实际访问量之间存在一些差异。例如，在仿冒域中，高科技行业排名前五，但实际访问量跌到了第六。同样，仿冒制药/医疗保健的域较少，但这些域的访问量反倒较高。

通过网络钓鱼获取凭据

品牌滥用有多种形式，包括具有相似外观的网站（完全盗用合法公司的徽标和设计）、欺诈性应用程序以及虚假社交媒体资料（模仿官方公司帐户）。为了确定这一问题的严重程度，我们分析了假冒页面，并将其分为不同类型：品牌仿冒、网络钓鱼、恶意应用程序、假冒网店、绕过付费墙程序以及假冒社交资料和网店。一定要注意的是，根据我们监控的页面，一家企业的域可能会分为多个类别。

我们的分析显示，以金融服务机构为目标的仿冒域中，网络钓鱼占主导地位，占所有记录案例的 68%（图 10）。品牌仿冒紧随其后，在所有已记录的域名中占比达到 24%。在用户频繁访问的网站中，网络钓鱼和品牌仿冒再次分别排名第一和第二。相比其他行业，金融机构中其他形式的品牌滥用（例如虚假社交媒体资料），则没有那么严重。尽管采用恶意应用程序的攻击数量较少，但还是需要注意，攻击者在采用越来越有创意的方法来扩大其攻击覆盖面。

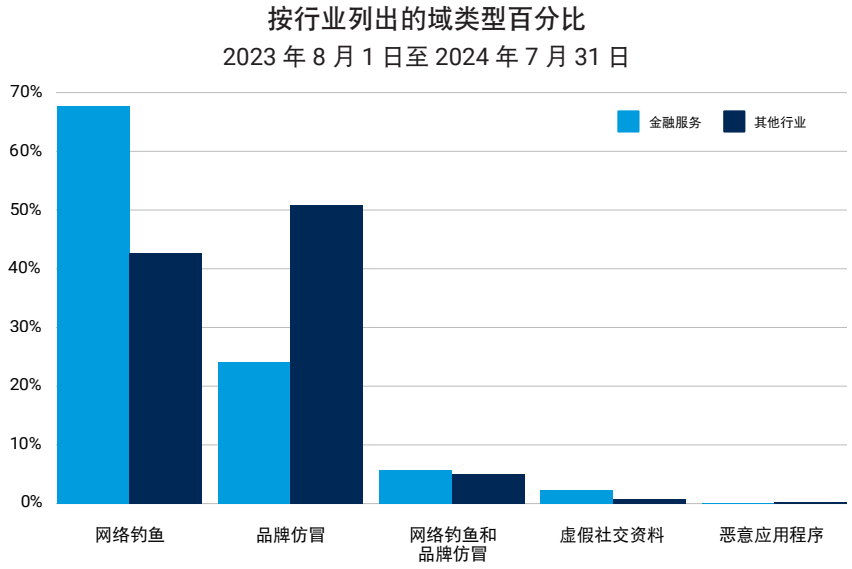


图 10：在我们记录的针对金融服务业的攻击中，绝大多数域是网络钓鱼网站，这一数字甚至超过了其他所有行业的总和

金融机构被视为值得高度信赖的实体，这也使意图利用这种信任关系的欺诈者将其作为主要目标。

尽管人们对网络钓鱼所带来风险的认知已经有所提升，但是人为因素仍然是最大的安全漏洞。攻击者使用的复杂技术进一步扩大了这种漏洞（有关详细信息，请阅读品牌滥用剖析部分），使得缺乏专业知识或经验的人群很难识别虚假页面。金融机构被视为值得高度信赖的实体，这也使意图利用这种信任关系的欺诈者将其作为主要目标。通过仿冒这些机构，攻击者欺骗用户来自愿地交出凭据，利用机构的声誉来使他们的攻击手段更有说服力，并且更容易得手。

要想保护企业及其客户，非常关键的一点在于使用具备品牌监控功能的技术，这样就能主动监控任何未授权的品牌使用，其范围包括了域名、移动应用程序和电子邮件通信。在确定存在仿冒情况之后，接下来就需要将其下线以阻止流量，否则就可能将客户暴露在品牌滥用和网络钓鱼所造成的危险（例如，数据盗窃）之中。

