Tarifa de 50% dos EUA e Ataques Cibernéticos ao Brasil

Autores: Marcelo Branquinho & Plataforma Safer
Data: 07 de agosto de 2025

Resumo

Após a imposição de uma tarifa de 50% por Donald Trump sobre os produtos importados do Brasil, implementada em agosto de 2025 e acompanhada de críticas ao STF e ao governo brasileiro, observou-se um aumento significativo nos ataques cibernéticos ao Brasil com origem nos Estados Unidos. Relatórios da TI Safe indicam uma elevação de 30% nessas tentativas de invasão, especialmente contra infraestruturas críticas como energia, siderurgia, petróleo e órgãos governamentais, com destaque para o STF — alvo de mais de 750 milhões de tentativas de invasão recentemente. Tradicionalmente, os principais vetores desses ataques eram Rússia, China e Israel, mas o aumento vindo dos EUA rompeu esse padrão. Especialistas avaliam que essa nova ofensiva tem motivações políticas e ideológicas, caracterizando-se como uma forma de hacktivismo, impulsionada pela retórica de Trump e pela polarização internacional, especialmente em torno da figura de Bolsonaro. Ainda que não haja indícios de coordenação oficial do governo dos EUA nos ataques, o ambiente de tensão geopolítica e as declarações públicas de Trump parecem ter encorajado agentes maliciosos, hacktivistas e cibercriminosos a explorar essa conjuntura. A resposta brasileira tem sido eficaz até agora, com defesas reforçadas e cooperação internacional ativa, mas o episódio evidencia como decisões políticas internacionais podem desencadear consequências severas também no ciberespaço.

Keywords: Tarifa Trump, Ataques cibernéticos, Hacktivismo, Infraestrutura crítica, Segurança cibernética

Introdução

Em **9 de julho de 2025**, o presidente dos EUA, Donald Trump, anunciou a imposição de uma **tarifa de 50% sobre todos os produtos importados do Brasil**, alegando que a relação comercial era "injusta" e citando razões político-ideológicas para a medidacnnbrasil.com.br. Essa sobretaxa entrou em vigor no início de **agosto de 2025**, agravando as tensões entre os dois países. Trump justificou a tarifa extraordinária, em parte, como resposta à conduta do Brasil em questões internas: ele criticou duramente o **Supremo Tribunal Federal (STF)** brasileiro pelo tratamento dado ao ex-presidente Jair Bolsonaro e pelo que chamou de "ataques insidiosos" às liberdades de expressão (referindo-se a ordens do STF envolvendo **plataformas digitais americanas**)cnnbrasil.com.br. O governo brasileiro rechaçou essas acusações; o presidente Lula da Silva afirmou que Trump estava tentando *"ditar regras para um país soberano"*, qualificando a ação tarifária como uma interferência política inaceitávelreuters.comreuters.com. Em suma, a relação bilateral atingiu seu **pior momento em décadas**, criando um ambiente de **confronto diplomático** raro entre Brasil e Estados Unidos.

Essa escalada nas **tensões diplomáticas** gerou preocupação não apenas no comércio, mas também em outras esferas – inclusive na segurança cibernética. Autoridades e analistas começaram a questionar se haveria repercussões além das tarifas, dada a crescente **interdependência digital** entre os países. Vale notar que os Estados Unidos são historicamente um dos principais parceiros tecnológicos do Brasil (com ampla presença de empresas de TI americanas no mercado brasileiro), mas agora se tornaram também fonte de atrito político. Esse **choque diplomático** abriu espaço para especulações sobre possíveis **retaliações indiretas**, incluindo a ação de hackers motivados pelo clima de hostilidade.

