Brasil concentra quase metade dos ataques cibernéticos na América Latina

Category: BRASIL,GERAL,TECNOLOGIA e CIÊNCIA
escrito por Ayumi Yohanna Miyamoto | 4 de março de 2026

O Brasil lidera o ranking de ataques de negação de serviço distribuído (DDoS) na América Latina. Um relatório de inteligência de ameaças divulgado pela NETSCOUT SYSTEMS mostra que o país registrou 470.677 ataques entre julho e dezembro de 2025, número que corresponde a quase metade dos 1.014.148 incidentes identificados em toda a região no mesmo período.

O levantamento evidencia o crescimento da pressão sobre infraestruturas digitais brasileiras e reforça o papel do país no cenário regional de ameaças cibernéticas, tanto pelo tamanho da sua infraestrutura quanto pela grande quantidade de serviços conectados.

Telecomunicações são principal alvo

Entre os setores mais atingidos pelos ataques DDoS, as empresas de telecomunicações sem fio lideram a lista, com 114.797 ocorrências. Em seguida aparecem infraestruturas de computação e serviços de hospedagem, que registraram 47.897 ataques, além das operadoras de telecomunicações com fio, com 34.051 incidentes.

Outros segmentos também foram alvo frequente das ofensivas digitais, incluindo:

- Comércio atacadista de equipamentos de escritório: 6.515 ataques
- Transporte rodoviário de cargas: 6.367 ataques
- Bancos: 5.583 ataques
- Outras empresas de telecomunicações: 3.010 ataques
- Organizações religiosas: 1.210 ataques

Segundo Geraldo Guazzelli, country manager da NETSCOUT SYSTEMS no Brasil, a concentração de ataques em telecomunicações reflete a importância estratégica dessas redes para a economia digital.

“Hoje existe uma base gigantesca para gerar ataques. Já monitoramos e mitigamos um ataque de 30 terabits por segundo, muito acima dos picos registrados anteriormente. O crescimento é impulsionado pela expansão da internet das coisas e pelas conexões de alta capacidade, como 5G e acesso sem fio fixo”, explica.

Ataques cada vez mais sofisticados

O relatório também identificou os principais métodos utilizados pelos invasores. O vetor TCP lidera o ranking, com 134.320 ataques, seguido por DNS Amplification, responsável por 98.558 ocorrências.

Outras técnicas relevantes incluem:

- TCP RST – 76.980 ataques
- STUN Amplification – 65.936 ataques
- TCP SYN/ACK Amplification – 65.915 ataques

De acordo com Guazzelli, os ataques atuais costumam combinar diversos métodos simultaneamente, formando ofensivas multivetoriais, que dificultam a detecção e a defesa.

“Em um dos casos analisados, o invasor trocou de vetor 24 vezes durante o mesmo ataque. Essa alternância exige defesas automatizadas e sistemas capazes de reagir rapidamente”,

afirma.

Escalada global de ciberataques

O estudo mostra que o aumento das ameaças não é exclusivo da América Latina. Em escala global, mais de oito milhões de ataques DDoS foram registrados em 203 países e territórios no segundo semestre de 2025, alguns chegando a picos de 30 Tbps.

Entre os fatores que impulsionam essa escalada estão:

- crescimento de botnets mais resilientes
- exploração de dispositivos da Internet das Coisas (IoT) comprometidos
- expansão de serviços de DDoS sob demanda, que facilitam a realização de ataques

Outro ponto de atenção é o avanço do uso de inteligência artificial em fóruns clandestinos. O relatório aponta aumento de 219% nas menções a ferramentas maliciosas baseadas em IA, utilizadas para explorar vulnerabilidades e ampliar redes de dispositivos comprometidos.

Brasil também virou base de ataques

Além de alvo frequente, o Brasil também passou a integrar a infraestrutura usada por criminosos para lançar ataques em escala global.

Segundo Guazzelli, isso ocorre devido à expansão de provedores regionais de internet e à crescente digitalização de serviços e dispositivos conectados. “Isso não significa que os ataques partem de agentes locais, mas que equipamentos e redes no país acabam sendo recrutados por botnets internacionais”, explica.

Diante desse cenário, especialistas defendem que empresas e provedores invistam em estratégias preventivas, monitoramento contínuo e cooperação entre redes, capazes de detectar e neutralizar ataques antes que eles provoquem interrupções

graves.

“O ponto não é mais perguntar se uma organização será atacada, mas quando isso vai acontecer. A preparação operacional e tecnológica é o que define quem consegue se recuperar rapidamente e quem sofre impactos prolongados”, conclui o especialista.

Fonte: Diário do Pará e Publicado Por: Jornal Folha do Progresso 04/03/2026/14:39:52

> *O formato de distribuição de notícias do Jornal Folha do Progresso pelo celular mudou. A partir de agora, as notícias chegarão diretamente pelo formato Comunidades, ou pelo canal uma das inovações lançadas pelo WhatsApp. Não é preciso ser assinante para receber o serviço. Assim, o internauta pode ter, na palma da mão, matérias verificadas e com credibilidade. Para passar a receber as notícias do Jornal Folha do Progresso, clique nos links abaixo siga nossas redes sociais:*
>
> - **Clique aqui e nos siga no X**
> - **Clica aqui e siga nosso Instagram**
> - **Clique aqui e siga nossa página no Facebook**
> - **Clique aqui e acesse o nosso canal no WhatsApp**
> - **Clique aqui e acesse a comunidade do Jornal Folha do Progresso**
>
> *Apenas os administradores do grupo poderão mandar mensagens e saber quem são os integrantes da comunidade. Dessa forma, evitamos qualquer tipo de interação indevida. Sugestão de pauta enviar no e-mail:folhadoprogresso.jornal@gmail.com.*

Envie vídeos, fotos e sugestões de pauta para a redação do JFP (JORNAL FOLHA DO PROGRESSO) Telefones: WhatsApp (93) 98404

6835– (93) 98117 7649.

“Informação publicada é informação pública. Porém, para chegar até você, um grupo de pessoas trabalhou para isso. Seja ético. Copiou? Informe a fonte.”

Publicado por Jornal Folha do Progresso, Fone para contato 93 981177649 (Tim) WhatsApp:-93- 984046835 (Claro) -Site: www.folhadoprogresso.com.br e-mail:folhadoprogresso.jornal@gmail.com/ou e-mail: adeciopiran.blog@gmail.com