案例研究：针对金融机构的撞库攻击日益复杂

在 2023 年到 2024 年期间，一家美国金融科技公司遭受了无休止的撞库攻击，目标是其面向客户的一款应用程序。这些攻击的规模令人震惊：在 24 小时内，Akamai 检测到来自不同 IP 地址的 3,000 多个告警，都是在尝试使用被盗的凭据渗透帐户。我们观察到一个 IP 地址尝试了至少 115 个用户名和密码组合。在 2024 年 7 月，我们总共记录到了超过 10 万个告警。

具有重大风险等级的欺诈性金融服务网站

凭借来自我们全球边缘网络的独家情报以及第三方提供的更多威胁情报数据，我们在检测品牌仿冒方面具有显著优势。我们使用这套综合系统开展细致的检查，并根据威胁评分对各个域进行分类。

我们使用三个关键要素计算威胁评分：

1. **置信度评分** —— 我们对某个事件是网络钓鱼尝试的确定程度
2. **严重级别** —— 与该事件相关的风险的等级（严重、高、中或低）
3. **频率系数** —— 在给定的时间范围内，与网站关联的事件/会话数

我们的评分系统平衡了这三个关键系数：置信度、严重性和频率。我们将这些评分结合起来，为每个可疑域生成全面的威胁分数，上限为 99，以确保全面评估潜在的威胁。

我们最新的分析发现，金融服务领域的威胁数量中位数评分为 85 分，这表明该行业持续面临着重大风险（图 11）。这一得分表明金融机构毫无疑问地成为了网络犯罪分子的目标，他们在永无休止地针对其庞大且敏感的数据存储发起攻击。

按行业统计的威胁评分

行业	威胁数量中位数评分	行业	威胁数量中位数评分
公共部门	**95**	游戏	**65**
金融服务	**85**	制造	**64**
商业服务	**85**	其他数字媒体	**62**
制药/医疗保健	**85**	商业	**61**
视频媒体	**71**	高科技	**60**

图 11：我们的威胁数量中位数评分结果表明，金融服务业的得分高得惊人

虽然公共部门的威胁数量中位数评分最高（这可能是由于其持有大量敏感信息，而安全资源有限），但金融服务业也不相上下，因潜在的巨大经济利益成为攻击者觊觎的目标。商业服务和制药/医疗保健等领域也具有相似的评分，表明网络犯罪分子的攻击目标趋向于多样化，但由于金融服务业的数据极为关键，因此仍是攻击的主要焦点。

这种高度的威胁水平要求企业立即采取行动，以强化防御措施并防范不断进化的威胁手段，以免造成重大财务损失和声誉损害。

品牌滥用剖析

欺诈和品牌滥用手段的成功，很大程度上依赖于品牌作为社交工程诱饵的传播力量。攻击者利用消费者对知名品牌的熟悉感和固有信任感，设计出与官方网站非常相似的假网站。在某些情况下，欺诈者甚至会完全复制代码，使得这些非法网站看起来几乎与真网站一模一样。生成式人工智能工具的兴起，可以帮助欺诈者消除会引发用户警觉的拼写和语法错误，使得消费者更难以区分官方网站与仿冒网站。

网络钓鱼工具包的出现，进一步加剧了网络钓鱼和仿冒活动的强度。

网络钓鱼工具包的出现，进一步加剧了网络钓鱼和仿冒活动的强度。只需低至 50 美元，攻击者就可以购买到网络钓鱼工具包，用来创建以假乱真的网络钓鱼网站。这些开发、构建和销售网络钓鱼工具包的网络犯罪分子团伙极大地降低了实施网络钓鱼和仿冒犯罪活动的门槛。Kr3pto 和 16Shop 这两个就是盛行的网络钓鱼工具包的例子。Kr3pto 针对的是英国银行，采用的手段是绕过双重身份验证，而 16Shop 则重点针对 PayPal 和 Amazon 等大品牌。在 2023 年 8 月开展的一次国际执法行动中，成功抓捕了 16Shop 的创建者。这些案例展现了网络钓鱼攻击的复杂性，以及各方为打击网络犯罪而协同开展的工作。

得分不高但屡试不爽：组合式域名仿冒

品牌滥用的另一个重要因素是使用与官方网站非常相似的域名。通常，攻击者会在购买或构建自己的网络钓鱼网站之后购买域名。这种时候，域名抢注及其许多变体等屡试不爽的手段扮演了重要角色。一种常见的伎俩是域名误植，攻击者会注册一个与公司名称的拼写略有不同的域（例如，acamai[.]com）后，然后盼望消费者在输入时敲错。另一种方法是组合式域名仿冒，具体做法是向域名添加额外的关键词，例如“support”、“login”或“help”。这种手法利用的是公司合法网站上常见的微网站。

