
PODCAST
bits
FABIOXAVIER
tecnologia • segurança
inovação • privacidade
O Fim de uma Era na Cibersegurança
A era da defesa manual acabou. A democratização do cibercrime e a Inteligência Artificial mudaram permanentemente as regras do jogo para 2026.
Deslize para ler mais →
fabioxavier.com.br

FABIOXAVIER
tecnologia • segurança
inovação • privacidade

PODCAST bits

O Movimento de Pinça Global

Estamos testemunhando um ataque duplo sem precedentes contra a infraestrutura digital:

Força Bruta

29.7 Tbps

Um renascimento violento dos ataques DDoS de rede, impulsionado pela Botnet Aisuru. Um aumento global de 168,2% em 2025.

Precisão Cirúrgica

+101,4%

Um salto alarmante em ataques Web DDoS criptografados e focados na camada de aplicação.

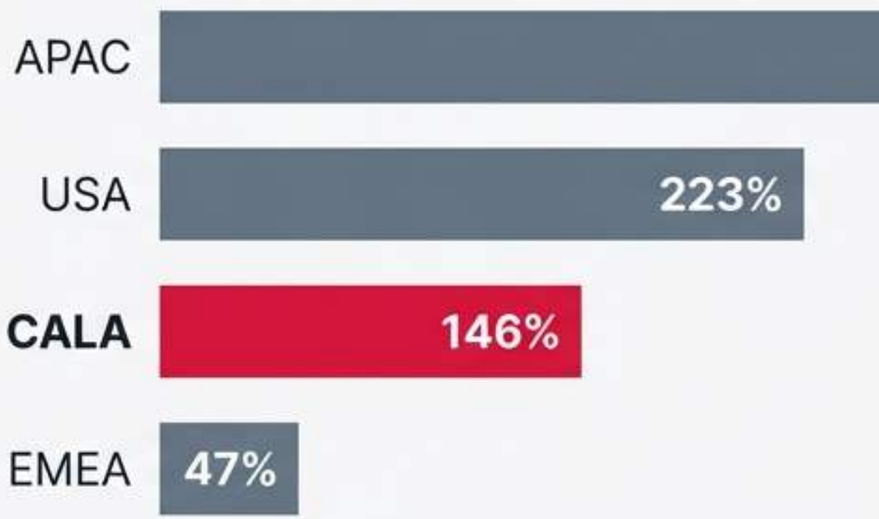
Ataques em massa não são mais eventos raros. Eles são o novo normal.

FABIOXAVIER
tecnologia • segurança
inovação • privacidade

PODCAST bits

A Tempestade na América Latina

A América Latina (CALA) não é apenas uma espectadora; tornou-se um alvo prioritário.



146%

Houve uma mudança clara de foco: os cibercriminosos abandonaram os ataques de rede comoditizados na região para focar em vulnerabilidades de APIs e na lógica de negócios das empresas latino-americanas.

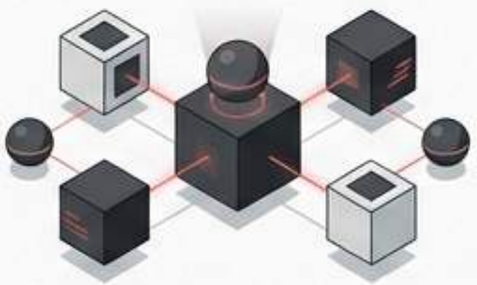
FABIOXAVIER
tecnologia • segurança
inovação • privacidade

PODCAST bits

A Invasão dos ‘Bad Bots’ no Brasil e LATAM

A automação é o principal multiplicador de força do cibercrime moderno.

15,2% de todos os ataques globais de Bad Bots agora miram a América Latina (acima dos 13,4% do ano anterior).



As transações de bots maliciosos quase dobraram globalmente (+91,8%). Ecossistemas coordenados estão realizando operações de scraping em larga escala e roubo de contas de forma totalmente automatizada.

FABIOXAVIER
tecnologia • segurança
inovação • privacidade

PODCAST bits

O Problema dos 5 Minutos

Seu tempo de resposta é irrelevante seo ataque termina antes de você perceber.

A maioria dos ataques volumétricos recordes agora dura menos de 5 minutos, e os maiores ataques Web DDoS terminam em menos de 60 segundos.

Essas campanhas orquestradas por algoritmos alternam rapidamente entre múltiplos vetores, tornando obsoletos os runbooks manuais e qualquer intervenção humana.

A mitigação precisa ocorrer na borda, em tempo real.

O Dilema da Identidade da Inteligência Artificial

A rápida adoção de agentes de IA fraturou nossos modelos de confiança digital.

Para funcionarem, os agentes 'bons' precisam de permissões de requisição POST (como fazer reservas ou compras). O problema?

Botnets maliciosos agora falsificam identidades de agentes de IA que não possuem padrões de verificação robustos (disfarçando-se de Anthropic ou xAI, por exemplo) para contornar mitigações tradicionais.

A sua segurança consegue distinguir um bot legítimo do ChatGPT de um ataque cibernético disfarçado?

