Ameaças de API aumentam para 40.000 incidentes no 1º semestre de 2025

Data: 2025-09-16 10:45:00

Autor: Inteligência Against Invaders

Os setores de serviços financeiros, telecomunicações e viagens estavam na mira dos agentes de ameaças no primeiro semestre do ano, depois que a Thales observou 40.000 incidentes apenas no período.

O negócio Imperva da empresa analisou dados de mais de 4000 ambientes em todo o mundo para produzir seu *Relatório de ameaças da API (H1 2025).*

O relatório afirmou que as APIs agora atraem 44% do tráfego avançado de bots, que é gerado por software sofisticado projetado para imitar o comportamento humano.

Entre as principais conclusões do relatório estão:

- Um aumento de 40% no preenchimento de credenciais e tentativas de controle de contas direcionadas a APIs sem autenticação multifator adaptável (MFA)
- A raspagem de dados foi responsável por quase um terço (31%) da atividade de bots de API
- Fraudes de cupons e pagamentos foram responsáveis por 26% dos ataques de API
- As tentativas de execução remota de código (RCE) representaram 13%
- Log4j, Oracle WebLogic e Joomla foram os produtos mais visados

“As APIs são o tecido conjuntivo da economia digital – mas isso também as torna sua superfície de ataque mais atraente”, disse Tim Chang, vice-presidente de produtos de segurança de aplicativos da Thales.

“O que estamos testemunhando não é apenas o aumento da escala de ataques, mas uma mudança fundamental na forma como os criminosos operam: eles não precisam injetar malware, eles podem simplesmente dobrar sua lógica de negócios contra você. Os pedidos parecem legítimos, mas o impacto pode ser devastador.”

Leia mais sobre ameaças de API: 99% das organizações relatam problemas de segurança relacionados a APIs

Os serviços financeiros representaram 27% dos incidentes de API no período, seguidos por telecomunicações e ISPs (10%), viagens (14%) e entretenimento e artes (13%), observou o relatório.

As APIs de sombra ainda são um grande ponto cego de segurança, com as organizações normalmente tendo de 10 a 20% mais APIs ativas do que pensam.

A Thales também relatou um grande ataque DDoS na camada de aplicação no primeiro semestre do ano, com um recorde de 15 milhões de solicitações por segundo (RPS).

O relatório afirmou que 27% do tráfego DDoS focado em API no período foi direcionado a alvos de serviços financeiros, uma vez que eles dependem fortemente de APIs para transações em tempo real, como verificações de saldo, transferências e autorizações de pagamento.

Chang alertou que o volume e a sofisticação dos ataques de API continuariam a aumentar nos próximos seis meses, com 2025 a caminho de 80.000+ incidentes.

“O melhor momento para agir foi ontem – o próximo melhor momento é agora”, concluiu.

“As organizações devem descobrir cada endpoint ativo, entender seu valor comercial e protegê-lo com defesas adaptáveis e sensíveis ao contexto se quiserem proteger a receita, a confiança e a conformidade.”