V11 EDIÇÃO 02

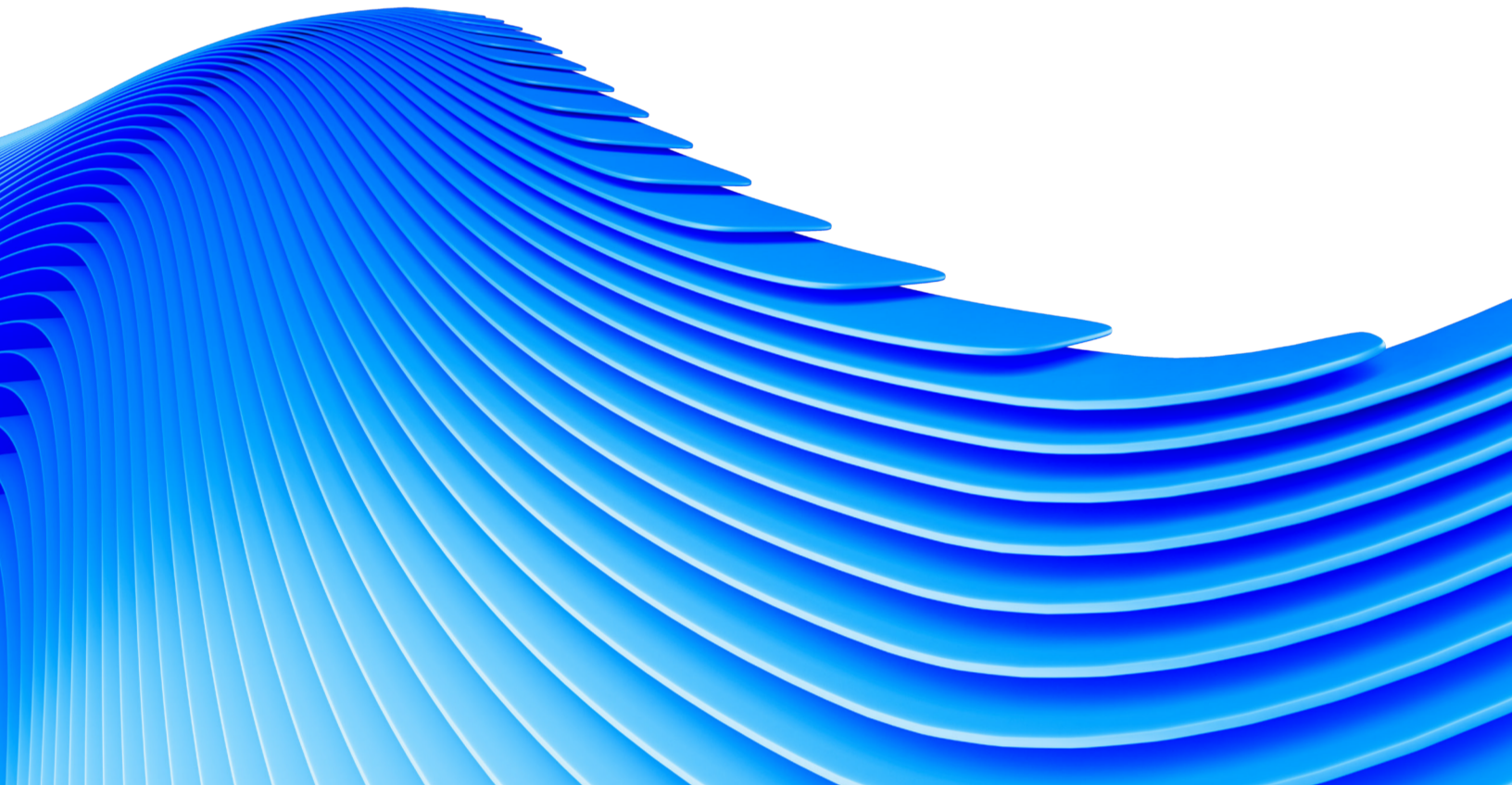
O cenário da segurança de apps e APIs em 2025:

Como a IA está mudando o panorama digital

Akamai

State Of the Internet/**Segurança**

Conteúdo



Introdução

O cenário de segurança de aplicações web no início de 2025 reflete complexidade e sofisticação sem precedentes em vetores de ameaças. As organizações estão enfrentando um aumento acentuado nos ataques direcionados a aplicações web. A Akamai observou mais de 311 bilhões de ataques a aplicações web e APIs apenas em 2024, representando um aumento de 33% ano a ano. Esse surto está diretamente correlacionado à adoção acelerada de serviços de nuvem, arquiteturas de microsserviços e aplicações com IA (inteligência artificial). Os fatores geopolíticos intensificaram ainda mais esse cenário, com os setores de alta tecnologia, comércio e mídia social experimentando o volume mais significativo de ataques DDoS (ataques distribuídos de negação de serviço) de camada 7 (camada da aplicação). Os agentes de ameaça agora estão implantando cadeias de destruição geradas por IA que automatizam todo o ciclo de vida dos ataques.

O relatório também constata que as APIs se tornaram o principal alvo, tendo a Akamai documentado 150 bilhões de ataques a APIs de janeiro de 2023 a dezembro de 2024. A integração de ferramentas SaaS (software como serviço) orientadas por IA com as plataformas principais via APIs expandiu substancialmente a superfície de ataque. As implicações financeiras são graves: os problemas de segurança de APIs atualmente custam às organizações aproximadamente US$ 87 bilhões por ano, e as projeções indicam que esse valor pode exceder US$ 100 bilhões até 2026 sem intervenção adequada. As APIs sombra e zumbis apresentam vetores de ataque particularmente vulneráveis em ecossistemas de API cada vez mais complexos.

A função da IA na segurança de APIs e aplicações web

A IA está transformando os cenários segurança de APIs e aplicações web, aprimorando os recursos de detecção e resposta a ameaças, ao mesmo tempo em que traz novos desafios. Em aplicações web, a IA é usada para automatizar a detecção de ameaças, prever possíveis violações e melhorar os tempos de resposta a incidentes. No entanto, a IA também permite que os invasores gerem malware orientado por IA, técnicas sofisticadas de web scraping e automatizem o ciclo de vida do ataque com metodologias de ataque dinâmicas.

Para APIs, a IA desempenha um papel essencial no gerenciamento e na proteção do grande número de interações de API. As ferramentas baseadas em IA são essenciais para detectar anomalias, identificar padrões de uso indevido e automatizar respostas a ameaças em tempo real. O gerenciamento de APIs orientado por IA continuará a evoluir, integrando análise preditiva e medidas de segurança automatizadas para proteger contra ataques cada vez mais sofisticados. Apesar desses avanços, os ataques acionados por IA a APIs, como preenchimento de credencial e exploração de lógica de negócios, continuam sendo uma preocupação significativa, exigindo estruturas de segurança robustas para combater essas ameaças com eficiência.

Divergentes, mas interconectadas: estratégias para ataques a aplicações web e APIs

Os ataques a aplicações web e a APIs, embora relacionados, visam diferentes aspectos da infraestrutura de uma aplicação:

- Os **ataques a aplicações web** visam componentes voltados para o usuário de aplicações web, como páginas de login voltadas para o público, e geralmente empregam técnicas menos sofisticadas.
- Os **ataques a APIs** se concentram na exploração de vulnerabilidades nos pontos de extremidade de APIs de uma aplicação e na lógica de back-end, exigindo uma compreensão mais profunda da estrutura e do comportamento da API.

As principais diferenças estão na superfície de ataque e na complexidade. Os ataques a aplicações web normalmente visam as partes visíveis da aplicação, enquanto os ataques a APIs exploram os canais de comunicação entre diferentes componentes de software. No entanto, ambos podem fornecer acesso não autorizado a dados confidenciais e recursos do sistema quando bem-sucedidos.

Entender as medidas de cibersegurança para ataques a aplicações web e a APIs simultaneamente é fundamental, pois as aplicações modernas dependem cada vez mais das APIs para funcionalidade. As organizações esperam um aumento de 39% em aplicações web em dois anos, por isso a interdependência da segurança da web e de APIs se tornou mais importante. Ao negligenciar qualquer aspecto, a organização pode se tornar vulnerável a ataques multivetoriais sofisticados, que exploram os pontos fracos tanto no front-end quanto no back-end das aplicações.

Perspectiva exclusiva da Akamai: a revelação de padrões de ameaças

A Akamai explora essa complexidade por meio de sua robusta infraestrutura de rede, capaz de processar mais de um terço do tráfego global da web, oferecendo visibilidade incomparável de padrões de ameaças. A união dessa perspectiva com percepções de suas equipes de pesquisa e ciência de dados permite que a Akamai forneça inteligência abrangente e acionável. Suas descobertas oferecem aos líderes de segurança os insights estratégicos necessários para tomar decisões sobre onde se concentrar na redução de riscos para maximizar o retorno sobre os investimentos em segurança.

Principais insights do relatório

As APIs impulsionadas por IA apresentam maior risco de segurança do que suas equivalentes.

A maioria das APIs impulsionadas por IA é acessível externamente e muitas dependem de mecanismos de autenticação inadequados, o que aumenta a vulnerabilidade à crescente variedade de ataques orientados por IA.

A IA fomenta o avanço técnico dos agentes de ameaças.

Isso inclui avanços como malware orientado por IA, verificação de vulnerabilidades, ataques a sistemas integrados por IA e técnicas sofisticadas de web scraping.

32%

A porcentagem de aumento dos incidentes relacionados ao Top 10 em Segurança de APIs do OWASP

Os ataques à segurança de APIs estão se tornando mais frequentes e os principais problemas identificados pelo Top 10 em Segurança de APIs do OWASP evidenciam vulnerabilidades em autenticação e autorização, expondo dados e funcionalidades confidenciais.

30%

Expansão de alertas de segurança vinculados à estrutura de segurança da MITRE

Os invasores estão usando técnicas avançadas, incluindo automação e IA, para explorar APIs. A estrutura de segurança da MITRE pode ajudar os defensores a identificar esses ataques de forma mais rápida e precisa.

33%

A porcentagem de expansão dos ataques globais na web ano a ano

O aumento dos ataques está diretamente ligado à rápida implementação de serviços de nuvem, microsserviços e aplicações com tecnologia de IA, que ampliam as superfícies de ataque e trazem novos desafios de cibersegurança.

Mais de 230 bilhões

O número de ataques na web direcionados a organizações do setor de comércio,

o que tornou esse setor o mais impactado, com quase três vezes mais ataques do que o setor de alta tecnologia, que ocupa o segundo lugar em número de incidentes.

73%

O aumento no total de ataques na web ano a ano na região APJ (Ásia-Pacífico e Japão),

passando de 29 bilhões em 2023 para 51 bilhões em 2024.

37%

A porcentagem de ataques na web na região EMEA (Europa, Oriente Médio e África) direcionados a APIs,

que representa a maior concentração de tais ataques em todas as regiões.

94%

O crescimento dos ataques DDoS de camada 7

entre o primeiro trimestre de 2023 e o quarto trimestre de 2024.

11,9 trilhões

O número de ataques DDoS de camada 7 direcionados à América do Norte

durante um período de dois anos, do primeiro trimestre de 2023 ao quarto trimestre de 2024.

7 trilhões

O número de ataques DDoS de camada 7 direcionados ao setor de alta tecnologia

entre janeiro de 2023 e dezembro de 2024, que o tornaram o setor mais impactado.

7,4 trilhões

O número de ataques DDoS de camada 7 direcionados à região APJ

durante um período de dois anos, do primeiro trimestre de 2023 ao quarto trimestre de 2024.

20%

A porcentagem de ataques DDoS de camada 7 relacionados a APIs que tiveram como alvo a região EMEA,

representando a maior concentração desse tipo de ataque em todas as regiões.

Aprimoramento de nossa inteligência de ameaças a APIs

A integração da Akamai com a Noname Security aprimorou significativamente os recursos de pesquisa e geração de relatórios sobre ameaças a APIs, fornecendo insights mais profundos sobre os riscos específicos de APIs. A Akamai está usando esse novo conjunto de dados (ainda nos estágios iniciais da integração de dados) para expandir nossa inteligência de ameaças existente e fornecer uma visão ampliada dos problemas de segurança de APIs.

Mapeamento de alertas para estruturas de segurança

Com o tempo, esse novo conjunto de dados fornecerá um mapeamento mais preciso dos alertas de segurança, abrangendo estruturas críticas de cibersegurança e padrões de conformidade, incluindo:

- Modelo MITRE ATT&CK (táticas, técnicas e conhecimentos comuns sobre adversários)
- GDPR (General Data Protection Regulation, Regulamento Geral de Proteção de Dados)
- PCI DSS (Payment Card Industry Data Security Standard, Padrão de Segurança de Dados da Indústria de Cartões de Pagamento)
- ISO (International Organization for Standardization, Organização Internacional para Padronização)
- Open Worldwide Application Security Project (OWASP)

Essas melhorias fortalecem significativamente a capacidade da Akamai de fornecer proteção robusta aos clientes. Ao adotarem essas estruturas, as organizações ampliam a compreensão sobre sua postura de segurança, cumprem os requisitos regulatórios e priorizam seus esforços de proteção com eficácia. Essa abordagem abrangente permite que as organizações aloquem recursos estrategicamente e desenvolvam planos direcionados à proteção de suas APIs e dados confidenciais.

Análise de uma amostra de dados de 30 dias

Neste relatório, examinamos a amostra de dados coletada ao longo de 30 dias para evidenciar a atividade global dos agentes de ameaça em cada estrutura de cibersegurança e em relação aos padrões de conformidade (Figura 1). Além disso, apresentamos uma análise aprofundada dos alertas da MITRE e do OWASP. Também exploramos o impacto desses riscos e incidentes de segurança sobre os padrões de conformidade.

	Atividade de 30 dias	Aumento mensal
OWASP	**5.907.000**	**32%**
MITRE	**2.817.000**	**30%**
ISO	**832.000**	**22%**
GDPR	**669.000**	**21%**
PCI DSS	**881.000**	**16%**

Fig. 1: Detalhamento de alertas de segurança de acordo com estruturas de segurança e padrões de conformidade

Alertas da MITRE

Em um período de 30 dias, observamos um aumento de 30% nos incidentes relacionados a técnicas da MITRE entre nossos clientes. Os invasores costumam recorrer especialmente à T1078 (contas válidas), explorando credenciais legítimas para obter acesso indevido a sistemas e redes. Como as APIs geralmente dependem de tokens para autorização, os adversários que os obtêm podem acessar dados confidenciais sem serem detectados.

Também detectamos a técnica T1566 (Phishing), em que os invasores conduziram campanhas de phishing para extrair tokens de API ou credenciais para ataques futuros. Com a ampliação da superfície de ataque pelas APIs, os agentes de ameaça passam a explorá-las com frequência crescente como ponto de entrada. Além disso, alertas relacionados à técnica T1190 (Exploit Public-Facing Application, exploração de aplicação exposta publicamente) revelaram invasores aproveitando vulnerabilidades de aplicações para se infiltrar nas redes. Outra técnica observada foi a T1580 (Cloud Infrastructure Discovery, descoberta de infraestrutura de nuvem), na qual adversários utilizaram APIs para reconhecimento ao sondar pontos de extremidade de nuvem expostos por meio de chamadas de API.

Embora a MITRE não tenha uma matriz de segurança de APIs dedicada, sua estrutura permanece crucial para as equipes de segurança e organizações que buscam insights sobre técnicas de invasores que visam APIs. Ao relacionar as táticas dos adversários aos comportamentos específicos de API, as equipes de segurança podem aprimorar a resposta a incidentes e a detecção de ameaças identificando estágios de ataque e as respectivas táticas, técnicas e procedimentos envolvidos. Essa abordagem aumenta a eficácia dos defensores na redução dos riscos.

Alertas do OWASP

O OWASP API Security Top 10 é um recurso essencial, que fornece insights práticos sobre o impacto e a gravidade da vulnerabilidade. Ele proporciona aos desenvolvedores e às equipes de segurança os recursos necessários para estabelecer prioridades com precisão, garantindo que as informações permaneçam pertinentes em um cenário de ameaças em constante transformação.

Durante o período de amostra de 30 dias, nossa análise revelou um aumento de 32% nos incidentes relacionados ao OWASP. Vulnerabilidades como BOPLA (Broken Object Property Level Authorization, autorização em nível de propriedade de objeto corrompida), autorização em nível de função corrompida e autenticação corrompida expõem diretamente dados confidenciais ou funções essenciais aos invasores. Mecanismos de autorização insuficientes permitem que os adversários escalem privilégios, apropriem-se de contas e acessem informações confidenciais, tornando-os alguns dos vetores de ataque mais perigosos dentre os que visam APIs.

A BOLA (Broken Object Level Authorization, autorização em nível de objeto corrompida) continua sendo uma vulnerabilidade crítica de segurança de APIs, mas de detecção desafiadora devido à sua dependência de falhas de lógica de negócios. Isso geralmente resulta em subnotificação ou baixas taxas de detecção. Para resolver isso, as organizações devem empregar soluções de segurança de APIs que estabeleçam relacionamentos claros entre os usuários e os recursos que eles normalmente acessam. Isso requer a definição de linhas de base comportamentais por meio de sofisticados algoritmos de machine learning, capazes de reconhecer padrões de acesso anômalos.