FABIOXAVIER
tecnologia • segurança
inovação • privacidade

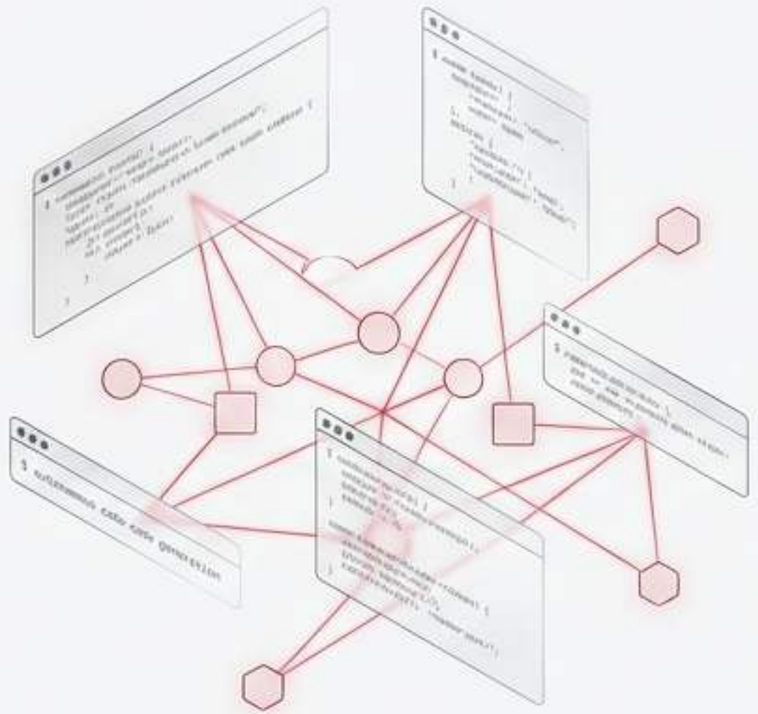
PODCAST bits

A Ameaça Invisível e o 'Vibe Hacking'

A IA generativa rebaixou a barreira de entrada para o cibercrime. Hackers com pouco conhecimento técnico agora usam linguagem natural para orquestrar campanhas complexas em horas.

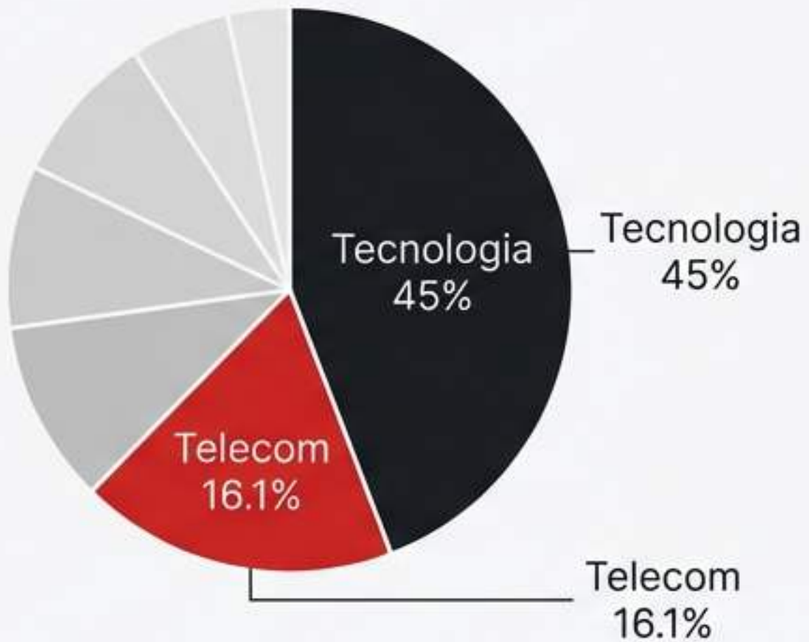
Pior ainda: as empresas agora enfrentam o ZombieAgent.

Ataques de injeção indireta de prompt (IPI) "zero-click" conseguem inserir lógicas maliciosas na memória de longo prazo de assistentes de IA corporativos, transformando-os em ameaças internas persistentes e silenciosas.



O Alvo Mudou: Tecnologia e Telecomunicações

Historicamente, o setor financeiro era o alvo principal. Em 2025, houve uma inversão brutal.



Por quê? Os atacantes buscam danos em cascata. Ao atingir provedores de nuvem e infraestrutura crítica de internet, eles derrubam milhares de clientes secundários simultaneamente.

A Nova Postura de Defesa para 2026

Para sobreviver nesta nova realidade de guerra algorítmica, as organizações devem abandonar processos manuais e adotar arquiteturas de autodefesa baseadas em 3 pilares:

1. Automação

Detecção e mitigação em tempo real, sem intervenção humana, para combater ataques na velocidade da máquina.

2. Escala Massiva

Arquiteturas de borda capazes de absorver inundações de classe Terabit.

3. Inteligência Integrada

Análise comportamental sofisticada para distinguir usuários legítimos de agentes de IA maliciosos e bad bots.

FABIOXAVIER
tecnologia • segurança
inovação • privacidade

PODCAST bits

As Regras do Jogo Mudaram.

Os atacantes já fizeram a transição para operações de larga escala guiadas por IA. Sua empresa está preparada para a Internet dos Agentes?

Descubra como proteger sua infraestrutura. Leia a análise completa no Radware 2026 Global Threat Analysis Report.

Acesse o link nos comentários →

Deixe sua opinião: Qual dessas tendências mais preocupa sua operação hoje?

FABIOXAVIER
tecnologia • segurança
inovação • privacidade

Cibersegurança em 2026: O Risco é Imediato

- Ataques em escala massiva
- Automação ofensiva
- IA aplicada ao cibercrime

Menor tempo de reação = Maior risco para sua infraestrutura digital, APIs, identidade e operações.

Acompanhe o BITS

Análises práticas, governança de TI e implicações para o setor público.
Siga no seu tocador favorito.

PODCAST bits

Aprofunde o Conteúdo

Acesse materiais complementares em:
fabioxavier.com.br

Fique Atualizado

Receba insights no seu feed.
Siga meu perfil:
linkedin.com/in/fabiocorreaxavier/

Leve a Discussão Adiante

Compartilhe e marque alguém de Segurança, TI ou Compliance que precisa ver isto.

fabioxavier.com.br