Akamai

State of the Internet

Os altos riscos da inovação

Tendências de ataque em serviços financeiros

Em uma era caraterizada por uma transformação digital sem precedentes, o setor de serviços financeiros está no centro da inovação e do risco. À medida que a tecnologia reformula o cenário das transações financeiras, ela também traz uma nova era de ameaças que visam o cerne da estabilidade econômica.

Ataques contra serviços financeiros e seus clientes

9 bilhões

Número de ataques a aplicações da Web e APIs de serviços financeiros

Número 1

Os serviços financeiros são o vertical mais atacado por DDoS, superando até mesmo o setor de jogos

50,6%

Os serviços financeiros tiveram o maior número de vítimas de ataques de phishing no 2º trimestre de 2023

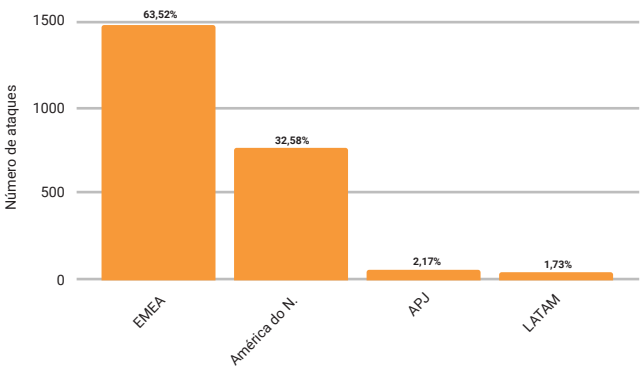
Mais de 1 trilhão

Número de solicitações de bots mal-intencionados

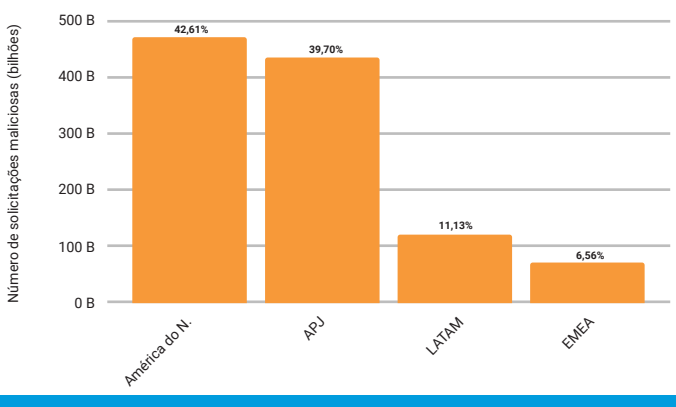
Cenários regionais

O número de ataques de DDoS de Camada 3 e Camada 4 na Europa, no Oriente Médio e na África (EMEA) é quase o dobro da América do Norte

Ataques de DDoS por região: serviços financeiros
1º de janeiro de 2022 a 30 de junho de 2023



Solicitações de bots maliciosos por região: serviços financeiros
1º de janeiro de 2022 a 30 de junho de 2023



Ásia-Pacífico e Japão (APJ) é a segunda região mais visada por solicitações de bots mal-intencionados

Possíveis riscos de segurança a serem monitorados

APIs de sombra

APIs não documentadas e não rastreadas podem representar problemas de monitoramento para empresas que não estão cientes de quem está usando essas APIs e de que maneira.

Scripts de terceiros

Os invasores podem explorar as vulnerabilidades do lado do cliente ou injetar código mal-intencionado em scripts de terceiros que são carregados como parte do website. Isso coloca os serviços financeiros em risco de Web skimming, o que pode fazer com que os dados dos clientes sejam roubados ou usados em transações não autorizadas.

Agregadores financeiros

As brechas de segurança entre os agregadores financeiros e a forma como os dados são coletados podem criar um novo caminho de exploração para os invasores, levando ao roubo de identidade.

Recomendações de segurança e práticas recomendadas

- Entenda sua superfície de ataque para desenvolver estratégias de mitigação e estabelecer controles de segurança
- Implante ferramentas de segurança de APIs para detectar e monitorar APIs não autorizadas
- Use a lista OWASP API Security Top 10 e a estrutura MITRE ATT&CK para desenvolver planos de treinamento e teste para sua equipe vermelha e grupos de teste de penetração
- Use uma estratégia de defesa multicamada que inclua a execução de auditorias de segurança regulares e a implementação de detecção e mitigação avançadas
- Use soluções como o Client-Side Protection & Compliance (antigo Page Integrity Manager) para mitigar os riscos causados por ataques do lado do cliente
- Crie um modelo de governança baseado na edge para fornecer visibilidade do tráfego de bots/APIs
- Realize um exercício em tempo real se você não tiver sofrido um ataque de DDoS nos últimos três trimestres; valide seus manuais e acompanhe as tendências de tamanho e velocidade para avaliar seu risco com base nos recursos atuais

Para obter mais informações e insights de tendências de ataque no setor de serviços financeiros, leia nosso relatório completo.

Baixar o relatório