O ataque de BOPLA explora problemas granulares de acesso em nível de campo nas APIs, que geralmente são ignorados durante os testes de segurança. Ao contrário do ataque de BOLA, que requer a alteração de IDs de objeto inteiros, os ataques de BOPLA visam propriedades específicas dentro dos objetos. Por exemplo, uma chamada de API DELETE que expõe PII (informações de identificação pessoal) em sua resposta constitui uma vulnerabilidade de BOPLA. Essa sutileza torna os problemas de BOPLA mais prevalentes do que os ataques de BOLA.

Um exemplo prático envolve uma solicitação de cancelamento de assinatura usando apenas um endereço de e-mail, em que a resposta da API inclui inadvertidamente o nome completo e o endereço do usuário. Essa exposição de dados confidenciais a partes não autorizadas ocorre porque o teste de segurança geralmente se concentra em objetos inteiros e não em propriedades individuais. Esse descuido contribui para o aumento da detecção de vulnerabilidades BOPLA em avaliações de segurança de APIs.

Outra vulnerabilidade crítica é o consumo irrestrito de recursos, que os invasores podem explorar para causar interrupções de serviço por meio do esgotamento de recursos ou ataques semelhantes a DDoS. Essa vulnerabilidade apresenta riscos que vão além dos impactos nos serviços, incluindo aumento dos custos operacionais decorrentes do uso excessivo de recursos de nuvem e intensificação dos riscos de ataques de força bruta. Sem a limitação de taxa adequada, os invasores podem sondar rapidamente as APIs, aumentando significativamente a exposição a ameaças e comprometendo a segurança. Além disso, esses ataques geram tráfego substancial, levando a aumentos significativos de custos para as organizações.

O consumo inseguro de APIs, que resulta de validação inadequada, filtragem de dados e falta de mecanismos de segurança durante integrações de APIs de terceiros, apresenta outro vetor de ameaça significativo. Esse problema torna-se cada vez mais preocupante à medida que as organizações passam a depender mais fortemente de APIs de terceiros para a transformação digital. Um estudo recente revelou que mais de 80% das organizações pesquisadas enfrentaram problemas com APIs de terceiros, o que destaca a importância da adoção de um modelo de segurança Zero Trust. Embora essa vulnerabilidade isoladamente não represente um risco catastrófico, ela pode se tornar uma grande ameaça de segurança quando combinada a outras fragilidades, como validação insatisfatória ou dependências inseguras. Por exemplo, a confiança de uma API financeira em transações de terceiros não verificadas pode levar a violações de segurança.

Os alertas de segurança relacionados ao PCI DSS e ao GDPR aumentaram 16% e 21%, respectivamente, enquanto os alertas relacionados ao ISO 27001 aumentaram 22%.

A garantia da conformidade das APIs

As práticas recomendadas para garantir a conformidade das APIs estabelecem a necessidade de associar cada alerta aos padrões normativos e de conformidade específicos que ele viola, a fim de permitir que as organizações obtenham insights imediatos sobre questões críticas e recebam diretrizes práticas para sua resolução. Essa abordagem proativa ajuda as organizações a manter a conformidade com normas, o que reduz o risco de multas regulatórias, repercussões legais e danos à reputação que podem levar a perdas financeiras significativas. Por exemplo, uma empresa aérea foi multada em £ 20 milhões depois que uma vulnerabilidade de API expôs os dados de 400.000 clientes, destacando as graves consequências da segurança inadequada de APIs nos termos do GDPR.

Os padrões de conformidade atuam como barreiras essenciais para que as organizações protejam dados confidenciais, preservem a segurança dos clientes e cumpram as obrigações legais e regulamentares. Padrões como PCI DSS, GDPR e HIPAA (Lei de Portabilidade e Responsabilidade de Seguros de Saúde) exigem o tratamento seguro de informações confidenciais, como dados de pagamento e PII. De acordo com nossa análise de dados, os alertas de segurança relacionados ao PCI DSS e ao GDPR aumentaram em 16% e 21% respectivamente, enquanto os alertas relacionados ao ISO 27001 aumentaram em 22%.

GDPR

O GDPR enfatiza a integração da proteção de dados e da privacidade do cliente em todo o ciclo de vida das APIs. Isso envolve design seguro, autenticação e autorização fortes, limitação de taxa, testes regulares de vulnerabilidade, criptografia e avaliações de riscos, mesmo durante os estágios iniciais de desenvolvimento. Essas medidas garantem a confidencialidade, a integridade e a disponibilidade dos dados.

PCI DSS

De maneira semelhante, o PCI DSS enfatiza a proteção de APIs que lidam com dados de cartões de pagamento, integrando a segurança nas fases de projeto, codificação e teste. Ele exige proteção contra vulnerabilidades da web e testes regulares para identificar e resolver falhas de segurança.

Os requisitos 10 e 11 exigem especificamente o registro e o monitoramento abrangentes de atividades de APIs, incluindo solicitações, respostas, tentativas de autenticação e alterações no sistema. Os registros devem ser mantidos por pelo menos 12 meses, com os três meses mais recentes prontamente acessíveis para análise. Além disso, recomenda que as organizações realizem verificações de vulnerabilidades externas após alterações significativas. Para garantir a conformidade com o PCI (Payment Card Industry), as organizações devem implementar controles rígidos, incluindo limitação de taxa, registro, RBAC (controle de acesso baseado em função) e gerenciamento de sessões para garantir a resiliência das APIs contra ameaças e riscos.

ISO 27001

O padrão ISO 27001 fornece uma estrutura sólida para gerenciar com eficiência os riscos de segurança da informação, melhorar a postura de segurança de uma organização e criar confiança entre colegas e clientes. Entre as práticas recomendadas estão:

- Implementar o controle de acesso (por exemplo, chaves de API) para verificar a identidade do usuário
- Empregar criptografia de dados completa
- Monitorar APIs para detecção de comportamento anômalo
- Realizar avaliações completas de riscos para identificar possíveis vulnerabilidades de APIs

Esses requisitos de conformidade destacam a interseção crítica entre a segurança das APIs e as estruturas normativas. A implementação adequada não só protege dados confidenciais, mas também atende simultaneamente a vários requisitos de conformidade. Para obter mais informações sobre padrões globais existentes e emergentes, consulte a seção Conformidade deste relatório.

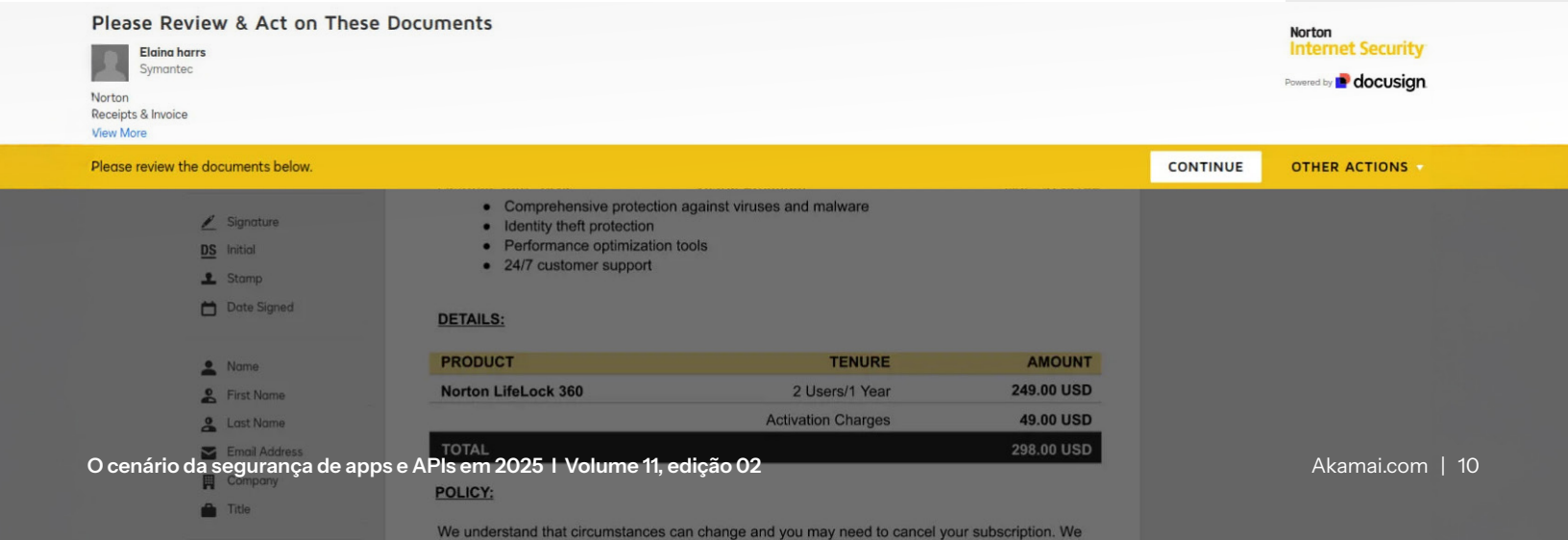
Lacunas de visibilidade de APIs: as trilhas secretas que levam aos dados

Violação de APIs

Em novembro de 2024, a Bleeping Computer relatou um ataque significativo contra um provedor de soluções de assinatura eletrônica. Os agentes de ameaça exploraram um componente central da API de gerenciamento e rastreamento de documentos do provedor, permitindo-lhes enviar faturas fraudulentas a inúmeras vítimas em potencial. Caso os destinatários assinassem inadvertidamente esses documentos, os invasores poderiam solicitar pagamentos de várias organizações.

Esse incidente ressalta os impactos prejudiciais da violação de APIs: agentes mal-intencionados podem explorá-las além da concepção original e transformá-las em canais inesperados para ataques. O surgimento da IA generativa agravou ainda mais esses riscos ao automatizar a descoberta de vulnerabilidades e a superação das limitações de taxa, viabilizando ataques mais rápidos e sofisticados.

Fonte: bleepingcomputer/Wallarm



Desafios na detecção de violação de APIs

As equipes de segurança encontram obstáculos substanciais na detecção de violações de API, principalmente devido à necessidade de estabelecer uma linha de base para distinguir comportamento normal de suspeito. Esse desafio enfatiza a necessidade crítica de monitoramento de comportamento em tempo real para identificar anomalias e ameaças de forma proativa.

Nosso Estudo sobre o impacto da segurança de APIs de 2024 revela uma tendência preocupante: apenas 13% das organizações pesquisadas realizam testes diários em suas APIs, o que representa uma queda expressiva de 37% em 2023. Esse declínio é especialmente alarmante diante do cenário atual de ameaças. A redução acentuada na frequência dos testes compromete a capacidade das organizações de identificar e responder a riscos emergentes, tornando-as mais vulneráveis a ataques sofisticados e potencialmente deixando falhas críticas sem correção por períodos prolongados.

A realização frequente de testes automatizados ao longo dos ciclos de desenvolvimento possibilita que as organizações detectem e corrijam problemas antecipadamente, eliminando a necessidade de ajustes onerosos em ambientes de produção. Em uma época em que a exploração de APIs emprega a cada dia mais métodos automatizados e secretos, os testes proativos desempenham um papel fundamental na mitigação de riscos.

APIs não gerenciadas: APIs zumbi e sombra

A visibilidade do patrimônio de APIs continua sendo um desafio crítico para as organizações, abrangendo tanto o rastreamento oficial de APIs quanto a identificação de dados confidenciais. O Estudo sobre o impacto da segurança de APIs de 2024 revela uma lacuna significativa: 47% das equipes de AppSec mantêm inventários completos de API, mas não identificam as APIs que lidam com dados confidenciais. Os profissionais seniores de segurança relatam limitações semelhantes, com 42% deles enfrentando esse problema de desatenção. E uma constatação alarmante é que número de empresas que possuem inventários completos de APIs e conhecimento da exposição de dados confidenciais diminuiu de 40% em 2023 para 27% em 2024. Esse Estudo sobre o impacto da segurança também destaca as APIs zumbis e sombra como uma das principais causas de incidentes de segurança de APIs.

Inventários incompletos deixam de identificar principalmente as APIs zumbis e sombra. As APIs zumbis, isto é, interfaces desatualizadas que permanecem ativas devido a desativação incompleta, rotatividade de pessoal ou outros fatores, representam vetores de ataque vulneráveis. As APIs sombra, desenvolvidas como soluções rápidas fora dos processos de aprovação padrão, representam ameaças comparáveis. Conforme indica a Pesquisa, um terço das transações de API mal-intencionadas visam as APIs sombra.

Medidas de segurança tradicionais, como WAFs (firewalls de aplicações web), provam ser ineficazes contra essas ameaças. As organizações precisam de soluções avançadas de detecção e monitoramento de APIs para identificar pontos de extremidade vulneráveis de maneira eficiente.

Um inventário abrangente de APIs é a base de uma estratégia de segurança eficaz, permitindo que as organizações monitorem padrões de uso, rastreiem históricos de versões, identifiquem vulnerabilidades e atendam aos requisitos normativos e de conformidade. Essa abordagem estratégica fornece uma visibilidade clara da infraestrutura digital de uma organização, que em última análise, pode fortalecer o gerenciamento de riscos e melhorar a postura geral de segurança.

Destaque de segurança

No primeiro trimestre de 2025, identificamos um ataque a uma empresa de comércio eletrônico por meio de violações de API. A API de envio de SMS da empresa não tinha uma autenticação adequada, permitindo que os invasores a explorassem usando mais de 200 endereços IP diferentes, um único token de autenticação e vários números de celulares aleatórios (legítimos e falsos).

A estratégia de ataque, embora simples, demonstrou grande eficácia: consistia em sobrecarregar a empresa por meio do registro massivo de números de celular e do envio de mensagens SMS para contatos fraudulentos, gerando prejuízos financeiros diretos. Cada número de celular registrado pelos invasores acarretava custos inesperados para a empresa, que depende de um serviço de gateway SMS para viabilizar a comunicação de textos entre seus aplicativos e dispositivos móveis, ou seja, um efeito com potencial de causar prejuízo à marca e à reputação. Uma estratégia de defesa em profundidade com várias camadas de medidas de segurança pode combater esse tipo de ataque e atenuar significativamente os riscos associados.

Nossos alertas revelaram que os agentes de ameaça lançaram 11.057 solicitações POST durante esse ataque, com 5.659 respostas bem-sucedidas (Figura 2).

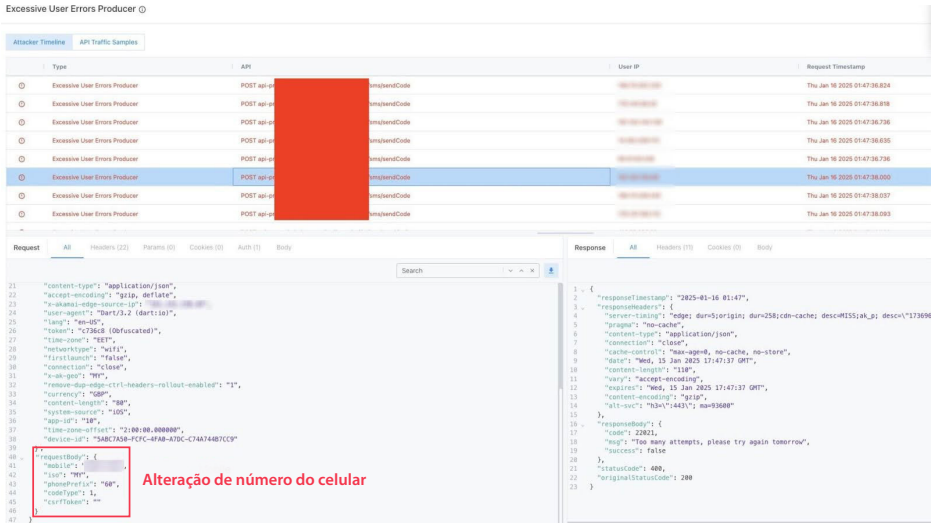


Fig. 2: Os agentes de ameaças inundam a API vulnerável com um fluxo intenso de solicitações

Essas solicitações automatizadas eram idênticas, com exceção de um parâmetro essencial:

Body param **mobile**: the following pattern is detected - **<number>**

Essas solicitações podem sobrecarregar o servidor e levar à negação de serviço ou podem indicar o acesso não autorizado bem-sucedido à API. Os WAFs tradicionais não têm a capacidade de detectar esses ataques sofisticados. Contudo, as soluções avançadas de segurança de APIs, capazes de estabelecer uma referência para o comportamento esperado das APIs, podem detectar esses ataques por meio de análise comportamental, mitigar riscos de forma proativa e impedir que os invasores intensifiquem os danos.

Ataques na web: comparação ano a ano e tendências

A pesquisa da Akamai revelou um aumento substancial nos ataques na web, direcionados a aplicações web e APIs durante o período de relatório, de janeiro de 2023 a dezembro de 2024 (Figura 3). Os volumes mensais de ataques aumentaram de quase 14 bilhões no início de 2023 para mais de 29 bilhões até outubro de 2024. Isso representa um crescimento de 65% nos ataques na web do primeiro trimestre de 2023 ao quarto trimestre de 2024.

