O cenário da segurança de apps e APIs em 2025

Como a IA está mudando o panorama digital

À medida que as organizações continuam investindo em aplicações com tecnologia de IA, o que acarreta novas vulnerabilidades, os agentes de ameaça estão usando a IA simultaneamente para automatizar toda a cadeia de destruição. O resultado é um aumento no volume e na sofisticação dos ataques a aplicações web e APIs.

Seis maneiras pelas quais a IA está ajudando os invasores

- Malware aprimorado por IA
- Verificação de vulnerabilidades impulsionada por IA
- Ataques a aplicações baseadas em LLMs (injeção de prompt, envenenamento de dados, técnicas de jailbreak)
- Técnicas sofisticadas de web scraping
- Ataques automatizados de negação de serviço distribuída (DDoS)
- Ataques limitados e lentos

Ataques na web

33%

de aumento em ataques globais na web ano após ano

⚠ Impacto

A IA está impulsionando a onda de ataques

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.

Tendências de ataques na web por setor

Mais de 230 bilhões

de ataques na web

O comércio foi o setor mais afetado por ataques na web, tendo sofrido quase o triplo do número de ataques do segundo setor mais afetado (alta tecnologia).

Ataques a APIs

32%

de aumento em incidentes relacionados ao OWASP API Security Top 10*

⚠ Impacto

APIs com tecnologia de IA são menos seguras

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.

30%

de aumento em alertas de segurança relacionados à estrutura de segurança MITRE*

⚠ Impacto

A estrutura MITRE permanece crucial para fornecer insights sobre técnicas de invasores que visam APIs

À medida que os invasores usam a automação e IA para explorar APIs, a estrutura MITRE pode ajudar os defensores a identificar esses ataques de forma mais rápida e precisa.

Ataques de DDoS da camada 7

94%

de aumento em ataques mensais de DDoS da camada 7

⚠ Impacto

Os ataques estão ficando mais sofisticados e fortes

Os ataques de DDoS da camada 7 explodiram com o aperfeiçoamento de técnicas de ataque para explorar vulnerabilidades específicas em APIs ou na lógica de aplicações web. Enquanto isso, os padrões de tráfego de ataques orientados por bots cada vez mais sofisticados simulam o uso legítimo de APIs.

Tendências de ataques de DDoS da camada 7 por setor

7 trilhões

O número de ataques de DDoS da camada 7 direcionados ao setor de alta tecnologia entre janeiro de 2023 e dezembro de 2024, tornando-o o setor mais impactado.

Estratégias de mitigação

- Empregar planos shift-left e DevSecOps de segurança de APIs
- Usar mecanismos de segurança adaptáveis
- Aplicar ferramentas de teste de APIs
- Implementar diretrizes de segurança do OWASP
- Desenvolver proteções especializadas contra DDoS
- Monitorar estruturas de segurança
- Empregar defesas de ransomware em camadas
- Usar soluções de defesa contra bots e firewalls impulsionados por IA

*Durante um período de 30 dias

Obtenha o relatório completo para insights exclusivos sobre tendências de ataque.

Baixe o relatório