Aumento Recente de Ataques Cibernéticos

Logo após o anúncio do *tarifaço* norte-americano, o Brasil observou um aumento significativo nas atividades de **ataque**

POWERED BY SAFER

cibernético originadas a partir dos EUA. De acordo com dados da empresa de segurança TI Safe, houve uma **alta de cerca de 30%** no número de tentativas de invasão vindas de endereços nos Estados Unidos **apenas na última semana de julho de 2025**baguete.com.br. Em outras palavras, com o Brasil **"na mira do governo americano de Donald Trump"**, registrou-se uma verdadeira ofensiva de hackers tendo como origem o território norte-americanobaguete.com.br. Esse salto abrupto coincide temporalmente com a implementação da tarifa de 50%, sugerindo uma possível **correlação temporal** entre a medida econômica e a intensificação dos ataques digitais.

Os **principais alvos** desses ataques recentes têm sido **infraestruturas críticas e instituições estratégicas** no Brasil. Setores vitais da economia e do governo foram visados. Entre eles, destacam-se:

- **Redes de energia elétrica** (empresas de fornecimento de energia)baguete.com.br
- **Siderúrgicas** (indústrias de aço e metalurgia)baguete.com.br
- **Plataformas petroquímicas** (instalações de petróleo e gás)baguete.com.br
- **Usinas** (incluindo usinas de geração de energia)baguete.com.br
- **Sistemas de saneamento** (infraestrutura de água e esgoto)baguete.com.br
- **Órgãos governamentais**, em especial o **Supremo Tribunal Federal (STF)**baguete.com.br

Esses setores são considerados de **alta criticidade** para o funcionamento do país, o que sugere que os agressores buscam causar **disrupção** ou enviar uma mensagem simbólica atingindo pontos nevrálgicos. De fato, a TI Safe relembra que diversos incidentes recentes envolvendo empresas brasileiras de energia vieram a público – por exemplo, ataques cibernéticos contra as companhias **Copel**, **Light**, **Cemig** e **EDP** foram noticiados na imprensabaguete.com.br. Esses casos evidenciam que a ameaça não é apenas teórica: atores

maliciosos têm tentado, na prática, violar sistemas reais de empresas e instituições brasileiras.

Dados e Padrões de Ciberataques: Antes e Depois

Os números reforçam a preocupação com a **onda atual de ciberataques** e permitem compará-la com padrões anteriores. Mesmo antes da crise tarifária, o **Brasil já figurava entre os países mais visados do mundo** em termos de ataques digitais. Especialistas em risco político e cibernético apontam que o Brasil é o **segundo país que mais sofre ataques cibernéticos no planeta, atrás apenas dos próprios Estados Unidos**, com estimativas em torno de **700 milhões de tentativas de ataque por ano**britcham.com.br. Isso equivale, em média, a milhares de investidas maliciosas por dia, ilustrando a escala colossal do desafio de segurança cibernética brasileiro. Em 2024 e início de 2025, observou-se uma tendência de alta nos incidentes: por exemplo, no primeiro trimestre de 2025, empresas no Brasil sofreram em média **2.600 ataques semanais**, um aumento de **21% em relação ao mesmo período do ano anterior**forbes.com.br. Regionalmente, a América Latina como um todo enfrentou um crescimento ainda maior (mais de 100% de alta no volume de ataques naquele período)forbes.com.br. Ou seja, já havia um **crescimento significativo** de ameaças cibernéticas em curso, atribuído em parte à maior atividade global de grupos hackers e à expansão das superfícies de ataque digitais.

Dentro desse panorama já preocupante, a **nova safra de ataques provenientes dos EUA** se destaca por romper com o perfil geográfico usual. Em condições normais, grande parte dos ataques cibernéticos contra alvos brasileiros se origina de redes em países como **Rússia, China e Israel**, de acordo com os registros da TI Safebaguete.com.br. Esses países frequentemente apareciam no topo das origens de tentativas de invasão, seja pela atuação de grupos hackers locais ou pela presença de servidores comprometidos usados em botnets globais. No entanto, na esteira da recente crise diplomática, houve uma **alteração notável nesse padrão**: houve um “aumento considerável partindo do solo americano”, algo não usual nessa

magnitudebaguete.com.br. Em outras palavras, **o volume de ataques com IPs de origem nos EUA cresceu desproporcionalmente** em comparação aos patamares históricos, alterando a distribuição típica das fontes de ameaça.