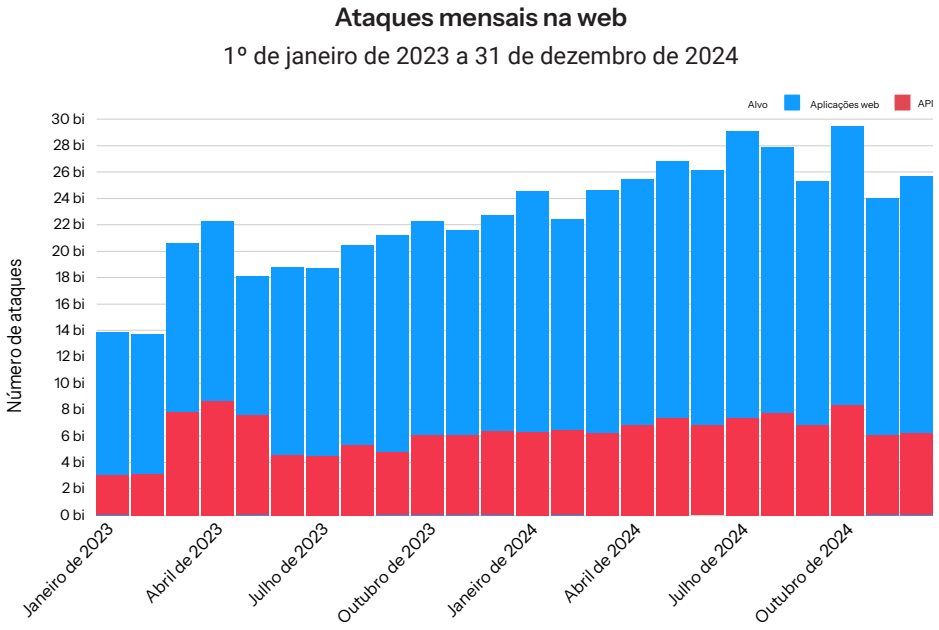


Fig. 3: Os ataques tradicionais na web que têm como alvo aplicações web e APIs aumentam continuamente, o que fica evidente pelo aumento de 65% entre o primeiro trimestre de 2023 e o quarto trimestre de 2024

Principais vetores: a convergência de riscos tradicionais e modernos, impulsionados por padrões comportamentais

Os profissionais de cibersegurança enfrentam complexidades crescentes ao proteger a infraestrutura digital de suas organizações contra uma variedade de ameaças, que vão desde ataques tradicionais na web a explorações sofisticadas que visam vulnerabilidades e configurações inadequadas.

Violações de restrições das solicitações de API: uma ameaça crescente

Uma análise abrangente dos pontos de extremidade de APIs ao longo de dois anos revela que as violações de restrição de solicitação de API representam uma área de preocupação para as organizações (Figura 4). Essas violações se manifestam quando as solicitações ou respostas não cumprem os parâmetros predefinidos ou requisitos estabelecidos, por exemplo, excedendo os limites de taxa ou enviando entradas de dados inválidas.

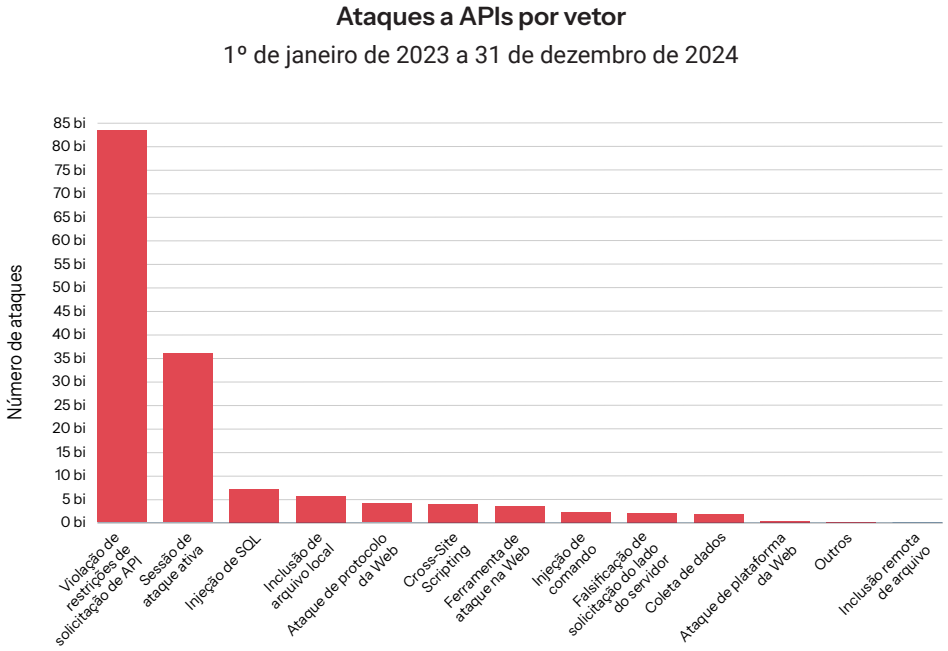


Fig. 4: Mais de 83 bilhões de violações de restrição de solicitações foram registradas em dois anos

As violações de restrição de solicitações de API representam uma ameaça crescente, com mais de 83 bilhões de ataques registrados ao longo de dois anos. Esse vetor de ataque teve um surto substancial de 24% de 2023 a 2024, destacando os perigos das violações de APIs. A prevalência dessas violações serve como um indicador essencial de possível violação de API, que pode precipitar uma cascata de efeitos adversos, incluindo degradação do desempenho do sistema, interrupções de serviço e aumento da vulnerabilidade a ataques direcionados.

Sessões de ataque ativas: ataques únicos que exigem uma solução criativa

As soluções da Akamai utilizam ferramentas de segurança inovadoras para combater os desafios únicos impostos por ataques específicos às APIs. No centro dessas soluções, há um mecanismo proprietário para detectar sessões de ataque ativas, que atua como uma ferramenta de defesa estratégica. Esse sistema usa a própria inteligência de ameaças da Akamai para identificar e rastrear comportamentos suspeitos, permitindo que as organizações frustrem proativamente as ameaças antes que elas se transformem em ataques em grande escala.

O sistema sinaliza agentes de ameaça e adota uma abordagem de "bloqueio temporário". Quando se trata de ataques modernos, os adversários dependem principalmente da automação para conduzir suas atividades de reconhecimento e execução de ataques. A Akamai identifica rapidamente essas sessões de verificação de vulnerabilidades, reage bloqueando o cliente temporariamente e as rotula como sessões de ataque ativas. Essa estratégia impede de forma eficaz que os possíveis agentes de ameaça realizem reconhecimento e explorem vulnerabilidades na rede.

Ao reduzir a janela de oportunidade para agentes mal-intencionados, as organizações podem reforçar substancialmente sua postura de segurança de APIs. Essa abordagem oferece proteção robusta contra uma série diversificada de possíveis ataques e melhora significativamente a resiliência geral da cibersegurança.

A importância dessa estratégia fica evidente em nossos dados. As sessões de ataque ativas tomaram a posição principal para aplicações web e APIs em termos de classificação geral (Figura 5). Em 2023, foram responsáveis por mais de 69 bilhões de ataques. Esse número aumentou para mais de 113 bilhões de ataques em 2024, o que representa um notável aumento de 63% ano após ano.

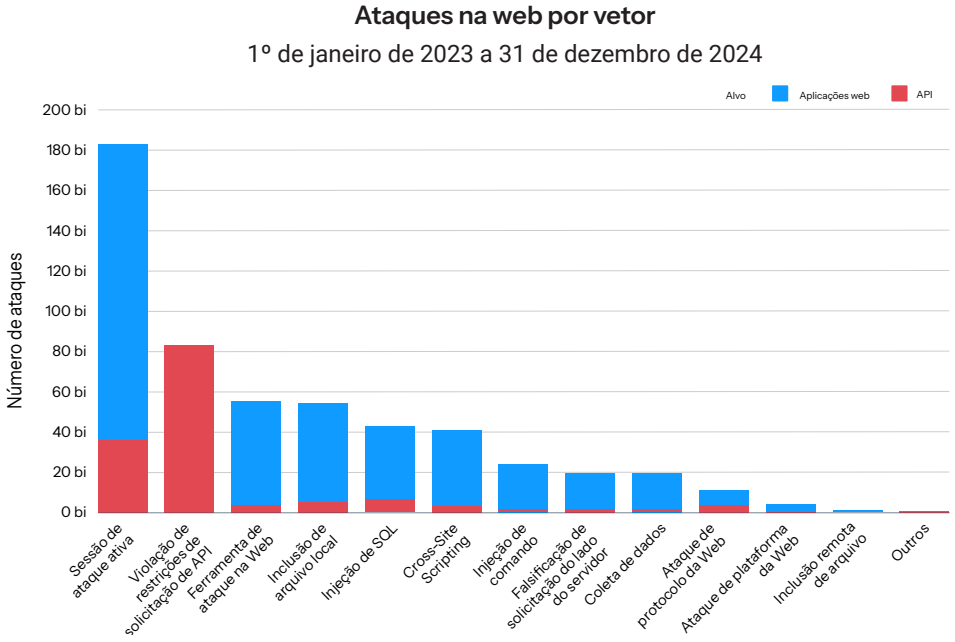


Fig. 5: A sessão de ataque ativa supera todos os outros vetores para aplicações web e APIs, com destaque para a incessante busca dos invasores por vulnerabilidades nas redes de seus alvos pretendidos

Por que não podemos ignorar as vulnerabilidades tradicionais da web na infraestrutura moderna

Os ataques de injeção continuam a demonstrar alta eficácia, apesar do avanço de metodologias sofisticadas de ataque baseadas em comportamento e do aumento da conscientização sobre as vulnerabilidades tradicionais da web. Entre janeiro de 2023 e dezembro de 2024, nossos dados revelam um crescimento expressivo no volume de ataques, com SQLi (Structured Query Language Injection, injeção de SQL) e injeção de comando registrando crescimentos anuais de 60% e 34%, respectivamente. Essas vulnerabilidades permitem que agentes mal-intencionados executem comandos não autorizados, comprometam a integridade do sistema e acessem dados confidenciais sem autenticação adequada, destacando sua relevância contínua no domínio de cibersegurança.

A presença abrangente dos bancos de dados SQL, reconhecidos por sua confiabilidade e escalabilidade no armazenamento de dados, contribui para que esses sistemas sejam alvos constantes. Os quatro bancos de dados mais usados operam com arquiteturas baseadas em SQL, enfatizando ainda mais a natureza crítica desse vetor de ataque.

Embora a lista de Top 10 em Segurança de APIs do OWASP tenha recebido atualizações, como a substituição de ataques de injeção por configuração incorreta de segurança em sua atualização de 2023, o risco associado a ataques de injeção permanece fundamental. Ao mesmo tempo, outros vetores estabelecidos, como LFI (inclusão de arquivo local) e XSS (cross-site scripting), continuam presentes em altos volumes. O Guia dos guardiões da cibersegurança de 2025 mostra a sofisticação das técnicas de exploração de XSS, incluindo injeção remota de recursos, roubo de cookies, desfiguração (deface) de websites e ataques de montagem de sessão, com base em ataques reais observados em 2024.

Essas descobertas ressaltam a necessidade da implementação de estratégias de defesa multicamadas. Os profissionais de cibersegurança devem adotar uma abordagem integrada, combinando codificação de saída eficaz, políticas rigorosas de segurança de conteúdo e WAFs avançados para neutralizar, de maneira eficiente, ataques cada vez mais sofisticados.

Ataques DDoS de camada 7: comparação ano a ano e tendências

De janeiro de 2023 a dezembro de 2024, a pesquisa da Akamai documentou um aumento drástico nos ataques DDoS de camada 7 (camada da aplicação) contra aplicações web e APIs (Figura 6). Os volumes mensais de ataques aumentaram de pouco mais de 500 bilhões no início de 2023 para mais de 1,1 trilhão em dezembro de 2024. Isso representa um crescimento de 94% nos ataques DDoS de camada 7 do primeiro trimestre de 2023 ao quarto trimestre de 2024.

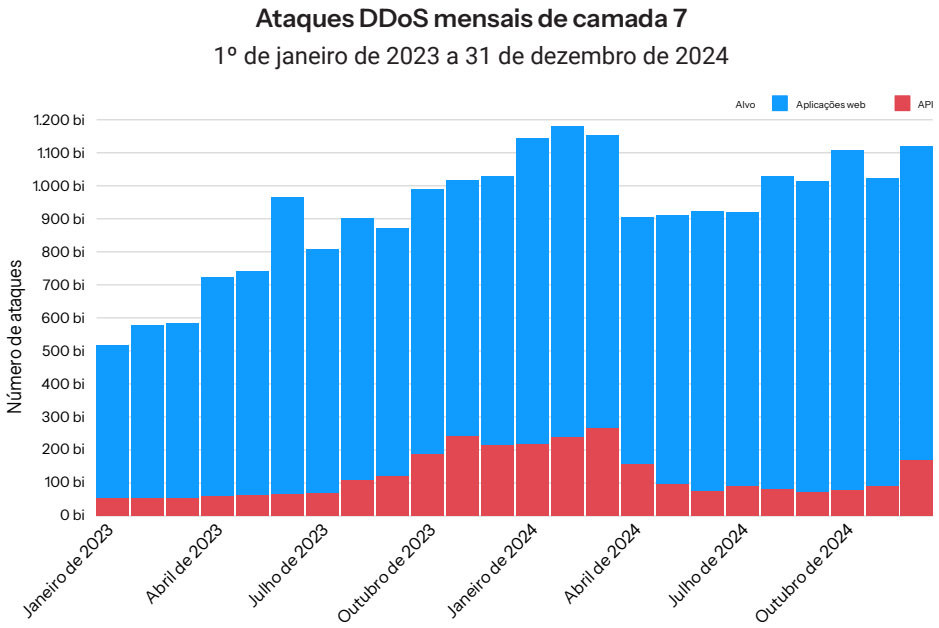


Fig. 6: O número de ataques DDoS de camada 7 direcionados a aplicações web e APIs continua a aumentar, conforme demonstrado por um aumento de 94% entre o primeiro trimestre de 2023 e o quarto trimestre de 2024

Ataques DDoS de camada 7 a aplicações e APIs

Inundações de HTTP persistem como um vetor principal de ameaça na evolução contínua dos ataques DDoS de camada 7, direcionados a aplicações web e pontos de extremidade de APIs. Esses ataques sobrecarregam os recursos de API, inundando-os com altos volumes de solicitações aparentemente legítimas que se concentram em operações com uso intenso de recursos. Os invasores refinaram suas técnicas, criando ataques DDoS de camada 7 para explorar vulnerabilidades específicas na lógica de aplicações web ou APIs, complicando, dessa forma, os esforços de detecção e atenuação. Além disso, os ataques gerados por bots estão cada vez mais sofisticados, gerando padrões de tráfego que imitam o uso legítimo de APIs com precisão.

A transmissão de IA dos invasores: navegação pelo caminho das APIs de forma automática ou manual

As tecnologias de IA generativa revolucionaram a integração empresarial por meio de APIs, "impulsionando" sua ampla adoção e aplicação prática. O mercado de APIs de IA está prestes a vivenciar um crescimento explosivo, com projeção de atingir US$ 179,14 bilhões até 2030, partindo de US$ 44,41 bilhões em 2025, a uma taxa de crescimento anual composta de 32,2%. Contudo, a crescente adoção de IA ocorreu paralelamente a uma escalada significativa nos ataques orientados por IA em APIs. O aumento das vulnerabilidades de API expostas pode ser atribuído em grande parte aos invasores que aproveitam a IA como uma ferramenta para reconhecimento e exploração, seja manual ou automaticamente.

Estratégias de ataque a APIs impulsionadas por IA

Direcionamento estratégico: os invasores empregam ferramentas de IA para identificar e analisar componentes específicos nas APIs visadas, desenvolvendo explorações sob medida com código mal-intencionado gerado por IA para vulnerabilidades específicas. Essa abordagem permite ataques precisos e eficazes nas vulnerabilidades da API.

Ataques automatizados: ao automatizar o processo de ataque, os cibercriminosos reduzem significativamente o tempo e os esforços necessários, identificando e explorando com rapidez as vulnerabilidades da segurança de APIs. Essa automação geralmente envolve bots baseados em IA, que representam uma ameaça grave para empresas e indivíduos.

Ataques volumétricos: os invasores armam a IA para sobrecarregar APIs com tráfego, inundando sistemas de segurança com volume e velocidade significativos. Ataques DDoS automatizados ilustram essa estratégia, em que os bots baseados em IA executam ataques contínuos e se ajustam dinamicamente às medidas de defesa.

Ataques baseados em comportamento: a IA analisa padrões de tráfego para criar ataques baixos e lentos que evitam a detecção operando abaixo dos limites típicos de alerta. Esses ataques geralmente visam vulnerabilidades comuns de APIs, como BOLA e autenticação corrompida.

A ironia das APIs com inteligência artificial

De forma paradoxal, as APIs com IA têm se mostrado notavelmente inseguras. A maioria das APIs impulsionadas por IA é acessível externamente e depende de mecanismos de autenticação inadequados, o que as torna mais vulneráveis a ataques. Nosso Estudo sobre o impacto da segurança de APIs de 2024 revelou que as APIs em ferramentas de IA generativa foram a principal causa de incidentes de API relatados por equipes de segurança de varejo/comércio eletrônico.

O cenário das ameaças de IA crescentes

Os avanços na tecnologia de IA têm impactado profundamente o cenário de ameaças às APIs, ampliando os desafios de segurança. Foram relatados aumentos recordes nas vulnerabilidades de API orientadas por IA no ano passado, com fontes afirmando que, pela primeira vez, a maioria das vulnerabilidades exploradas registradas pela CISA (Cybersecurity and Infrastructure Security Agency) dos EUA estava relacionada a APIs.