根据 Akamai 的研究，尽管组合式域名仿冒（添加关键词）是一种被低估的手法，但采用这种手法的活动域的数量超过了域名误植（添加、删除或更换字母）。很有趣的一点是，在欺诈网站中，添加最多的关键词之一是“com”。

在现实中还存在另外一些手法，使得消费者更难识别仿冒网站，这增加了这些攻击的成功率。

传播机制

仿冒和网络钓鱼网站通过多种机制来传播和兜售，最主要的一种机制是电子邮件。这些电子邮件消息会使用官方徽标以假乱真，而且邮件内容十万火急，比如要求马上更新帐户信息等。但是，品牌滥用并非仅限于网站和电子邮件，攻击者还会通过社交媒体来散布攻击手段，这进一步扩大了攻击覆盖面和欺骗手法。

看似无害，实则暗藏玄机（链接）

在现实中还存在另外一些手法，使得消费者更难识别仿冒网站，这增加了这些攻击的成功率。例如，使用短网址、二维码、图像超链接以及短信中的文本链接，用来混淆恶意链接。与电子邮件使用垃圾邮件过滤器来防止这种滥用不同，文本诈骗可能不会被阻止，并且有更高的机会被阅读或打开。

金融行业中的区域性网络钓鱼和品牌仿冒攻击

品牌滥用影响着世界各地的企业和消费者，但由于品牌仿冒和网络钓鱼网站的流量比较集中，一些地区更容易遭受欺诈和滥用攻击。我们的分析表明，在过去的 12 个月中，欧洲、中东和非洲地区检测到的网络钓鱼和仿冒网站的流量最高，甚至超过了北美地区（图 12）。这一排名涵盖了金融服务业和其他行业。

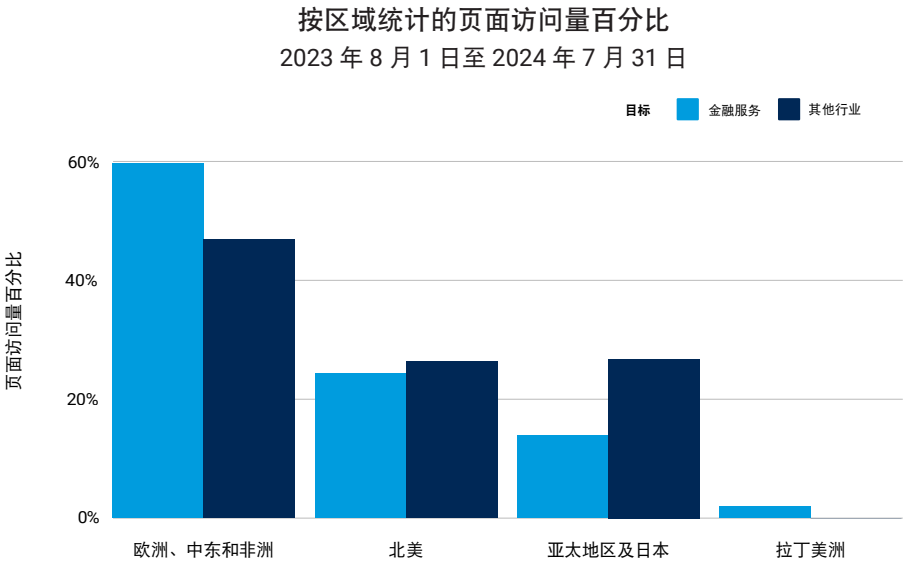


图 12：欧洲、中东和非洲地区超过北美，
成为金融服务业受网络钓鱼和品牌滥用影响最大的地区

虽然在拉美地区以及亚太地区及日本 (APJ) 记录到的页面访问量相对较少，但这并不表明针对性攻击也较少。相反，这些调查结果可能表明，拥有庞大客户群的全球品牌集中在了北美以及欧洲、中东和非洲地区。这种情况为攻击者带来了更庞大的潜在受害者群体。我们还可以将此调查结果归因于自 2023 年以来 V3B 等网络钓鱼工具包的出现，这些工具包专门针对欧洲银行。