Para dimensionar o problema em termos concretos: **somente nos últimos três meses**, o site e os sistemas do STF – alvo simbólico na atual conjuntura – **detectaram e bloquearam cerca de 752 milhões de tentativas de invasão**baguete.com.br. Trata-se de um número impressionante de ataques impedidos. Desde o começo de 2025, a segurança do STF registrou mais de **280 mil alertas de atividades suspeitas**, incluindo tentativas repetidas de adivinhação de senhas e inserção de vírus, todas neutralizadas pelos mecanismos de defesa do Tribunalbaguete.com.br. Embora esses dados englobem ataques de origens variadas, eles exemplificam a **intensidade do assédio digital** contra instituições brasileiras. Com a recente elevação das tensões, grande parte desse tráfego malicioso adicional foi atribuída a fontes nos Estados Unidos, conforme mencionado, aumentando o **desafio de filtrar e bloquear** acessos indevidos. Muitos dos ataques observados utilizam **redes de bots ("robôs")** para disparar um volume massivo de requisições simultâneas, numa tática clássica de **negação de serviço (DDoS)** visando tirar sites e sistemas do arbaguete.com.br. Essa técnica tem sido detectada repetidamente contra órgãos governamentais brasileiros, exigindo infraestrutura robusta para absorver o fluxo malicioso.

De maneira geral, os **relatórios globais** também confirmam que as ameaças cibernéticas estão em alta em todos os continentes. O Instituto Brasileiro de Cibersegurança (IBSEC), em seu relatório anual *The State of Global Cyber Security 2025*, apontou um **crescimento de 44% no volume de ataques cibernéticos no mundo** em comparação ao ano anteriorbaguete.com.br. Novas modalidades de ataque vêm ganhando força, como o avanço de códigos maliciosos furtivos (*infostealers*), o uso de **Inteligência Artificial generativa** em campanhas de phishing e o fortalecimento do modelo de **ransomware como serviço (RaaS)**, entre outrosbaguete.com.br. Dentro desse contexto, o que o Brasil enfrenta não é isolado; contudo, a **espike de**

POWERED BY SAFER

ataques associados aos EUA na última semana de julho claramente destoa do padrão de ameaças geralmente esperado, indicando um fenômeno possivelmente ligado à conjuntura político-comercial específica entre os dois países.

Possível Relação Causal e Motivação dos Ataques

A coincidência temporal e o perfil dos alvos sugerem fortemente uma relação entre a **política tarifária americana recente e a onda de ataques cibernéticos** contra o Brasil. Embora seja difícil provar *causalidade direta* em eventos cibernéticos (dada a natureza anônima e global da internet), **fontes confiáveis indicam uma correlação notável**. O próprio levantamento da TI Safe conclui que o *"tarifaço" e o choque diplomático entre os dois países encorajaram hackers a tentar invadir infraestruturas críticas* brasileirasbrazileconomy.com.br. Em outras palavras, a medida dos EUA e a retórica hostil que a acompanhou agiram como um *gatilho motivacional* para agentes maliciosos intensificarem suas ações contra alvos no Brasil.

Especialistas em **cibersegurança** caracterizam muitos desses incidentes como casos de **"hacktivismo"** – ativismo político-ideológico realizado por meio de ataques digitais. Segundo Marcelo Branquinho, CEO da TI Safe, muitos ataques recentes são **motivados por política e ideologia**, refletindo as polarizações globais atuaisbaguete.com.br. Esse tipo de **ativismo digital** ocorre quando grupos de hackers, alinhados a certas causas ou facções, tentam derrubar ou prejudicar sistemas de entidades associadas a projetos ou decisões polêmicasbaguete.com.br. No caso em pauta, a narrativa de que o governo brasileiro (especialmente o STF) estaria "censurando" ou perseguindo figuras conservadoras – amplificada pelas declarações de Trump – pode ter servido de combustível retórico para esses grupos. **Hackers simpatizantes** da causa de Bolsonaro ou adeptos da ideologia de Trump poderiam enxergar as instituições brasileiras como *inimigas políticas*, decidindo agir por conta própria em uma espécie de **retaliação digital**. De fato, Trump publicamente classificou o julgamento de Bolsonaro como uma "caça às bruxas" e acusou o STF

de ferir liberdades de americanos nas redes sociaiscnnbrasil.com.br, o que pode ter inflamado comunidades online extremistas a “defender” esses interesses atacando sites brasileiros.