Ataques a aplicações web impulsionados por IA e estratégias de defesa

A influência da IA na segurança de aplicações web, com a introdução de novos vetores de ataque e recursos defensivos, também foi profunda. As principais áreas em que a IA alterou significativamente o cenário de cibersegurança para ataques a aplicações web incluem malware aprimorado por IA, verificação de vulnerabilidades orientada por IA, ataques a sistemas envolvidos com IA, técnicas sofisticadas de web scraping e sistemas WAF com tecnologia de IA.

Malware aprimorado por IA

Especialistas em cibersegurança identificaram malwares sofisticados que exploram IA para atacar aplicações web. Em uma campanha de e-mail de 2024, destinada a usuários franceses, os invasores inseriram um código mal-intencionado, provavelmente desenvolvido com auxílio de IA generativa, para executar o malware AsyncRAT. Esse exemplo destaca a crescente tendência de criação e implantação de malware auxiliado por IA, o que representa novos desafios para os profissionais de segurança de aplicações web.

Verificação de vulnerabilidades direcionada por IA

A IA revolucionou a verificação de vulnerabilidades para aplicações web, oferecendo recursos defensivos e ofensivos para uso benéfico ou mal-intencionado. Essas ferramentas orientadas por IA agora automatizam as pesquisas por vulnerabilidades comuns, como SQLi, XSS, falsificação de solicitação entre sites e SSRF (falsificação de solicitação do lado do servidor). Além disso, realizam análises orientadas por IA de possíveis impactos e geram recomendações acionadas por IA para etapas de correção.

Ataques a sistemas envolvidos com IA

A integração da IA, principalmente de LLMs (modelos grandes de linguagem), em aplicações web introduziu novas vulnerabilidades de segurança. *Ataques de injeção de prompt* visam sistemas de IA para contornar as proteções do modelo. Um exemplo notável inclui uma vulnerabilidade na IA do Slack, já corrigida, que permitiu a coleta de dados de canais privados por meio de injeção indireta de prompt. Os *ataques de envenenamento de dados* corrompem o funcionamento dos modelos de IA ao alterar estrategicamente uma pequena fração dos conjuntos de dados, podendo comprometer a integridade e a confiabilidade do sistema. *Técnicas de Jailbreaking* ignoram as proteções de LLM, permitindo que os invasores substituam restrições, extraiam dados confidenciais e produzam resultados danosos. Esses vetores de ataque emergentes exigem vigilância reforçada e novas estratégias de defesa.

Técnicas sofisticadas de web scraping

A IA aprimorou os recursos de web scraping e, com isso, criou novos desafios para a segurança de aplicações web. Essas ferramentas de scraping direcionadas por IA agora oferecem métodos de extração de dados mais eficientes e melhor capacidade de evasão de medidas anti-scraping. Desde o início da década de 2020, técnicas sofisticadas de web scraping têm utilizado a IA para processar dados, mas houve um aumento substancial recente na frequência de scraping realizado em LLM. Em grande parte, esse fenômeno se deve ao crescimento das consultas baseadas em agente, que têm impulsionado a demanda por fontes de dados em tempo real (não estáticas).

Isso fez com que o custo médio por solicitação em aplicações web variasse entre US$ 0,01 e US$ 0,50, dependendo de fatores como complexidade da solicitação, infraestrutura de hospedagem, entre outros. O comércio foi o setor mais impactado pelo aumento do scraping em LLM inicialmente. No entanto, o cenário evoluiu e agora outros setores, como serviços financeiros, jogos de azar, mídias digitais e mídias de vídeo, também estão enfrentando os impactos dessa mudança.

Sistemas WAF com tecnologia de IA

Por outro lado, com o impulso da IA, os sistemas WAF de última geração estão sendo aprimorados para detectar e mitigar de maneira mais eficiente uma ampla gama de ciberameaças, incluindo bots, ataques DDoS, scrapers e scanners. Os sistemas WAF com tecnologia de IA ajudam a combater ataques cibernéticos sofisticados, pois WAFs tradicionais com conjuntos de regras estáticas têm dificuldade contra ameaças de dia zero e exigem atualizações manuais.

A estratégia de machine learning multicamadas proporciona reconhecimento de padrões, aprendizado adaptável, detecção de anomalias e melhor tempo de resposta. Por meio de treinamento que se baseia em bilhões de eventos diários e da aplicação de uma abordagem em camadas com monitoramento contínuo, os sistemas WAF com tecnologia de IA visam antecipar proativamente ameaças em constante evolução e garantir a proteção dos clientes.

Tendências do setor

Dentre os setores, o comércio apresentou um número de ataques na web superior a qualquer outro setor, quase três vezes maior do que o setor de alta tecnologia, o segundo mais atacado entre o primeiro trimestre de 2023 e o quatro trimestre de 2024 (Figura 7). Além disso, durante o mesmo período, o setor de comércio registrou um volume de ataques a APIs muito superior à soma total dos ataques a APIs enfrentados pelos 10 principais setores restantes.

Ataques na web por setor

1º de janeiro de 2023 a 31 de dezembro de 2024

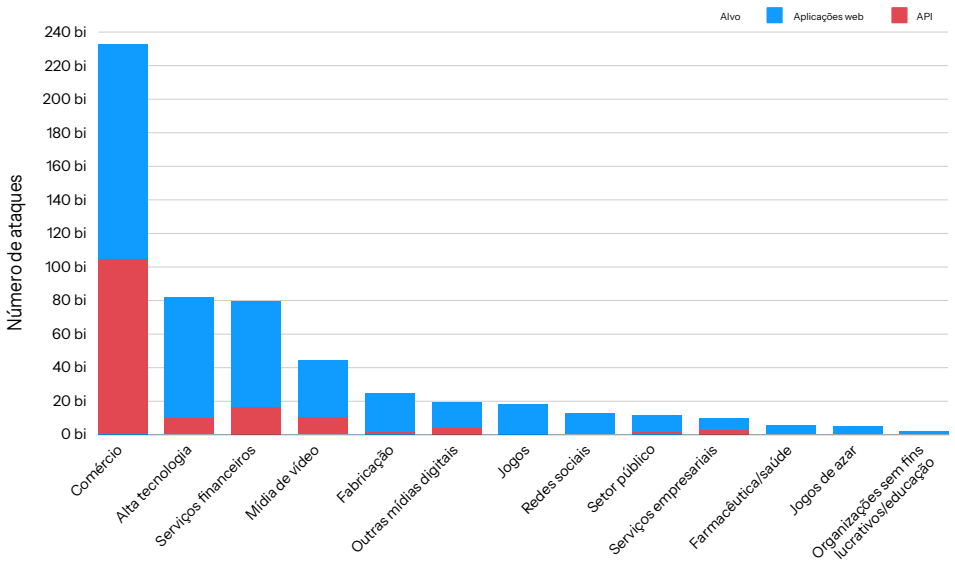


Fig. 7: Comércio, alta tecnologia e serviços financeiros foram os três principais setores mais visados por ataques na web

No geral, os ataques DDoS de camada 7 (camada da aplicação) tiveram como principal alvo o setor de alta tecnologia, que foi o mais visado dentre todos. Durante o período do primeiro trimestre de 2023 ao quarto trimestre de 2024, o número de ataques ultrapassou 7 trilhões. O setor de alta tecnologia foi seguido por redes sociais e comércio (Figura 8). No entanto, ao longo desse mesmo período, o setor de comércio voltou a registrar o maior número de ataques DDoS de camada 7 direcionados a APIs, ultrapassando novamente os demais setores.

Ataques DDoS de camada 7 por setor

1º de janeiro de 2023 a 31 de dezembro de 2024

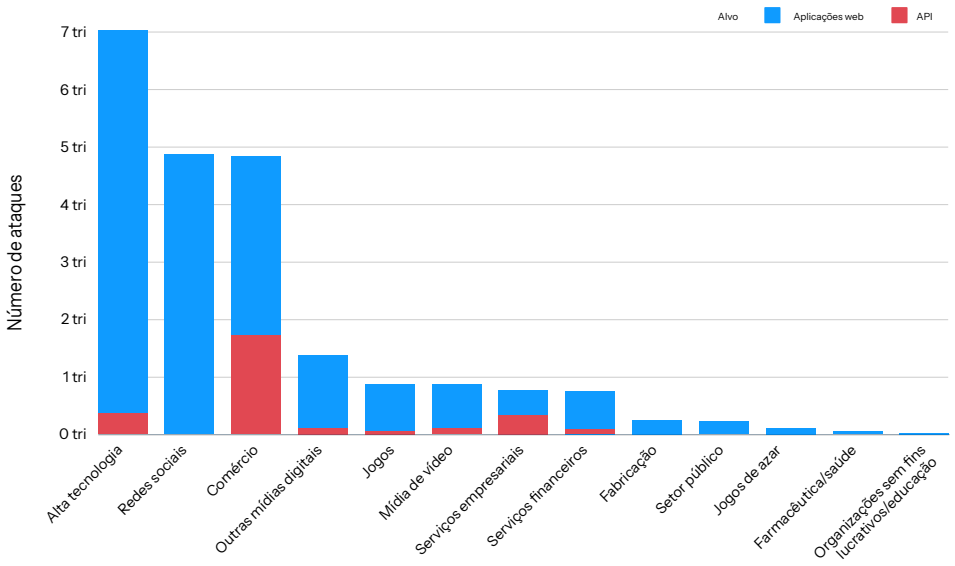


Fig. 8: Ataques DDoS de camada 7 por setor

Comércio

Além de incorrer em mais de 230 bilhões de ataques na web, que representaram mais de 40% do total geral entre 2023 e 2024, o setor de comércio foi alvo de uma escala inédita de ataques DDoS de camada 7. Dados da Akamai indicam que, durante esse período, foram registrados mais de 4,8 trilhões de ataques.

Esse volume total revela um padrão de segmentação estratégica, em que as aplicações web são alvo de cerca de 64,25% dos ataques, enquanto os 35,75% restantes incidem sobre as APIs. Essa distribuição evidencia a abordagem de duplo vetor, adotada pelos invasores, para comprometer as plataformas de comércio, ressaltando a complexidade do cenário de ameaças na atualidade.

As entidades comerciais representam alvos particularmente lucrativos devido à concentração de dados confidenciais de clientes, informações de pagamento e transações financeiras. A exploração direta de credenciais de pagamento roubadas, contas de clientes comprometidas e informações pessoais identificáveis confidenciais gera oportunidades financeiras imediatas para agentes de ameaça, incentivando ataques direcionados. Ao contrário de alguns setores em que dados comprometidos exigem etapas adicionais para serem convertidos em ganhos financeiros, as plataformas de comércio geralmente fornecem ativos diretamente exploráveis aos invasores.

Varejo como alvo principal

O varejo é o segmento mais visado dentro do setor de comércio, enfrentando um volume de ataques significativamente maior devido a diversas características particulares.

As operações de varejo normalmente mantêm ecossistemas digitais complexos, incorporando várias plataformas e sistemas. Suas iniciativas de transformação digital ousadas frequentemente dão prioridade à rapidez no lançamento no mercado em detrimento da segurança mais abrangente, resultando em vulnerabilidades. A adoção de estratégias omnicanal acaba ampliando involuntariamente a complexidade da superfície de ataque. Além disso, a forte dependência de fornecedores terceirizados contribui para uma cadeia de fornecimento complexa, com inúmeros pontos de comprometimento em potencial.

A variação sazonal do tráfego resulta em períodos previsíveis de alta demanda, tornando-se um alvo estratégico para invasores. Durante a temporada de festas de fim de ano, incidentes cibercriminosos aumentam entre 25% a 30%, conforme dados do Internet Crime Complaint Center do FBI. As plataformas de comércio eletrônico também estão entre os alvos mais vulneráveis, registrando um aumento de 31% nos ataques cibernéticos durante dezembro, em comparação com a média anual.

A evolução dos ataques a aplicações web

Os ataques a aplicações web estão passando por uma transformação significativa, impulsionados por avanços tecnológicos e metodologias de invasores em constante mudança. Os agentes de ameaça empregam táticas cada vez mais avançadas para explorar falhas em aplicações web, ajustando continuamente suas estratégias para driblar as medidas de segurança que estão em constante evolução. O aumento das ferramentas de ataque automatizadas, em conjunto com a integração de algoritmos de machine learning, permitiu que os invasores iniciassem campanhas mais precisas e direcionadas contra as aplicações web dos varejistas.

Além disso, a mudança para arquiteturas de microsserviços e o desenvolvimento orientado por API expandiram a superfície de ataque, levando à necessidade de uma reavaliação dos paradigmas de segurança tradicionais. Essa evolução exige uma abordagem proativa dos profissionais de cibersegurança, com ênfase em monitoramento contínuo, mecanismos de defesa adaptáveis e profundo entendimento dos vetores de ataque emergentes no cenário de aplicações web.

O cenário de ameaças de bots

O cenário de ameaças de bots está evoluindo rapidamente por meio do avanço tecnológico, especialmente com invasores que integram recursos de IA generativa. Essa evolução aprimorou as estratégias de ataque por meio de explorações de dia zero mais rápidas e técnicas sofisticadas de evasão que contornam as defesas tradicionais. Evidências mostram que os ataques de fraude por bots baseados em IA contra varejistas aumentaram consistentemente entre agosto de 2022 e abril de 2024, com um pico impressionante de 137% em janeiro de 2024. A dificuldade de detecção agrava ainda mais essas ameaças, com as empresas levando, em média, quatro meses para identificar ataques de bots, enquanto enfrentam prejuízos financeiros e impactos negativos em sua reputação.

Os bots agora funcionam como vetores centrais no cenário cibernético do varejo, facilitando a apropriação indevida de contas, fraude de cartão de crédito e violação de vale-presente. Eles funcionam como facilitadores de campanhas de ataque em grande escala, aproveitando dados roubados de sites comprometidos para executar ataques de preenchimento de credencial em outras plataformas, gerando um efeito cascata que impacta ecossistemas de varejo. Essa atividade contribui para a "industrialização" da fraude online, permitindo que redes criminosas globais utilizem ferramentas automatizadas para expandir suas operações a uma escala muito superior aos métodos manuais tradicionais.

Para obter uma lista de recomendações sobre como proteger melhor as aplicações web e as APIs de sua operação de varejo contra ataques relacionados a bots e IA, consulte a seção Mitigação.

Serviços financeiros

O setor de serviços financeiros se tornou um alvo prioritário de ataques na web e continua enfrentando ataques DDoS de camada 7. Entre janeiro de 2023 e dezembro de 2024, os ataques na web ultrapassaram 79 bilhões, enquanto os ataques DDoS de camada 7 somaram mais de 761 bilhões, afetando tanto aplicações web quanto APIs no mesmo período.

Esse volume sem precedentes destaca a vulnerabilidade do setor e sua atratividade para agentes de ameaças. Diversos fatores contribuem para esse aumento, incluindo o papel essencial do setor na infraestrutura econômica global, o alto valor dos dados financeiros e o potencial de causar interrupções significativas.

A digitalização de serviços financeiros

A digitalização de serviços financeiros expandiu a superfície de ataque para cibercriminosos. A implementação de personalização orientada por IA, operações bancárias como serviço e soluções financeiras integradas trouxe consigo novas vulnerabilidades. Os conflitos geopolíticos, particularmente a guerra Rússia–Ucrânia, têm impulsionado o hacktivismo que visa instituições financeiras. Fatores econômicos, como a ascensão das criptomoedas e a possível implementação de uma reserva cripto, aumentaram o interesse dos agentes de ameaça no setor financeiro.

Os ataques a aplicações web estão se transformando rapidamente, adaptando-se a novas tecnologias e explorando vulnerabilidades emergentes. Os invasores agora utilizam a IA avançada e os algoritmos de machine learning para contornar as medidas de segurança tradicionais e lançar ataques mais direcionados e persistentes. O crescimento das arquiteturas sem servidor e dos microsserviços introduziu novos vetores de ataque, enquanto o uso cada vez maior de APIs ampliou os pontos de entrada para agentes mal-intencionados. Além disso, a transição para aplicativos móveis e baseados em nuvem exigiu uma revisão das estratégias de segurança, pois essas plataformas apresentam desafios únicos na proteção de dados e no controle de acesso.

A relevância do segmento bancário como um alvo estratégico de ataques

No setor de serviços financeiros, o setor bancário se destaca como o segmento mais visado para ataques na web (Figura 9). Como ocorre no setor de comércio, o ataque de preenchimento de credencial também está surgindo como um dos principais vetores de ameaça no setor bancário.