虽然欧洲、中东和非洲地区的可疑域和页面访问量超过了大多数地区，但亚太地区及日本具有最高的威胁数量中位数评分：97。尽管拉美的网站访问量最低，但威胁数量中位数评分却达到了 94，高得令人吃惊。这表明，拉美地区以及亚太地区及日本的消费者在访问各种网站时，其银行信息和其他敏感数据被盗的风险更高。

在亚太地区及日本，有几个因素导致了针对金融服务业的品牌滥用的危险日益上升。首先，亚太地区及日本的大部分金融服务机构均已实现了高度数字化，几乎所有服务都能在线上完成，无需前往任何实体营业网点。亚太地区及日本的互联网普及率和数字化采用率在全球处于领先地位，对于网络犯罪分子来说，这使得该地区成为颇有吸引力的目标。其次，在此地区的一些国家/地区中，社交媒体最为活跃。金融服务机构已经借助这些平台来增强与客户的互动，以争夺市场份额并赢得更好的客户忠诚度。亚太地区及日本的社交媒体和消息收发消息应用程序的广泛使用，使得网络犯罪分子可以通过更多的攻击媒介来发起网络钓鱼和仿冒攻击，通常是通过滥用人们对这些平台的信任。

不断演变的合规要求：全球网络安全法规如何重塑金融机构

在被问及抢劫银行的原因时，臭名昭著的银行劫匪 Willie Sutton 给出了著名的回答：“因为那里有钱。”当然，对于当今针对金融机构的网络攻击，Sutton 的说法也很贴切。然而，经济利益动机只是一部分原因。金融机构发现自己越来越多地受到具有政治动机以及地缘政治战略动机的攻击者的进攻。这些动机，再加上“那里有钱”这一实际情况，给金融机构制造了一场完美的风暴，因为这是受攻击最严重的行业。

这不足为奇。一直以来，金融业在社会中发挥着关键的核心作用，始终是被严加监管的对象。尽管过去对金融机构的监管侧重于保护消费者与金融机构的交易，但现在，监管机构正寻求对金融机构和服务公司应用关键基础架构式的安全和弹性监管措施。这种新趋势不仅对金融机构本身提出更多要求，对这些机构的信息和通信技术 (ICT) 提供商也是如此。

关于网络安全和运营弹性法规的例子有很多。欧盟有《数字运营弹性法案》(DORA)，强制要求金融实体及其供应商采取可靠的 ICT 风险管理框架，并定期进行测试和事件报告。在美国，证券交易委员会 (SEC) 颁布了网络安全重要性法规，要求包括金融机构在内的上市公司披露可能会对其运营造成重大影响的网络事件。在澳大利亚，澳大利亚审慎监管局 (APRA) 制定了标准，要求实体维护的信息安全能力，要与其信息资产所受威胁的规模和程度相符（法规 CPS 234）。

这些例子说明，目前全球趋势是加强金融领域的网络安全和运营弹性，以防范不断演变的风险并确保金融稳定性。

鉴于这些法规，金融机构在采购 ICT 和安全服务时，有责任进行尽职调查，以确保供应商符合这些制定出的严格标准。金融机构选择的供应商不仅要提供弹性服务，还要了解相关法规，提供必要的监测功能来识别和防范不断演变的威胁，并帮助将这些情报应用于持续运营之中。

监测能力至关重要，因为您无法保护您不知道自己是否拥有的资源（或您正在连接的资源），也无法防御您不知道是否存在的威胁。Akamai Guardicore 平台等服务不仅可以提供防御攻击的能力，而且还可以帮助客户了解数据流、识别异常情况并对网络资产进行正确分段，从而缓解威胁。与此类似，该平台的 API 安全服务旨在识别 API 流量来协助管理影子 API，以及识别潜在的 API 攻击。

为了反映这种新趋势，而银行也许应该将监测能力 (Visibility) 添加到传统的 CIA 三要素，即机密性 (Confidentiality)、完整性 (Integrity) 和可用性 (Availability) 之中，变成 VCIA 四要素：监测能力、机密性、完整性和可用性。