Importante salientar que, até o momento, **não há evidências de que os EUA, em nível governamental, estejam orquestrando ataques cibernéticos contra o Brasil** como forma de guerra híbrida oficial. As investidas observadas têm o *perfil de atores não-estatais*, isto é, **cibercriminosos independentes ou coletivos hacktivistas** aproveitando a conjuntura acirrada. Esses grupos podem estar agindo por iniciativa própria, sem coordenação direta de autoridades, embora possam contar com a simpatia (tácita ou explícita) de alas políticas. Em muitos casos, os ataques também podem incluir **cibercrime oportunista**, visando ganho financeiro. A TI Safe lembra que uma parcela significativa das ofensivas digitais é movida por interesses financeiros – por exemplo, **ransomware** implantado para extorsão monetáriabaguete.com.br. No meio do caos geopolítico, **gangues de ransomware** poderiam tentar explorar vulnerabilidades em empresas brasileiras, esperando que a distração ou a pressão aumentada facilite suas exigências de resgate. Portanto, a **motivação dos ataques recentes** pode ser mista: uma combinação de **retaliação política (hacktivismo)** e **oportunismo criminoso**, ambos catalisados pela deterioração das relações entre Washington e Brasília.

Do ponto de vista de **relações internacionais**, analistas avaliam que a confrontação iniciada pela tarifa criou um *ambiente propício* a esse tipo de incidente. Embora a América do Sul não fosse, a princípio, prioridade na agenda de enfrentamentos dos EUA de Trump, a decisão de **“punir” o Brasil** por questões políticas internas acabou **fragilizando a confiança mútua** e abrindo brechas para ações hostis de terceirosbr.boell.orgreuters.com. O governo brasileiro, por sua vez, optou por cautela na resposta comercial (evitando retaliações tarifárias imediatas)britcham.com.br, mas isso não impediu atores informais de promoverem *ataques sombra*. Em suma, a **disputa tarifária** funcionou como um catalisador de animosidades que **transbordaram para o ciberspaço**.

Resposta e Prevenção em Andamento

Apesar do aumento alarmante nos ataques, até agora **não há registros de danos catastróficos** ou interrupções prolongadas causadas por esses incidentes – graças, em parte, à pronta resposta das equipes de segurança cibernética brasileiras. As instituições e empresas mais visadas têm reforçado suas defesas e monitorado seus sistemas em regime de 24/7. O STF, por exemplo, conseguiu **bloquear a totalidade das tentativas de invasão detectadas em seus sistemas recentemente**baguete.com.br, preservando a continuidade de suas operações. Empresas especializadas, como a TI Safe, reportam que **nenhum dos ataques teve sucesso entre seus clientes**, dado o uso de arquiteturas de segurança em camadas, políticas rigorosas de backup e planos de contingênciabrazileconomy.com.br. Ou seja, embora a ofensiva hacker tenha aumentado, *a barreira defensiva também foi elevada* para acompanhar.

Autoridades brasileiras também têm intensificado a **cooperação internacional em segurança cibernética** e o compartilhamento de informações de ameaças, inclusive com parceiros nos Estados Unidos, para rastrear origens e responsabilizar criminosos quando possível. No âmbito doméstico, especialistas sugerem que este episódio sirva de alerta para reduzir **vulnerabilidades em sistemas críticos**. Medidas como manter **equipamentos atualizados**, reforçar a segurança de roteadores, VPNs e outros dispositivos de borda (gateway), e adotar *práticas de segurança por design* em novos sistemas são apontadas como essenciaisbaguete.com.br. Há também um movimento para **formação de mais profissionais de cibersegurança** no Brasil, visto que a demanda por especialistas cresce à medida que ataques se multiplicam. Iniciativas no setor público e privado buscam investir em **Inteligência Artificial** aplicada à detecção e resposta a incidentes, visando reagir a ameaças em segundos ou minutos, minimizando impactosbrazileconomy.com.brbrazileconomy.com.br.