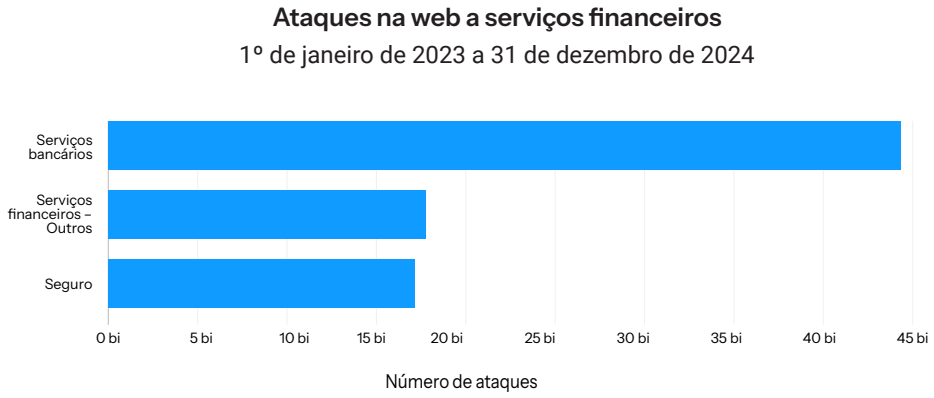


Fig. 9: O segmento bancário é o mais visado em ataques na web no setor de serviços financeiros

A prevalência de serviços bancários online, em conjunto com a natureza crítica do acesso às contas, atrai cibercriminosos. Os retornos financeiros de ataques bem-sucedidos são expressivos, podendo gerar ganhos significativos mesmo com um número reduzido de contas comprometidas. A hesitação do setor bancário em adotar medidas de segurança mais rigorosas, como a autenticação multifator, para evitar impactos na experiência do usuário, tem contribuído inadvertidamente para aumentar sua vulnerabilidade.

A proeminência do segmento bancário como alvo de ataque é ainda mais exacerbada por vários fatores. A sensibilidade ao tempo de inatividade cria oportunidades para extorsão, pois os agentes de ameaças exploram as preocupações com interrupções de serviço. Além disso, a crescente evolução das técnicas de ataque, incluindo o uso de IA e machine learning para escapar da detecção, representa desafios significativos para os mecanismos de defesa tradicionais.
O cenário regulatório, com requisitos rigorosos de conformidade e possíveis multas por violações de segurança, acrescenta outra camada de complexidade aos desafios de cibersegurança do segmento bancário.

Alta tecnologia

O setor de alta tecnologia continua sendo um dos que mais recebem ataques DDoS de camada 7 e na web. Para os objetivos de nossos relatórios, o setor de alta tecnologia abrange os segmentos de telecomunicações, software e hardware empresariais, além de software e hardware para consumidores. Nossos dados indicam que esse setor foi o segundo mais visado no comércio em número total de ataques na web, ultrapassando 81,7 bilhões no período de 2023 a 2024. Além disso, a alta tecnologia foi o setor com a maioria dos ataques DDoS de camada 7: mais de 7 trilhões no período de dois anos.

As aplicações web de alta tecnologia geralmente utilizam consultas complexas de banco de dados e conteúdo dinâmico, criando vulnerabilidades que os invasores exploram para sobrecarregar servidores com facilidade. Essas vulnerabilidades contribuem para a elevada incidência de ataques DDoS de camada 7 que atingem o setor. As redes blockchain enfrentaram um aumento significativo nos ataques DDoS, com invasores usando táticas como inundações de HTTP e transações de spam para impedir transações legítimas, mesmo diante da arquitetura descentralizada da blockchain. O impacto financeiro crítico causado pelo tempo de inatividade operacional no setor de alta tecnologia incentiva invasores a lançarem ataques DDoS capazes de desativar serviços essenciais. A dependência do desenvolvimento de software moderno em arquiteturas centradas em API amplia os riscos, pois invasores frequentemente exploram pontos de extremidade codificados de forma insegura em ataques de inundação de HTTP.

O segmento de telecomunicações enfrenta desafios semelhantes

Afetado por um número significativo de ataques a APIs, o segmento de telecomunicações enfrenta desafios semelhantes de cibersegurança. Aplicações web e APIs nesse setor de alta tecnologia enfrentam ameaças como violações de dados, ataques DDoS e vulnerabilidades na cadeia de fornecimento. Essas fragilidades resultaram em diversas violações de dados de grande repercussão.

Em janeiro de 2025, pesquisadores identificaram vulnerabilidades críticas de API em uma importante rede de telecomunicações, expondo 3.000 empresas a riscos de segurança. A investigação revelou falhas significativas de segurança, incluindo fragilidades no processo de verificação "Conheça seu cliente" e uma vulnerabilidade de passagem de caminho em APIs de back-end que permitia acesso não autorizado a sistemas internos.

A Internet das coisas (IoT) introduz novos vetores de ataque

O setor de alta tecnologia continua a lidar com a evolução das vulnerabilidades de aplicações web e APIs em uma era de rápido avanço tecnológico. Essa evolução abrange a ampla adoção de dispositivos de Internet das coisas (IoT), que introduzem novos vetores de ataque devido à falta de medidas de segurança robustas em muitos dos dispositivos. A rápida expansão das infraestruturas multinuvem frequentemente resulta em configurações inadequadas do ambiente, criando oportunidades para exploração de pontos de entrada por agentes maliciosos.

As vulnerabilidades em dispositivos de Internet das coisas e sistemas de nuvem integrados sem segurança apropriada tornam-se, cada vez mais, alvo de sofisticados ataques orientados por IA. As plataformas SaaS enfrentam riscos elevados de ataques a APIs devido à sua extensa superfície de ataque. A proliferação das soluções de IA e a crescente dependência de plataformas SaaS de terceiros ampliaram significativamente a exposição do setor de alta tecnologia a ataques a APIs. A contínua adoção dessas tecnologias aumenta o risco de exploração, exigindo medidas de segurança rigorosas e monitoramento contínuo.

Tendências regionais

OBSERVAÇÃO: Alteramos o formato de nossos relatórios regionais para tornar os dados mais acessíveis aos leitores e destacar facilmente as tendências de ataque em todas as regiões, incluindo América do Norte (NA); Ásia-Pacífico e Japão (APJ); Europa, Oriente Médio e África (EMEA) e América Latina (LATAM). Também adicionamos um gráfico de visualização rápida para consulta imediata aos dados abordados nesta seção (Figura 10).

Dados de ataques na web Dados de ataques DDoS de camada 7

Região	Volume de ataques na web	Número de ataques DDoS de camada 7	Principais vetores de ataque na web	Principais áreas-alvo	Principais setores-alvo
APJ	80 bi, 14% API	7,4 tri, 6% API	Sessão de ataque ativa, LFI, XSS	Austrália (20,3 bi), Índia (17,3 bi), Singapura (15,9 bi)	Serviços financeiros, comércio, redes sociais
				Singapura (4,7 tri), Índia (607 bi), Coreia do Sul (283 bi)	Mídias sociais, outras mídias digitais, comércio
EMEA	116 bi, 37% API	2,6 tri, 20% API	Sessão de ataque ativa, violação de restrição de solicitação de API, LFI	Reino Unido (30,3 bi), Países Baixos (19,5 bi), Espanha (14,2 bi), Alemanha (12,8 bi)	Comércio, mídias de vídeo, serviços financeiros
				Alemanha (569 bi), Reino Unido (506 bi)	Comércio, outras mídias digitais, mídias de vídeo
LATAM	3 bi, 12% API	258 bi, 18% API	Sessão de ataque ativa, WAT, SSRF	Brasil (19,3 bi), México (2 bi)	Comércio, serviços financeiros
				Brasil (175 bi), México (39 bi)	Comércio, serviços financeiros
América do Norte	327 bi, 29% API	11,9 tri, 16% API			

Fig. 10: Visualização rápida das regiões, de janeiro de 2023 a dezembro de 2024 (LFI indica inclusão de arquivo local; XSS, cross-site scripting; WAT, ferramenta de ataque na web; SSRF, falsificação de solicitação do lado do servidor)

Duas tendências de ataques a aplicações e APIs

Nossa análise comparativa entre regiões sobre ataques a aplicações web e APIs e ataques DDoS de camada 7 ao longo do período de 24 meses, de janeiro de 2023 a dezembro de 2024, destaca duas tendências principais (Figura 11).

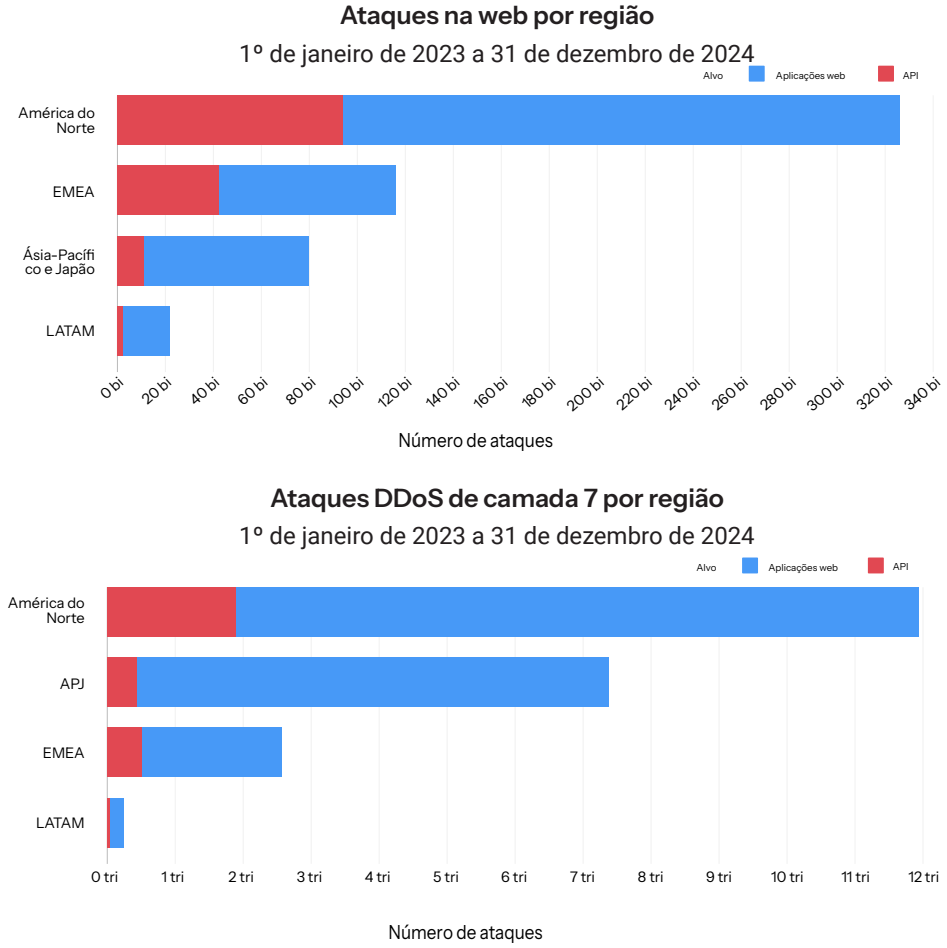


Fig. 11: Ao longo do período do relatório, a EMEA registrou a maior porcentagem de ataques a APIs globalmente, enquanto a APJ apresentou o segundo maior volume de ataques DDoS de camada 7

Tendência de ataque nº 1: os ataques a APIs foram difundidos na EMEA, o que poderia ser atribuído a taxas de adoção de API mais altas do que em outras regiões, bem como a operações bancárias abertas e ao PCI DSS V 4.0, que estão impulsionando o uso de APIs e podem introduzir riscos de segurança. (Consulte a seção Aprimoramento de nossa inteligência de ameaças a APIs para obter uma análise detalhada dos riscos específicos de APIs.)

Dando continuidade à tendência observada em 2023 pela primeira vez, a EMEA registrou a maior concentração de ataques na web voltados para APIs ao longo do período de 24 meses: dos 116 bilhões de ataques na web ocorridos na região, 37% tiveram as APIs como alvo. Em comparação, a América do Norte registrou 327 bilhões de ataques na web e 29% contra APIs. Na região APJ, 14% dos 80 bilhões de ataques na web visaram APIs, enquanto na LATAM, esse percentual foi de 12% do total de 3 bilhões de ataques.

A EMEA também apresentou a maior concentração de ataques DDoS de camada 7 contra APIs (20%), seguida pela LATAM (18%), América do Norte (16%) e APJ (6%). No geral, os ataques DDoS de camada 7 direcionados a APIs representaram uma parcela relativamente pequena do total de ataques na web em cada região. Prevemos que essas porcentagens aumentem ao longo do tempo devido a diversos fatores, como ataques mais sofisticados orientados por bots e uma onda de ataques orientados por IA explorando vulnerabilidades de APIs.

Tendência de ataque nº 2: a APJ apresentou o segundo nível mais alto de ataques DDoS de camada 7 em uma base global de 7,4 trilhões (em comparação com 11,9 trilhões na América do Norte). A EMEA registrou 2,6 trilhões e a LATAM atingiu 258 bilhões. Essa tendência foi identificada inicialmente em nosso relatório SOTI Fortalezas digitais em perigo e continua sendo atribuída à alta concentração de tentativas de ataque contra a mídias sociais na região APJ.

Análise detalhada das tendências nas regiões APJ, EMEA e LATAM

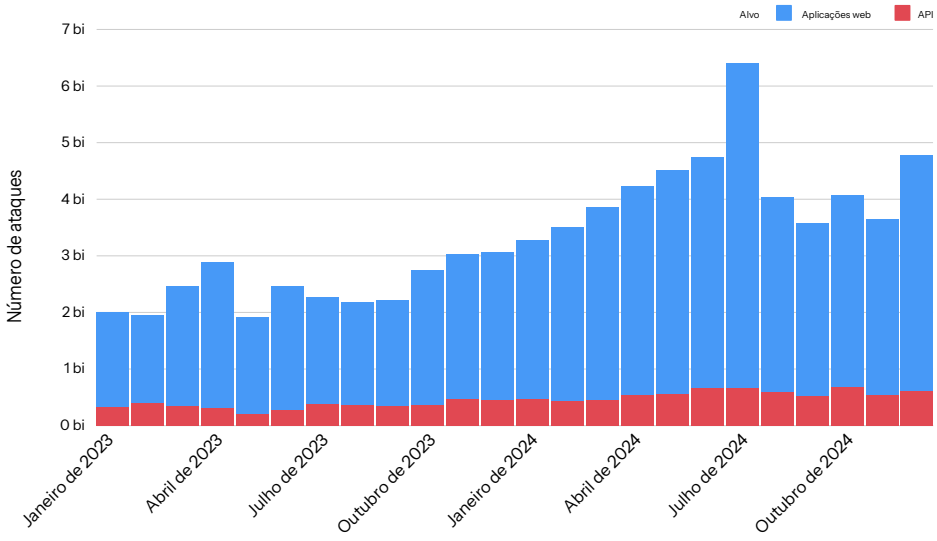
Nesta seção, destacamos algumas das principais tendências observadas nessas regiões. Também incluímos dados específicos de áreas dentro dessas regiões em que há volume suficiente de eventos de ataque para fornecer insights estatisticamente relevantes.

Ataques contra aplicações web e APIs: análise de tráfego

A comparação das tendências mensais de ataques na web entre regiões revela contrastes significativos (Figura 12).

APJ: ataques mensais na web

1º de janeiro de 2023 a 31 de dezembro de 2024



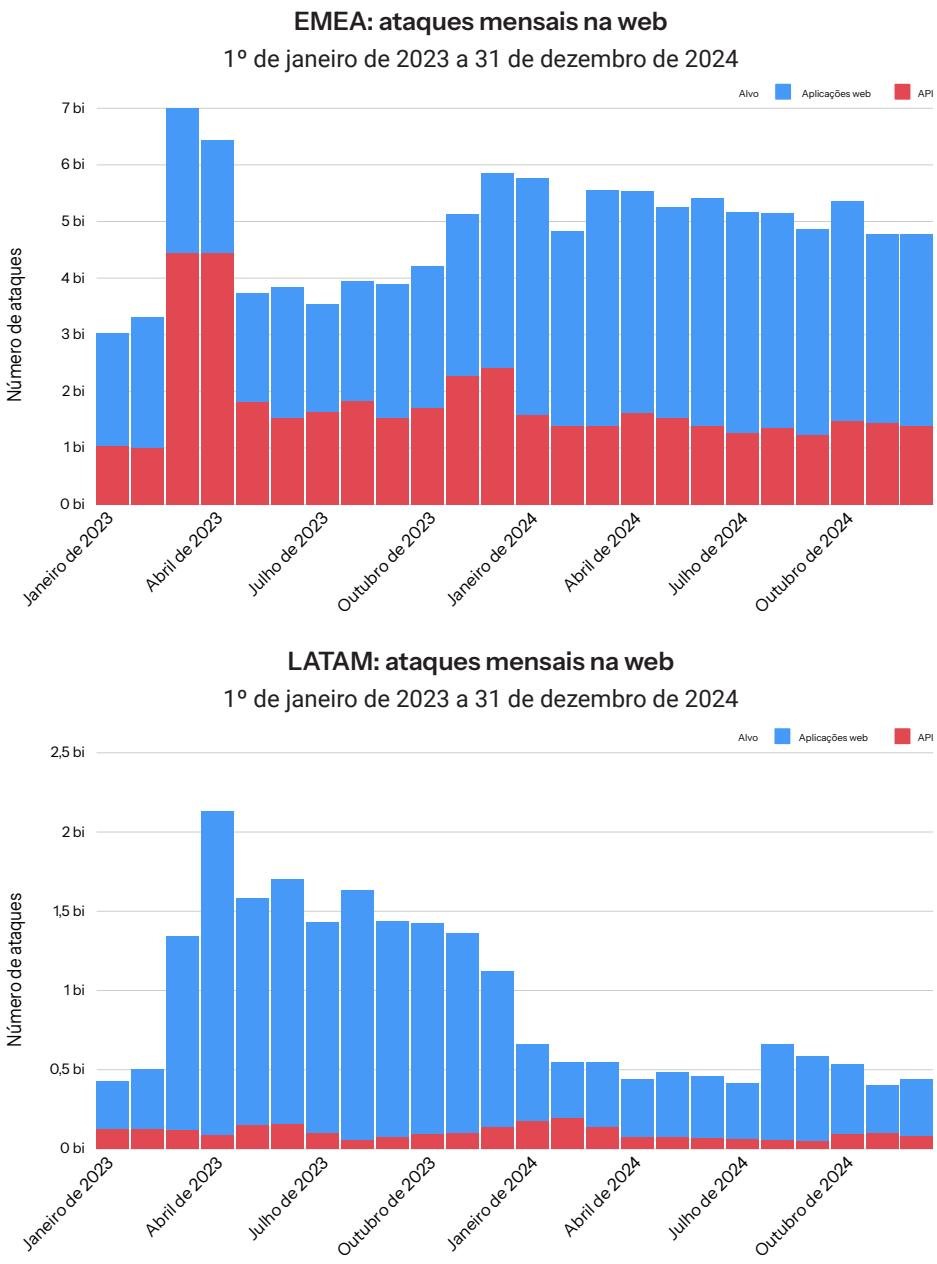


Fig. 12: A atividade dos ataques a aplicações web resultou em um aumento no número total desses ataques nas regiões APJ e EMEA, enquanto na América Latina houve uma queda acentuada

A APJ registrou um aumento expressivo de 73% no total de ataques na web ano após ano, passando de 29 bilhões em 2023 para 51 bilhões em 2024. Na EMEA, o crescimento anual foi moderado, atingindo 16% (de 54 bilhões para 62 bilhões). No entanto, esse aumento foi impactado por um evento discrepante nos dados, que, se desconsiderado, elevaria a taxa para aproximadamente 33%. Na América Latina, os ataques na web diminuíram significativamente, caindo de 16 bilhões em 2023 para 6 bilhões em 2024, uma redução anual de 61%.