James Casey
副总裁兼首席隐私官，
Akamai

借助 Zero Trust 来加强防御措施

信任关系为金融机构树立声誉奠定基础。但是，要想保护复杂的环境和机密数据，信任很容易成为巨大的责任。攻击者可以通过许多方法来利用隐含信任，包括：

- 网络钓鱼攻击，用以冒充企业内的个人
- 利用第三方供应商中的漏洞进行攻击，用于访问高价值目标
- 内部威胁，出于恶意目的滥用访问权限

基于边界的传统安全措施已经不足以应对越来越复杂的攻击方式，因为这种方法认定所有来自内部的流量都是可信的。考虑到金融服务业的高风险，维护具有弹性的安全态势极为关键。这种情况下，Zero Trust 框架就势在必行。这种安全防护方法遵循了任何连接请求、用户或设备都是潜在危险的工作原理。此方法实施持续验证并删除隐含信任，默认情况下拒绝对资源的访问，只有在请求方已通过身份验证并获得授权时才允许。

Zero Trust 可以确保那些处理受监管数据的系统的安全，增强了金融机构在面对不断变化的监管要求时的合规性，让企业能够避免因审计失败而受到处罚。此方法针对传统系统额外提供了控制措施，提供了精细的监测能力，以便检测出试图访问关键应用程序的未授权用户。

Zero Trust 模型通过限制对关键系统的访问来限制东西向流量，并可防止勒索软件等威胁的横向移动。这种遏制策略可以隔离受感染的系统，保护关键数据和资产。由于针对金融服务业的勒索软件攻击数量大幅增长，因此强调 Zero Trust 在保护敏感信息时的重要性是理所应当的。通过精细监测能力，Zero Trust 可以帮助您在复杂环境中检测并消除威胁，这对于防止勒索软件扩散和保护关键资产非常重要。

Zero Trust 的另一个显著优势是它能够保护应用程序之间的数据流，这对于基于云的应用程序的安全部署至关重要。这不仅可以推动现代化改造，还可确保在不断变化的威胁形势下保护机密信息，使金融机构能够持续创新又不损害安全性。实施 Zero Trust 框架可以增强安全态势，并顺应机构防范未来不断演变的威胁的需求。

分段是一项不错的技术，微分段则更为有用。

分段这种架构级方法可以将网络划分为较小的区段，其目的在于增强性能和安全性。利用微分段安全技术，您可以将网络按逻辑划分为不同的安全段，并能精细到单独的工作负载级别。然后，您就可以为每个不同的区段采取适当的安全控制措施和服务交付方法。

微分段也是 Zero Trust 的基础。据近期 Akamai 的一份报告称，金融服务业网络安全领导者认为，先进的 Zero Trust 是实施分段项目最常见的驱动因素。实际上，几乎所有已经实施分段的领导者都在部署或者已经部署了 Zero Trust 安全框架 (99%)，不过有不到一半 (47%) 的领导者表示其 Zero Trust 框架已经全面完成并妥善定义，因而达到了成熟的水平。

微分段可用于现有系统中，其部署速度快于防火墙等传统方法。此方法可将对勒索软件的响应时间减少达 13 小时，并简化了所有 IT 环境中的管理。它还可以通过精准的数据控制来帮助满足合规性要求。

一个真实案例展示了现代化微分段的影响力：某项目将实施时间从 2 年削减到 6 个月，仅使用一位工程师，并将成本减少了 85%。这一案例说明了微分段可以如何节省企业的时间和金钱。IT 主管应该将这些成果与其当前的安全成本和实施时间进行比较。

为了强化网络安全态势，金融机构必须优先实施高级分段策略。首席信息安全官应带头开展工作，使安全措施与不断发展的行业标准保持一致，集成微分段方法作为强大的 Zero Trust 架构的基石。IT 主管必须确定时间表来定期进行安全审计和战略更新，以确保他们的防御能够抵御复杂的网络威胁。

这种积极主动的方法不仅有助于防范当前的漏洞，还可以让企业高效地应对新出现的网络安全挑战。通过采用这些措施，金融机构可以创建全面的安全框架，不仅解决眼前的问题，而且能够进行长期风险管理。

[微分段] 不仅有助于防范当前的漏洞，还可以让企业高效地应对新出现的网络安全挑战。

抵御措施

要想保护金融机构免受各种网络威胁，您需要实施兼顾多方面的方法。接下来我们针对网络钓鱼、品牌仿冒、DDoS 攻击和勒索软件，探讨几种关键的防范策略。

网络钓鱼和品牌仿冒保护

在保护机构免受网络钓鱼和品牌仿冒的侵害时，请考虑使用第三方品牌保护服务来快速检测和下线欺诈内容。对员工和客户开展培训也很重要。为员工定期开展安全意识培训，让他们了解如何识别网络钓鱼和仿冒攻击。明确地说明如何识别机构中的合法通信。针对仿冒攻击尝试制定快速响应计划，包括在识别出骗局后，有相应的流程告知合作伙伴和客户。