O aumento dos ataques a aplicações web parece ser o principal fator que motivou a elevação no número total de ataques na web, enquanto os ataques a APIs permaneceram em níveis reduzidos, especialmente na APJ e na LATAM.

Na EMEA, após um crescimento no primeiro semestre de 2023, relacionado a ataques de grande escala, voltados para o setor do comércio na Espanha, os níveis de ataque a APIs diminuíram e permaneceram em níveis reduzidos em 2024, embora ainda fossem relativamente altos em comparação com outras regiões.

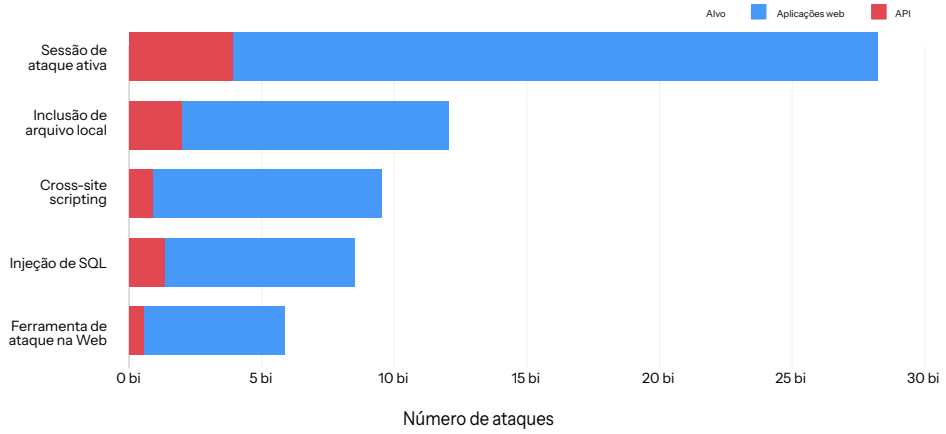
Na LATAM, a queda nos ataques na web coincidiu com uma mudança de foco dos agentes de ameaças, que passaram a direcionar seus esforços do setor de comércio para outras áreas, como produtos farmacêuticos e serviços empresariais, além de diversificar suas estratégias com ataques como ransomware.

Ataques contra aplicações web e APIs: tendências de táticas

Nos últimos dois anos, agentes de ameaças continuaram a recorrer a métodos tradicionais e consagrados, mas o uso de vetores de ataque na web baseados em comportamento também foi elevado (Figura 13).

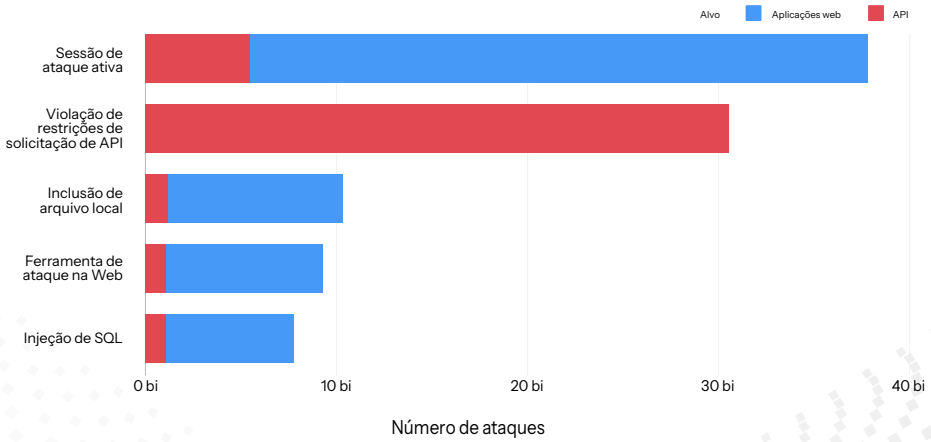
APJ: ataques na web por vetor

1º de janeiro de 2023 a 31 de dezembro de 2024



EMEA: ataques na web por vetor

1º de janeiro de 2023 a 31 de dezembro de 2024



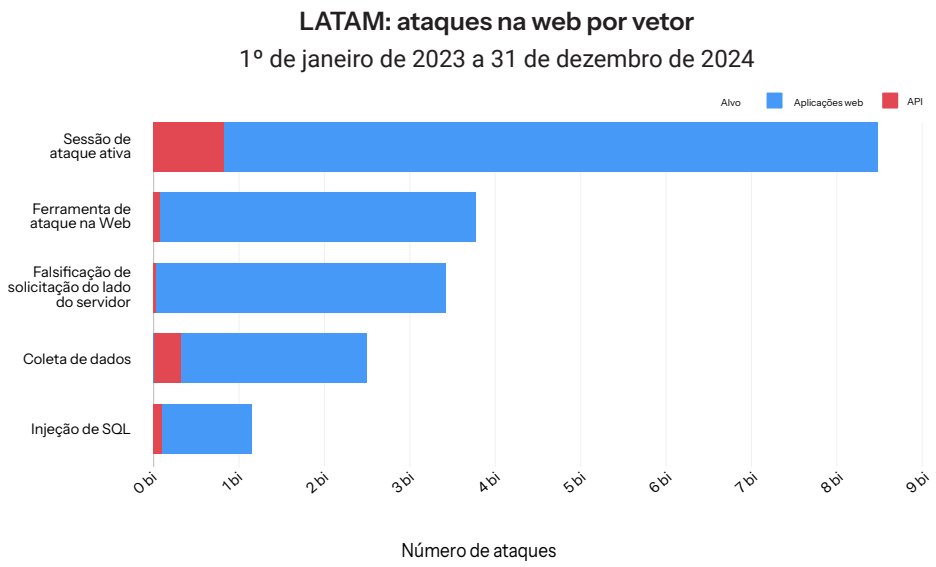


Fig. 13: Em todas as regiões, os principais vetores de ataque incluíram métodos tradicionais e modernos baseados em comportamento, especificamente voltados para violações de APIs

Em todas as regiões, os vetores de ataque tradicionais persistem, o que é consistente com as tendências globais, incluindo LFI, SQLi e XSS, bem como o SSRF registrado na América Latina. Em nosso Guia dos guardiões de 2025, destacamos a importância de manter o foco no XSS e sua relevância contínua na proteção contra vulnerabilidades da web.

Durante esse período, a intensificação das violações de APIs por agentes de ameaças foi acompanhada por um aumento nos problemas com vetores de ataques modernos e baseados em comportamento. Os agentes de ameaças usam esses vetores para identificar vulnerabilidades a serem exploradas. Ao analisar esses vetores em nível regional, pesquisadores da Akamai observaram:

- O principal vetor de ataque em todas as regiões foi a sessão de ataque ativa, na qual nossos controles inteligentes bloqueiam proativamente solicitações de agentes de ameaças conhecidos por um determinado período.
- A violação de restrição de solicitação de API foi o segundo vetor mais prevalente na EMEA, onde se concentram mais os ataques direcionados às APIs. Os invasores exploram APIs ao contornar requisitos como limites de taxas e entrada de dados.
- Em todas as regiões, as ferramentas de ataque na web figuraram entre os cinco principais vetores. Os agentes de ameaça usam esse vetor para sondar o alvo e solicitar informações sobre sua segurança, suas configurações ou possíveis vulnerabilidades passíveis de exploração para fins mal-intencionados.

Para obter mais detalhes sobre esses principais vetores, consulte a sessão Ataques na web.

Ataques contra aplicações web e APIs: principais alvos

Ao avaliar a concentração dos ataques em cada região, observamos que, na APJ, Austrália (20,3 bilhões), Índia (17,3 bilhões) e Singapura (15,9 bilhões) foram os países mais atingidos por ataques a aplicações web e APIs, seguidos por Japão (6,3 bilhões), China (6,2 bilhões), Coreia do Sul (4,9 bilhões), Nova Zelândia (2,9 bilhões) e Hong Kong SAR (2,2 bilhões).

Na EMEA, os países mais afetados por ataques a aplicações web e APIs foram Reino Unido (30,3 bilhões), Países Baixos (19,5 bilhões), Espanha (14,2 bilhões) e Alemanha (12,8 bilhões). Em seguida, destacam-se Áustria com 8,2 bilhões, França (7,5 bilhões), Itália (4,1 bilhões), Suíça (3,7 bilhões), Bélgica (3,5 bilhões) e Israel (3,3 bilhões).

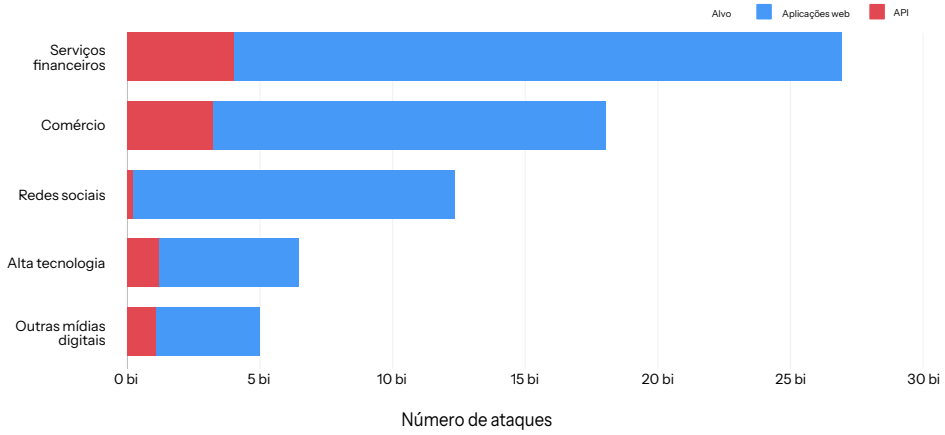
Na LATAM, o Brasil concentrou a maior parte dos ataques a aplicações web e APIs, registrando 19,3 bilhões, enquanto México (2 bilhões) e Chile (0,4 bilhão) apresentaram apenas uma fração desse total na região.

Setores em risco

A análise das tendências por setor revelou que, nas regiões APJ, EMEA e LATAM, comércio e serviços financeiros estiveram consistentemente entre os três principais setores mais visados por ataques na web (Figura 14).

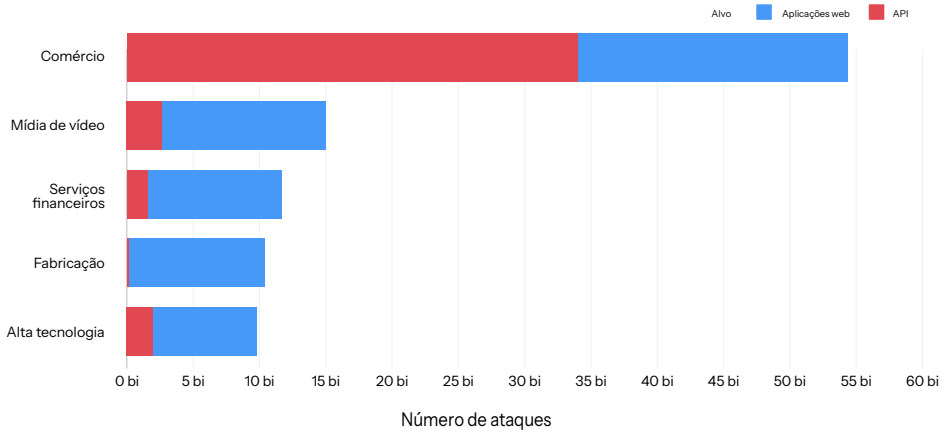
APJ: ataques na web por setor

1º de janeiro de 2023 a 31 de dezembro de 2024



EMEA: ataques na web por setor

1º de janeiro de 2023 a 31 de dezembro de 2024



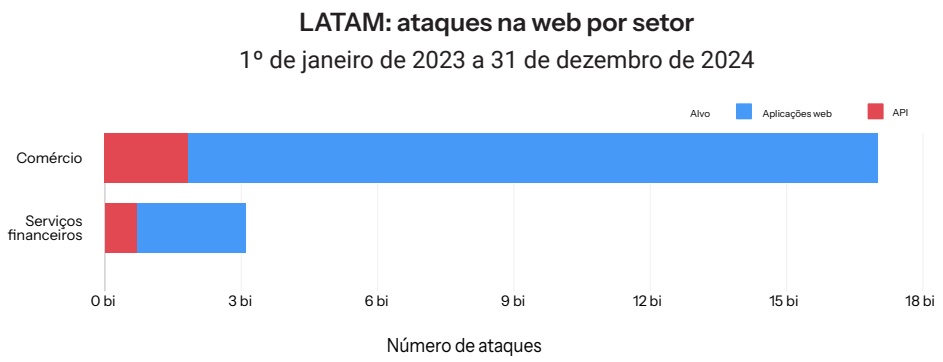


Fig. 14: Os setores de comércio e serviços financeiros estiveram entre os três mais visados nas regiões APJ, EMEA e LATAM

Na região APJ, o setor de serviços financeiros foi o mais atacado, registrando 27 bilhões de ataques na web, seguido pelo comércio, com 18 bilhões. Esses números representam um crescimento anual de 52% e 161%, respectivamente. O setor de mídia digital foi o principal alvo de ataques a APIs, com 22% do total, seguido por comércio (18%) e serviços financeiros (15%).

Na EMEA, o comércio foi o setor mais afetado por ataques na web, tendo atingido 54 bilhões, mais de três vezes do segundo setor mais atingido. Apesar da alta concentração, o total de ataques na web contra o comércio diminuiu 10% anualmente, devido a um aumento excepcional registrado em 2023 que provocou distorção dos dados na região. No entanto, a EMEA ainda registrou um crescimento de 16% ano a ano no número total de ataques na web, impulsionado pelo aumento dos ataques contra outros setores, incluindo serviços financeiros (152%) e manufatura (96%). Ao analisar detalhadamente os ataques direcionados a APIs na região, vemos que 63% do total de ataques na web contra o setor de comércio tiveram APIs como alvo.

A LATAM apresentou uma tendência semelhante, em que os ataques na web contra o comércio somaram 17 bilhões, mantendo-se acima dos demais setores. No entanto, o volume de ataques no setor caiu 76% ano a ano. Enquanto isso, os setores farmacêutico e de serviços empresariais registraram aumentos anuais de 107% e 129%, respectivamente. Além disso, 11% dos ataques direcionados ao comércio envolviam APIs. No setor financeiro, a concentração de ataques a APIs foi ainda maior, chegando a 23%.

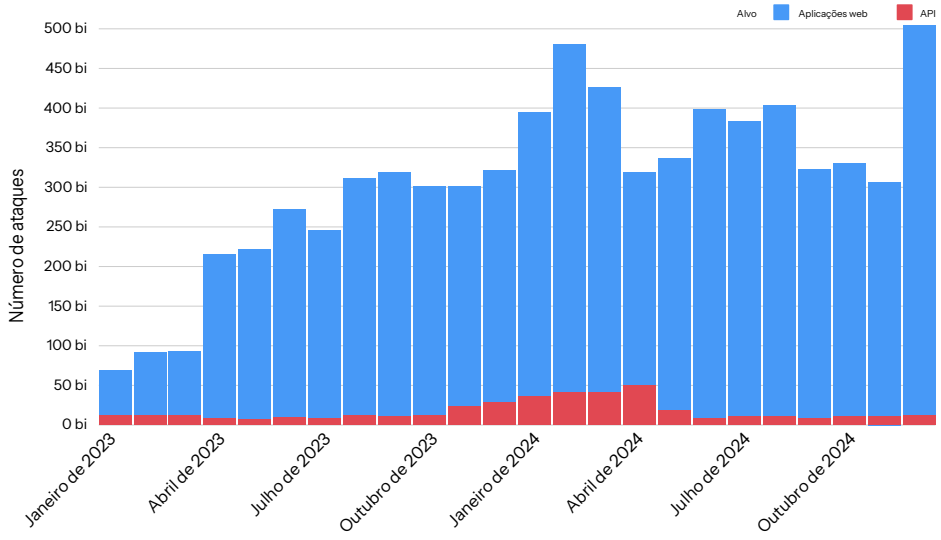
Os setores de comércio e serviços financeiros compartilham características que os tornam alvos frequentes de ataques a aplicações web e APIs: ambos operam em ecossistemas complexos, dependem fortemente de APIs e lidam com dados valiosos. Os agentes de ameaça combinam métodos tradicionais e estratégias emergentes para explorar vulnerabilidades e alcançar seus objetivos.