此外，还可以实施以下保护技术：

- 注册类似的域名来防止域名误植，并使用域监控服务来检测相似的域。
- 使用强大的、唯一的密码和密码管理器来加强身份验证协议，并为所有帐户和系统实施可靠的多重身份验证 (MFA)。
- 部署电子邮件身份验证协议，例如发件人策略框架 (SPF)、域名密钥识别邮件 (DKIM)，以及基于域的消息身份验证、报告和一致性 (DMARC)，来防止电子邮件欺骗。使用防网络钓鱼解决方案和高级电子邮件过滤功能来检测并阻止恶意电子邮件。
- 通过获取 SSL 证书、实施 HTTPS 并使用反欺诈工具，来检测网站和移动应用程序上的可疑活动，保护您的网站和数字渠道。
- 提供安全门户，并为敏感通信实施加密消息收发，用来保护通信渠道。

DDoS 防护

要保护金融机构免受 DDoS 攻击的侵害，需要采取多层防御策略。实施主动式策略，例如使用专用 DDoS 检测、抵御攻击和保护产品；配置速率限制；以及在 CDN 上缓存内容。此外，请及时掌握最新的安全措施，例如补丁管理、事件响应计划、针对暴露于 DDoS 的 IP 地址和关键子网的缓解控制方法、访问控制策略、网络分段和防火墙。实施主动式策略，例如配置速率限制；在 CDN 上缓存内容；以及使用专用的 DDoS 检测、防范和保护产品。

要想保护 DNS 基础架构，请持续监控和分析入站 DNS 流量，并选择使用混合平台而不是传统 DNS 防火墙。了解攻击者使用的手法、技术和程序有助于您更好地防范 DDoS 攻击。

勒索软件防护

如本报告前文所述，使用网络分段，尤其是微分段来实施 Zero Trust，对于限制勒索软件在金融机构的传播极为关键。实施像这样的可靠网络安全措施，有助于防御勒索软件攻击者采用的高级技术。此外，时刻保持警惕并使用 MITRE ATT&CK 框架，来深入了解攻击者常用的手法和技巧，并按照打破勒索软件杀伤链中所述强化您的行动手册。

持续更新您的防御系统，教育员工识别并有效应对潜在威胁。将强大的外围防御、端点保护、电子邮件过滤和定期补丁管理融于一体。建立对网络流量、系统日志和用户行为的持续监控，并实施威胁检测实践，来主动识别勒索软件威胁。

定期实施安全的数据备份，包括物理隔离的备份，以确保在遇到勒索软件攻击时能够快速恢复关键信息。为所有用户帐户实施 MFA 来额外增加一层安全防护。

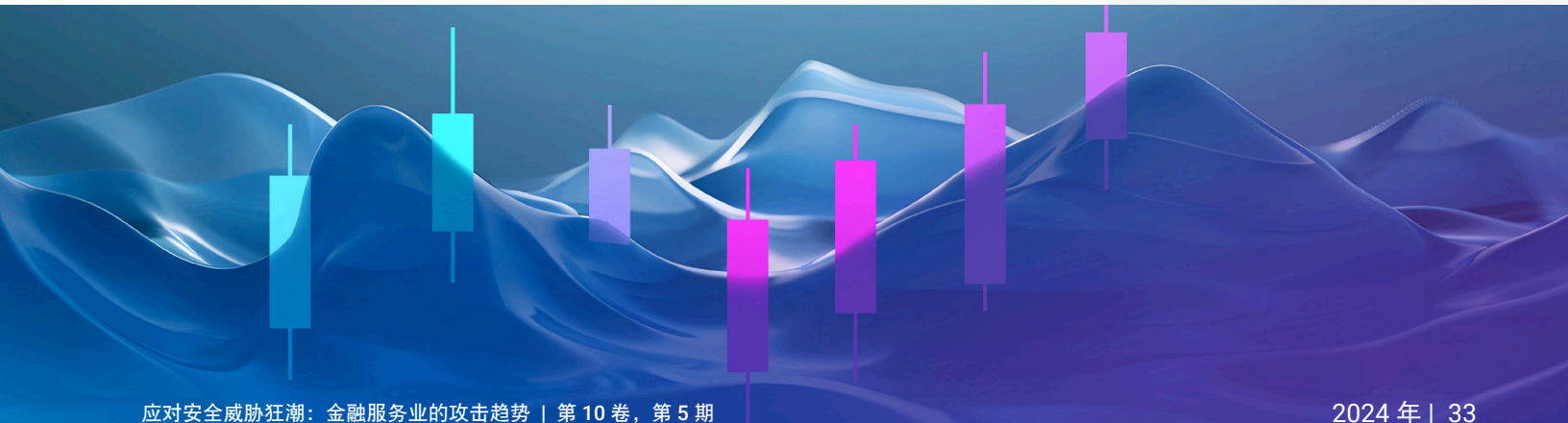
实施这些全面的防范策略之后，您就可以大幅增强金融机构抵御各种网络威胁的能力，确保运营连续性，保护您的声誉，以及维护客户信任。