Ataques DDoS de camada 7: análise de tráfego

Uma comparação das tendências mensais de ataques DDoS de camada 7 entre as regiões revela que a APJ foi o ponto principal e EMEA e LATAM registraram um fluxo e refluxo de ataques (Figura 15).

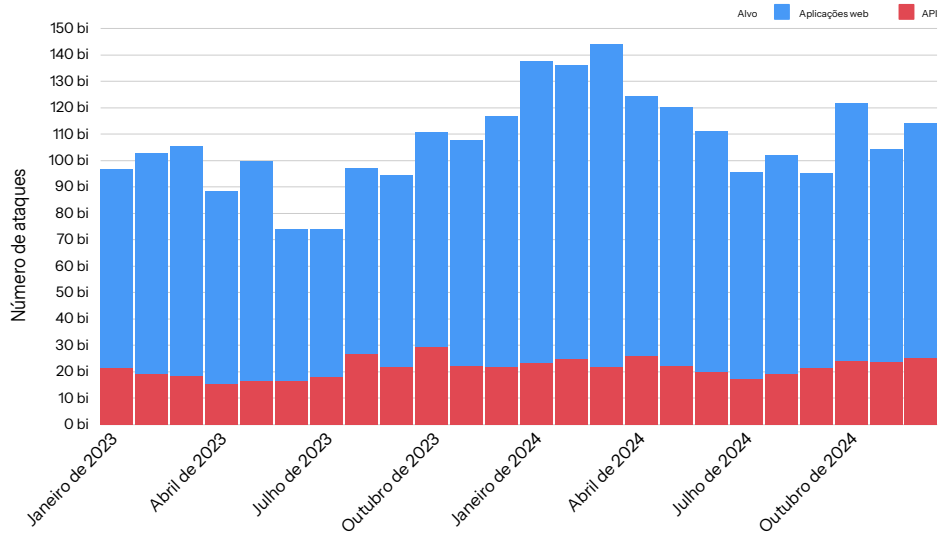
APJ: ataques DDoS mensais de camada 7

1º de janeiro de 2023 a 31 de dezembro de 2024



EMEA: ataques DDoS mensais de camada 7

1º de janeiro de 2023 a 31 de dezembro de 2024



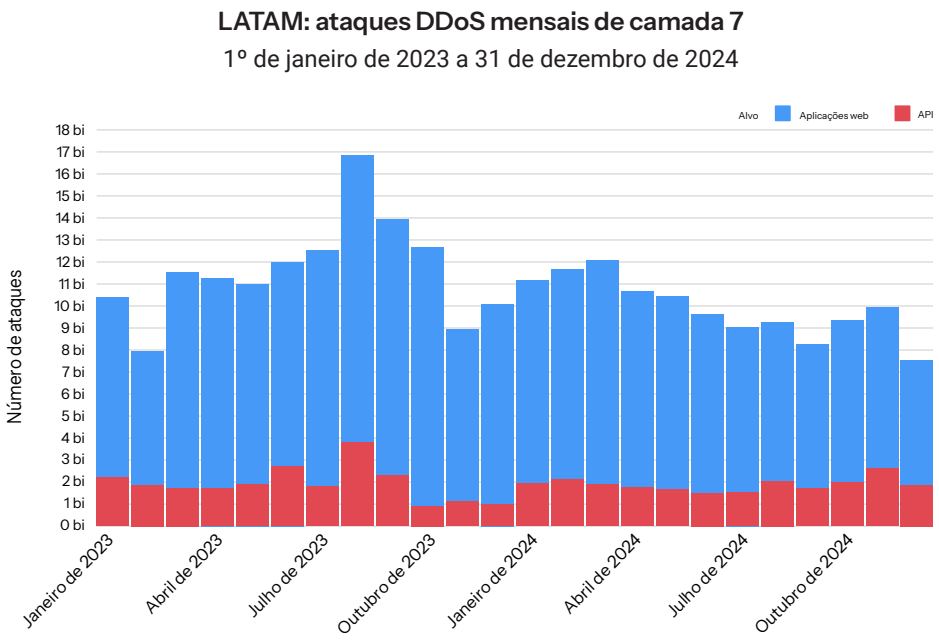


Fig. 15: Os ataques DDoS de camada 7 aumentaram nas regiões APJ e EMEA, enquanto os ataques na LATAM diminuíram em 2024

A região APJ registrou crescimento anual de 66% nos ataques DDoS de camada 7, atingindo seu maior volume em 24 meses com um pico de 504 bilhões em dezembro de 2024. Esse aumento foi impulsionado principalmente por ataques focados no setor de redes sociais.

Na EMEA, os ataques DDoS de camada 7 atingiram o pico em março de 2024, com quase 145 bilhões e, após uma queda, voltaram a aumentar, atingindo um crescimento anual de 20%. Isso pode ser atribuído a uma confluência de fatores geopolíticos e tecnológicos. As tensões contínuas na região têm impulsionado as atividades hacktivistas. Essa tendência é exacerbada pelo aumento de ferramentas aprimoradas por IA e DDoS como plataformas de serviço, que reduziram a barreira à entrada de cibercriminosos.

A região da LATAM sofreu um aumento significativo nas tentativas de ataque DDoS de camada 7 no início do período de relatório, o que coincidiu com um crescimento nos ataques de inundação de HTTP com o objetivo de sobrecarregar os recursos de API (um vetor de ataque discutido em detalhes na seção Ataques DDoS de camada 7: comparação ano a ano e tendências. A atividade atingiu um pico de 16,8 bilhões em agosto de 2023 e depois diminuiu durante o restante do período até atingir 7,5 bilhões, o que representa uma redução anual de 15% nos ataques.

Ataques DDoS de camada 7: principais alvos

Em todas as regiões, observamos pouca ou nenhuma mudança nas áreas e setores visados por agentes de ameaça em comparação com nossa análise anterior de ataques DDoS de camada 7.

Na região APJ, Singapura registrou a maior concentração de ataques, atingindo 4,7 trilhões. Em seguida, estão Índia (1,1 trilhão), Coreia do Sul (607 bilhões), Indonésia (283 bilhões), China (246 bilhões), Japão (111 bilhões), Austrália (108 bilhões) e Taiwan (81 bilhões).

Na EMEA, os países com o maior número de ataques DDoS de camada 7 foram Alemanha (569 bilhões) e Reino Unido (506 bilhões), seguidos por Israel (205 bilhões), Suécia (193 bilhões) e Malta (160 bilhões). A Itália (158 bilhões), a Suíça (147 bilhões), a França (129 bilhões), os Países Baixos (111 bilhões) e a Espanha (96 bilhões) completaram o Top 10.

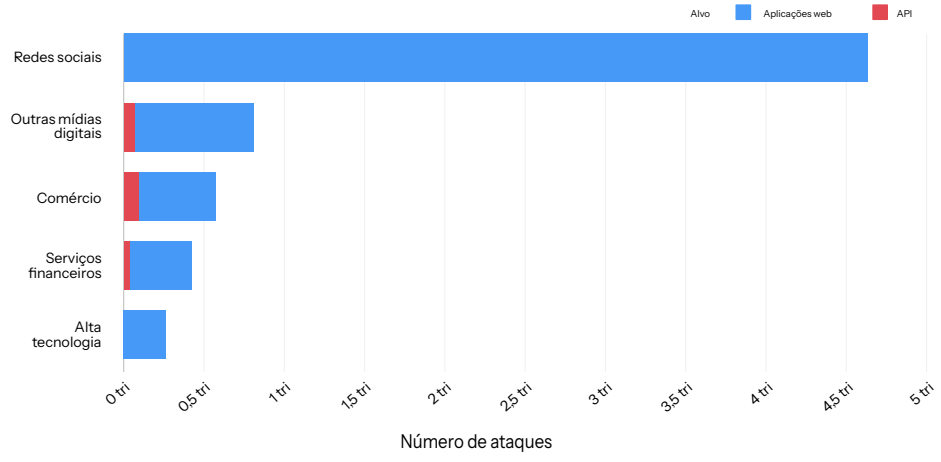
Na LATAM, o Brasil teve a mais alta concentração de ataques DDoS de camada 7 com 175 bilhões, seguido pelo México (39 bilhões) e pela Costa Rica (19 bilhões).

Setores em risco

Não houve alteração nos principais setores afetados pelos ataques DDoS de camada 7 nas regiões APJ e EMEA (Figura 16) em relação ao relatório SOTI de aplicações seguras anterior. Conforme detalhamos nesse relatório, os ataques DDoS de camada 7 contra plataformas de mídias sociais na região APJ aumentaram entre janeiro de 2023 e junho de 2024, em correlação a conflitos militares de grande escala e a eventos eleitorais amplamente mediados ao redor do mundo. Isso não é surpreendente, uma vez que essas plataformas costumam registrar enormes volumes de tráfego durante períodos de instabilidade geopolítica. Como previsto, a tendência se intensificou durante o restante de 2024 devido às eleições na região APJ e nos Estados Unidos. Esses fatores contribuíram para o crescimento anual de 130% dos ataques ao setor.

APJ: ataques DDoS de camada 7 por setor

1º de janeiro de 2023 a 31 de dezembro de 2024



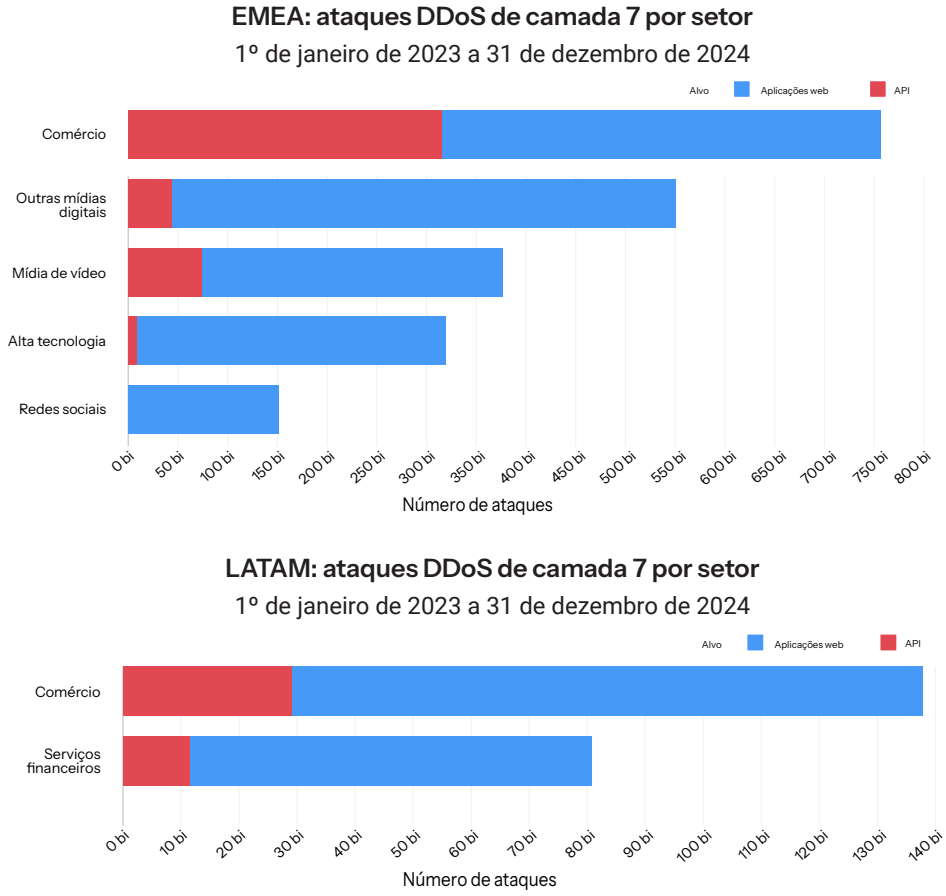


Fig. 16: Os principais setores afetados por região permaneceram inalterados desde nossa análise anterior; o comércio foi consistentemente o setor mais visado por ataques DDoS de camada 7 contra APIs

Na EMEA, o comércio permaneceu como o setor mais afetado por ataques DDoS de camada 7, seguido por outras mídias digitais e mídia de vídeo. Os setores que tiveram o maior crescimento anual nesses ataques incluíram alta tecnologia (70%), mídias sociais (23%) e comércio (14%). Essas alterações demonstram a rapidez com que os invasores podem mudar seu foco entre setores e regiões e destacam a importância de acompanhar tendências mais amplas.

O comércio também foi setor mais visado na LATAM por ataques DDoS de camada 7, seguido por serviços financeiros. Durante o período de relatório, os níveis contínuos de atividade desse tipo de ataque permaneceram razoavelmente consistentes em todos os setores.

Refletindo a tendência global, entre os setores mais visados pelos ataques DDoS de camada 7, o setor de comércio registrou a maior concentração de ataques a APIs em todas as regiões. Na região EMEA, 43% dos ataques contra o comércio visavam APIs, 21% na LATAM e 16% na região APJ.

Devido a fatores como instabilidade geopolítica e o impacto econômico potencial causado por interrupções em serviços de alta visibilidade, setores como comércio, mídias e serviços financeiros foram os principais alvos de ataques DDoS de camada 7 na EMEA e na LATAM nos últimos dois anos. Na seção Tendências do setor, confira uma análise detalhada sobre fatores e métodos que orientam a intensa atividade direcionada aos setores de comércio e serviços financeiros.

Conformidade

Perspectiva global e da América do Norte

O cenário de cibersegurança global em 2025 é caracterizado por complexidade e volatilidade sem precedentes. As tensões geopolíticas, particularmente os conflitos em andamento na Ucrânia e no Oriente Médio, intensificaram as ciberameaças e os ataques patrocinados pelo estado. A ascensão do hacktivismo, especialmente de grupos pró-russos que visam as nações ocidentais, tem complicado ainda mais o cenário das ameaças. Em termos econômicos, a rápida transformação digital em todos os setores ampliou a superfície de ataque, com cibercriminosos visando cada vez mais infraestruturas críticas e aproveitando tecnologias avançadas, como a IA, para aprimorar seus recursos.

Esses fatores, combinados com pressões econômicas globais e mudanças políticas em países mais relevantes, criaram uma tempestade perfeita para profissionais de cibersegurança em todo o mundo. Proteger aplicações web e APIs é um desafio essencial para as organizações. Os esforços de hackers éticos, profissionais de cibersegurança e organizações como a Akamai para garantir a proteção desses pontos de entrada reforçam as crescentes exigências de conformidade.

Órgãos reguladores em todo o mundo estão adotando requisitos mais rigorosos de conformidade em cibersegurança para aplicações. Na América do Norte, a ênfase passou a ser em estratégias abrangentes de gerenciamento de risco, acompanhadas por requisitos obrigatórios de comunicação de incidentes. A Cyber Incident Reporting for Critical Infrastructure Act (Lei de relatórios de ciberincidentes na infraestrutura crítica) dos Estados Unidos, prevista para entrar em vigor em 2026, exige que organizações de infraestrutura crítica mantenham um inventário atualizado de seus sistemas de informação, classifiquem riscos cibernéticos e realizem avaliações de sua postura de segurança anualmente, no mínimo. Essa lei enfatiza a necessidade de medidas de segurança robustas em aplicações, especialmente aquelas usadas em setores críticos, como energia, fabricação de produtos químicos e tecnologia da informação.

Da mesma forma, o Canadá e o México estão alinhando suas normas aos padrões internacionais, concentrando-se na proteção de dados e na segurança de infraestruturas críticas. Apesar das diferenças entre regulamentações específicas, a tendência global aponta para requisitos de segurança de aplicações cada vez mais rigorosos, abrangendo melhor validação de valores de entrada, práticas de desenvolvimento seguro e auditorias de segurança periódicas.

O cenário de segurança de APIs está enfrentando desafios paralelos, com as APIs se tornando alvos principais dos cibercriminosos, devido à sua função essencial na ativação de serviços de integração e troca de dados. Órgãos reguladores em todo o mundo estão respondendo por meio da introdução de normas mais rigorosas que exigem das organizações a implementação de robustas medidas de segurança de APIs.

Entre elas estão a detecção, o monitoramento e a proteção contínua e obrigatória de APIs contra ameaças em constante evolução. Na América do Norte, a prioridade está na realização de avaliações abrangentes de riscos dos ecossistemas de APIs, com ênfase em práticas de desenvolvimento seguro, mecanismos de autenticação avançados e capacidade de identificação de ameaças em tempo real. A rápida adoção de ferramentas SaaS orientadas por IA, muitas vezes integradas por APIs, expandiu significativamente a superfície de ataque, levando os reguladores a exigir abordagens de segurança mais sofisticadas.