结论

金融机构纷纷迎接数字化转型，意在提升客户体验、运营效率和竞争优势，然而安全挑战日益加剧，监管环境不断变化，合规也压力越来越大。在本期 SOTI 报告中，我们探讨了金融服务业面临的各种由来已久和最新出现的威胁，这种形势突显了持续评估和增强安全解决方案的必要性。随着威胁手段越来越复杂，务必要加强防御措施和完善安全策略，确保始终领先一步。

而现在，金融机构已经取代了长久以来作为 DDoS 攻击头号目标的游戏行业的位置，这种令人担忧的趋势突显了不断上升的风险。黑客行动主义和地缘政治气候等因素使得金融服务业相比从前更易遭受攻击。同时，针对金融机构的品牌仿冒和钓鱼网站产生的流量规模和严重程度，以及攻击者在先前的仿冒网站下线后创建新域名的速度之快，都令人触目惊心。对于企业而言，跟踪这些活动会耗费大量资源，安全团队需要各种解决方案，包括下线服务、威胁情报以及跨多个数字渠道检测品牌仿冒和网络钓鱼活动。

在成为网络钓鱼和其他骗局的受害者后，消费者和监管机构通常会追究金融机构的责任，即使机构没有直接过错也是如此。更重要的是，网络钓鱼和品牌仿冒通常是更危险攻击的前兆，因此及早打断攻击循环至关重要。能否果断采取行动意味着两种截然不同的结局：或是发生数据泄露，登上次日的头条新闻；或是成功保住机构声誉和客户信任。



鉴于针对金融机构的攻击永无休止，保护机密信息以防止欺诈和滥用仍是一个艰巨的挑战。对于有效防御针对员工的网络钓鱼攻击和防止勒索软件在网络中传播到关键资产，采用像 Zero Trust 这样的安全框架至关重要，这还能确保遵守现有和新出现的全球法规。

本报告提供了有关金融服务业最新攻击趋势的可行见解，使您能够加强防御。通过时刻保持警惕并实施本报告中概述的策略，您就可以在不断演变的威胁环境中，更好地保护企业和客户。

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

DDoS（第 7 层）

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。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。

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。

本报告中的数据涵盖了从 2023 年 1 月 1 日到 2024 年 6 月 30 日的 18 个月时间段。

品牌仿冒攻击

Akamai Brand Protector 是一款防滥用解决方案，旨在保护企业及其客户免遭品牌仿冒攻击，例如网络钓鱼、假冒网站、虚假社交帐户和恶意应用程序。该产品使用 Akamai 的全球边缘网络，每天分析超过 900 TB 的数据量来检测威胁，以防影响到客户。此情报还借鉴了来自合作伙伴的第三方信息源，以便跨各种平台提供全面的潜在威胁视图。

该产品会分析检测到的可疑域的各种特征，并确定其风险水平，从而计算出该域的威胁得分。此外，它还会监控这些可疑域，跟踪关联的数据，并提醒受影响的客户注意这些试图利用品牌形象的恶意活动。

该报告中的数据涵盖了从 2023 年 8 月 1 日到 2024 年 7 月 31 日的 12 个月时间段中，检测到的可疑域数量。

致谢名单

研究总监

Mitch Mayne

编辑与创作

James Casey
Lance Rhodes
Badette Tribbey

审稿和主题撰稿

Cheryl Chiodi
Ziv Eli
Reuben Koh
Gal Meiri
Richard Meeus
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 为抵御针对金融服务业的威胁而提供的解决方案，请访问我们的**金融服务页面**。