À medida que a complexidade dos ambientes de APIs aumenta, especialmente com o avanço da IA e das aplicações de machine learning, os requisitos de conformidade precisam se adaptar para minimizar os riscos relacionados a violação de dados, acessos não autorizados e interrupções de serviço. Embora regiões como APJ, LATAM e EMEA estejam desenvolvendo suas próprias normas específicas, a tendência global é a harmonização dos padrões de segurança de APIs para lidar com a natureza interconectada da arquitetura digital moderna.

Perspectiva para a região APJ

Esta região está passando por uma transformação significativa em seu cenário regulatório, com novos requisitos de conformidade impactando organizações em diversos setores. Em Singapura, as recentes mudanças na legislação de cibersegurança ampliaram o escopo para abranger sistemas críticos de infraestrutura de informação tanto físicos quanto virtuais, incluindo aqueles hospedados em plataformas de nuvem e localizados no exterior. O Japão atualizou as leis do National Center of Incident Readiness and Strategy for Cybersecurity (Centro Nacional de Prontidão para Incidentes e Estratégia de Cibersegurança) enquanto a Índia modernizou sua lei de TI, com a aprovação da Digital Personal Data Protection Bill (Projeto de Lei de Proteção de Dados Pessoais Digitais). A Austrália lançou sua Estratégia de Segurança Cibernética 2023–2030, reforçando o compromisso da região com o fortalecimento das medidas de cibersegurança. Como parte dessa estratégia, no final de 2024 foram realizadas alterações na Australian Security of Critical Infrastructure Act (Lei de Segurança de Infraestrutura Crítica da Austrália) e uma nova Cyber Security Act 2024 (Lei de Cibersegurança de 2024) entrou em vigor. Sua imposição agora abrange também ativos secundários, como dispositivos de Internet das coisas, aplicações e APIs que processam dados confidenciais. Essas novas regulamentações incentivam as organizações a revisarem e aperfeiçoarem suas práticas de segurança para aplicações web, com foco especial na proteção de infraestruturas críticas e dados confidenciais.

O PCI DSS v4.0.1 impacta de maneira significativa as organizações que lidam com dados de cartões de pagamento. O prazo de conformidade estipulado foi 31 de março de 2025. Essa nova versão estabelece exigências mais rígidas para aplicações web, incluindo a adoção de controles para todos os scripts das páginas de pagamento que operam nos navegadores dos clientes, além da implementação de soluções técnicas automatizadas para detectar e prevenir continuamente ataques baseados na web. As organizações na região APJ precisam agora conduzir análises completas de lacunas, atualizar suas políticas de segurança e implementar ajustes técnicos essenciais para atender aos padrões reforçados de proteção para aplicações web.

No contexto das APIs, a região APJ vem registrando um foco crescente na segurança dessas interfaces, impulsionado, em parte, pela adoção gradual de iniciativas de open banking. Embora a região ainda não tenha adotado integralmente as normas de open banking no nível da EMEA, os países têm a oportunidade de abordar de maneira proativa as preocupações relacionadas à segurança de APIs. Uma pesquisa realizada em agosto de 2024 sobre segurança de APIs na região destacou que as APIs internas são as mais utilizadas, enquanto o acesso de usuários externos continua sendo a principal preocupação no controle de acesso a elas. Esses dados evidenciam a necessidade de as organizações implementarem medidas robustas de segurança de APIs, incluindo protocolos avançados de autenticação e autorização, criptografia de dados e mecanismos de detecção e monitoramento contínuos. À medida que a região avança em direção às diretrizes de open banking, será preciso que as organizações priorizem a segurança de APIs para garantir a conformidade com normas em evolução e se proteger contra ameaças emergentes.

Perspectiva para a região EMEA

O cenário da cibersegurança na EMEA está passando por uma transformação significativa, impulsionada por uma complexa interação de tensões geopolíticas, avanços tecnológicos e mudanças regulatórias. A região enfrenta desafios únicos, com conflitos contínuos na Ucrânia e no Oriente Médio que intensificam ciberameaças e ataques patrocinados pelo estado. Além disso, a ascensão do hacktivismo, particularmente de grupos pró-russos que visam países europeus, fez da região um foco primordial para operações cibernéticas politicamente motivadas.

O cenário de APIs na EMEA está enfrentando desafios semelhantes. As APIs se tornaram alvos estratégicos para cibercriminosos devido à sua importância na viabilização de serviços de integração e na troca de dados. Além disso, a rápida adoção de ferramentas SaaS orientadas por IA, frequentemente integradas por APIs, ampliou consideravelmente a superfície de ataque.

Como resposta a essas ameaças em expansão, a União Europeia implementou um conjunto abrangente de normas de cibersegurança. A versão atualizada da Diretiva NIS2 (Network and Information Systems) (Diretiva de Sistemas de Rede e Informações), em vigor desde janeiro de 2025, ampliou significativamente seu escopo para incluir 18 setores críticos e impôs exigências rigorosas de cibersegurança para entidades de médio e grande porte.

Para o setor financeiro, a DORA (Digital Operational Resilience Act) (Lei de Resiliência Operacional Digital), em vigor desde 17 de janeiro de 2025, substitui a NIS2, exigindo estruturas robustas de gerenciamento de riscos de tecnologia da informação e comunicação, mecanismos para comunicação de incidentes e programas de testes de resiliência operacional digital para aplicações utilizadas em serviços financeiros. Além disso, o PCI DSS v4.0.1, que se tornou obrigatório em 31 de março de 2025, introduz novos requisitos de conformidade, centrados nas crescentes necessidades de segurança, processos de segurança contínuos, metodologias flexíveis e procedimentos de validação aprimorados. A futura revisão da PSD3 (EU Payment Services Directive) (Diretiva Relativa a Serviços de Pagamento da UE) tem por objetivo resolver as deficiências da PSD2 ao endurecer os mecanismos de compartilhamento de dados, os requisitos de segurança e aprimorar a supervisão no setor dos serviços financeiros.

A Cyber Resilience Act, ou CRA (Lei de resiliência Cibernética), que entrou em vigor em 10 de dezembro de 2024, introduz padrões de cibersegurança obrigatórios para produtos com elementos digitais comercializados na União Europeia, exigindo que os fabricantes implementem medidas de segurança durante todo o ciclo de vida de produtos conectados. Para desenvolvedores e usuários de aplicações, a CRA abrange smartphones e tablets como vetores de riscos significativos. Essa inclusão exige que as organizações tratem os terminais móveis como componentes fundamentais de sua estratégia geral de cibersegurança e implementem medidas de segurança rigorosas ao longo do ciclo de vida da aplicação.

No Reino Unido, a futura Cyber Security and Resilience Bill (Projeto de Lei de Cibersegurança e Resiliência) fortalecerá as defesas cibernéticas do país e a proteção dos serviços públicos essenciais. As atualizações essenciais propostas pelo projeto de lei sobre cibersegurança ampliarão o escopo para proteger mais serviços digitais e cadeias de fornecimento, fortalecer a fiscalização e aumentar as exigências de geração de relatórios.

Perspectiva para a região LATAM

O cenário de cibersegurança da LATAM está evoluindo rapidamente, tendo em vista tanto as tendências tecnológicas globais quanto os desafios econômicos e políticos exclusivos da região. Nesse contexto, a rápida transformação digital em todos os países da LATAM, em conjunto com as vulnerabilidades de sistemas cada vez mais interconectados, tornou a região um alvo atraente para cibercriminosos e indivíduos patrocinados pelo estado. Os setores de comércio e serviços financeiros surgiram como alvos principais para ataques cibernéticos. Varejistas do comércio eletrônico, processadores de pagamentos, instituições financeiras, seguradoras, startups de fintech e plataformas de criptomoedas estão especialmente vulneráveis a ameaças que visam sua infraestrutura digital, em particular suas aplicações web e APIs.

Os países da LATAM estão cada vez mais atentos a esses desafios e avançam significativamente na criação e aplicação de normas específicas, com ênfase na proteção de aplicações web e APIs. O Brasil tem se destacado nesse cenário ao adotar a LGPD (Lei Geral de Proteção de Dados Pessoais), que entrou em vigor com rigorosos requisitos de proteção e segurança de dados. Embora não aborde diretamente a segurança de aplicações web ou APIs, a LGPD tem incentivado as organizações a fortalecerem sua postura de cibersegurança, incluindo a proteção de suas interfaces digitais.

Da mesma forma, o Chile promulgou seu Marco de Cibersegurança, que entrou em vigor em 1º de janeiro de 2025. Essa lei estabelece a Agência Nacional de Cibersegurança e descreve medidas abrangentes para prevenir, relatar e resolver incidentes de cibersegurança em vários setores, incluindo aqueles fortemente dependentes de aplicações web e APIs. Em janeiro de 2025 a Argentina publicou o Plano Federal para a Prevenção de Cibercrime e Gerenciamento Estratégico de Cibersegurança (2025–2027).

Há desenvolvimentos promissores no âmbito de regulamentações específicas para APIs. O México, por exemplo, adotou legislações voltadas para o setor financeiro, incluindo fintechs, com as quais estabelece requisitos rigorosos para que serviços de proteção ao crédito e câmaras de compensação desenvolvam APIs seguras. Essa iniciativa demonstra um reconhecimento crescente da importância das APIs nos ecossistemas digitais contemporâneos e reforça a necessidade de medidas de segurança específicas. Além disso, a Lei Federal de Proteção aos Dados Pessoais Mantidos por Indivíduos no México regula o tratamento de informações pessoais, impondo obrigações às empresas e organizações para garantir a segurança dos dados.

A Colômbia tem avançado igualmente em sua estrutura regulatória, expandindo seu escopo legal ao lançar políticas públicas sobre cibersegurança para instituições públicas e criando um sistema de gerenciamento de riscos de segurança digital com diferentes níveis de relatórios de resposta a incidentes. Embora não se concentre exclusivamente em APIs, essas medidas inevitavelmente afetarão as práticas de segurança relacionadas a elas nas organizações.

Em toda a América Latina, cresce a adesão de iniciativas setoriais, por exemplo, estruturas de finanças abertas, que estabelecem padrões de segurança de APIs voltados à proteção dos dados dos clientes. Essas normas ganham mais importância principalmente no setor financeiro, em que a segurança das APIs desempenha um papel fundamental na preservação da integridade das transações e na proteção de informações confidenciais dos clientes. À medida que os países latino-americanos continuam priorizando os avanços de segurança e alinhando suas normas de cibersegurança aos padrões internacionais, podemos esperar que diretrizes mais abrangentes e específicas surjam para aplicações web e segurança de APIs.

Mitigação

Em um cenário de ameaças crescentes com técnicas de ataque mais sofisticadas em ascensão, a proteção de aplicações web e APIs representa um desafio essencial para as organizações. Algumas das técnicas de salvaguarda e mitigação que recomendamos são:

- **Estabelecer um plano de segurança de APIs abrangente:** adote uma abordagem uma abordagem shift-left e de DevSecOps, garantindo que a segurança seja integrada desde a concepção do projeto de API até a fase de pós-produção. Garanta a descoberta e a visibilidade contínuas para conhecer toda a superfície de ataque, incluindo APIs ocultas (APIs sombra, herdadas e zumbis). Fortaleça a segurança com medidas avançadas de autenticação e autorização. Utilize padrões rigorosos, como OAuth 2,0, MTLS, controle de acesso baseado em função (RBAC) ou atributo (ABAC); implemente a limitação de taxa e mitigação de bots para evitar violações. Implemente monitoramento e proteção em tempo real: detecção de ameaças, monitoramento de anomalias e medidas de segurança de tempo de execução para identificar e bloquear ataques à medida que ocorrerem. Garanta a conformidade com normas como DORA, GDPR, HIPAA, NIS2 e PCI DSS e estabeleça políticas de governança de APIs para garantir segurança em escala.
- **Implementar medidas robustas de cibersegurança:** adote um mecanismo de segurança adaptável que monitore o ambiente digital e responda às ameaças continuamente em tempo real, além de fornecer inteligência avançada contra ameaças e proteção de tempo de execução. Além disso, utilize ferramentas de testes de APIs, como o DAST (teste dinâmico de segurança de aplicações), para ajudar a garantir que os requisitos de segurança fundamentais, como acesso seguro, criptografia e autenticação, sejam devidamente atendidos.
- **Adotar uma defesa proativa contra ameaças:** implemente ferramentas especializadas de proteção contra ataques DDoS, configure a limitação de taxa e otimize o armazenamento em cache via CDN (Rede de Entrega de Conteúdo). Além disso, adote práticas de gerenciamento de patches, políticas rigorosas de controle de acesso e segmentação de rede. Proteja também a infraestrutura do DNS (Sistema de Nomes de Domínio) com monitoramento contínuo de tráfego e plataformas híbridas.
- **Mitigar vulnerabilidades de APIs:** siga as diretrizes de segurança recomendadas, como as fornecidas pelo OWASP, para fortalecer a segurança de APIs e mitigar riscos decorrentes de práticas de codificação inadequadas e configurações incorretas na arquitetura. Essas falhas podem gerar vulnerabilidades exploráveis, facilitando o acesso não autorizado ou a manipulação de dados por agentes mal-intencionados.

- **Implementar defesa contra ameaças de ransomware:** use uma abordagem em camadas para combater ransomware. Implemente soluções Zero Trust para bloquear tráfego mal-intencionado, use microssegmentação para ter visibilidade detalhada e controle de acesso preciso e aproveite a estrutura MITRE ATT&CK para entender os padrões de ataque e melhorar as estratégias de resposta.
- **Preparar-se para IA:** utilize uma estratégia de defesa abrangente que inclua soluções de defesa contra bots, ferramentas de segurança com tecnologia de IA, firewalls especializados e medidas proativas, como avaliações contínuas e modelos Zero Trust, para lidar com novos riscos de segurança introduzidos pelo uso crescente da IA. Proteja os sistemas de IA com uma abordagem multifacetada: mitigue ameaças específicas, como injeção de prompt e envenenamento de dados, por meio de conscientização sobre modelos e conjuntos de dados; realize testes proativos de vulnerabilidades e adote defesas avançadas, como monitoramento comportamental, validação de conteúdo e respostas automatizadas a ataques, integradas tanto no ambiente de desenvolvimento quanto de tempo de execução.

Metodologia

Ataques de DDoS contra aplicações web e da camada 7

Esses dados descrevem alertas da camada de aplicação sobre o tráfego observado por meio do nosso WAF (firewall de aplicações web). Os alertas de ataques a aplicações web são acionados quando detectamos uma carga útil mal-intencionada em uma solicitação enviada a websites, aplicações ou APIs protegidos. Os alertas de DDoS de camada 7 são acionados quando detectamos anomalias volumétricas no número de solicitações enviadas a websites, aplicações ou APIs protegidos. Esses alertas podem ser acionados por solicitações mal-intencionadas e benignas. Normalmente, as solicitações são benignas, mas o alto volume de solicitações indica más intenções. Os alertas não indicam o êxito de um ataque. Embora esses produtos permitam um alto nível de personalização, coletamos os dados apresentados aqui de uma forma que não considera as configurações personalizadas das propriedades protegidas.

Os dados foram extraídos de uma ferramenta interna para análise de eventos de segurança detectados na Akamai Cloud, uma rede de aproximadamente 340 mil servidores, mais de 4 mil locais e quase 1.300 redes em mais de 130 países. Nossas equipes de segurança usam esses dados, medidos em petabytes por mês, para pesquisar ataques, sinalizar comportamentos mal-intencionados e fornecer inteligência adicional às soluções da Akamai.

Esses dados cobriram um período de 24 meses de 1º de janeiro de 2023 a 31 de dezembro de 2024.

Dados sobre ataques à segurança de APIs

A integração da Akamai com a Noname Security aprimorou significativamente nossos recursos de pesquisa e geração de relatórios sobre ameaças a APIs. Atualmente, esse conjunto de dados está nos estágios iniciais de integração e análise. Para este relatório, utilizamos uma amostra de dados de 30 dias do primeiro trimestre de 2025 para analisar a distribuição de alertas de segurança de APIs com base em suas estruturas de proteção e nos padrões de conformidade correspondentes. Esse conjunto de dados continuará evoluindo e proporcionará uma visão mais abrangente dos desafios de segurança de APIs no futuro.

Créditos

Diretor de pesquisa

Mitch Mayne

Editorial e redação

Charlotte Pelliccia
Lance Rhodes
Badette Tribbey
Maria Vlasak

Análise e contribuição sobre o tema

Tom Emmons
Reuben Koh
Richard Meeus
Stas Neyman
Steve Winterfeld

Análise de dados

Chelsea Tuttle

Materiais promocionais

Barney Beal
Ashley Linares

Marketing e publicação

Georgina Morales Hampe
Emily Spinks

State of the Internet/Segurança

Leia as edições anteriores e fique por dentro das próximas versões dos aclamados relatórios State of the Internet/Security da Akamai. akamai.com/soti/

Pesquisa sobre ameaças da Akamai

Mantenha-se em dia com as mais recentes análises de inteligência de ameaças, relatórios de segurança e pesquisas sobre cibersegurança. akamai.com/security-research

Acesse os dados deste relatório

Visualize versões em alta qualidade das tabelas e dos gráficos mencionados neste relatório. Essas imagens podem ser usadas e consultadas livremente, desde que a Akamai seja devidamente creditada como a fonte e que o logotipo da Akamai seja mantido. akamai.com/sotidata

Pesquisa sobre segurança da Akamai

Leia o blog de pesquisas sobre segurança da Akamai para obter uma perspectiva rápida sobre as pesquisas mais importantes da atualidade. akamai.com/blog/security-research