Conclusão

A investigação indica que **existe, sim, uma correlação temporal clara** entre a imposição da tarifa de 50% pelos Estados Unidos e o aumento de ataques cibernéticos contra alvos brasileiros. Nas horas e dias seguintes ao anúncio da medida comercial punitiva, observou-se um **pico de investidas hacker oriundas dos EUA** – um desvio notável em relação ao padrão usual de ameaçasbaguete.com.br. Embora não se possa afirmar que haja uma relação de causalidade *comprovada* (no sentido de um plano coordenado diretamente pelo governo dos EUA), o **contexto sugere fortemente uma ligação**: o clima de animosidade e confronto desencadeado pela tarifa **"encorajou" atores maliciosos** a agirem contra o Brasilbrazileconomy.com.br. Especialistas em segurança e analistas internacionais convergem na opinião de que a motivação por trás desses ataques é **majoritariamente política e ideológica**, isto é, trata-se de **hackers engajados** – possivelmente alinhados com a retórica de Trump ou com a defesa de Bolsonaro – buscando retaliar ou pressionar o governo brasileiro no campo digitalbaguete.com.br.

Em termos de **dados**, o Brasil vinha enfrentando um volume elevado de ciberataques globalmente (segundo mais atacado do mundo), mas a crise recente adicionou um *componente inédito* ao problema: um salto específico de ofensivas partindo dos Estados Unidos, de magnitude ~30% acima do normal em um curto intervalobaguete.com.br. Essa alteração abrupta nos padrões de ataque reforça a ideia de uma **conexão circunstancial** com as tensões político-comerciais. Felizmente, até agora as defesas cibernéticas nacionais mostraram-se eficazes em conter os ataques, evitando prejuízos maioresbaguete.com.br. Não obstante, o episódio evidencia a necessidade de **vigilância redobrada**.

Em conclusão, **fontes confiáveis confirmam** uma correlação preocupante entre a tarifa de 50% imposta pelos EUA e um aumento no número de ataques cibernéticos contra o Brasil. A correlação é principalmente **temporal e motivacional**: surgiu concomitantemente ao atrito diplomático e parece ser impulsionada por fatores ideológicos

POWERED BY SAFER

(hacktivismo). Essa constatação serve de alerta tanto para os riscos indiretos de decisões de política internacional (que podem extrapolar o campo econômico e atingir a segurança digital) quanto para a importância de fortalecer continuamente a **resiliência cibernética** do Brasil. Em um mundo cada vez mais interconectado, **ações geopolíticas e ataques cibernéticos andam lado a lado** – e o caso da tarifa de Trump e dos hackers contra o Brasil é um exemplo concreto dessa nova realidadebaguete.com.brbrazileconomy.com.br.

POWERED BY SAFER

Referências Utilizadas:

- CNN Brasil – *“Trump anuncia tarifa de 50% para Brasil”* (09/07/2025)cnnbrasil.com.br.
- Reuters – *“50% US tariff on Brazilian goods taking effect...”* (06/08/2025)reuters.comreuters.com.
- Baguete – *“Ataques dos EUA ao Brasil crescem 30% em uma semana”* (01/08/2025)baguete.com.brbaguete.com.brbaguete.com.brbaguete.com.br.
- Brazil Economy – *“Ciberataques dos EUA no Brasil disparam 30% em uma semana, diz TI Safe”* (31/07/2025)brazileconomy.com.brbrazileconomy.com.brbrazileconomy.com.br.
- Exame – *“A vulnerabilidade do Brasil às big techs em meio à guerra tarifária”* (10/07/2025)britcham.com.br.
- Forbes Brasil Tech – *“Com o aumento de ataques cibernéticos, CISOs ganham espaço...”* (06/08/2025)forbes.com.br.
- IBSEC – *The State of Global Cyber Security 2025* (dados citados em Baguete)baguete.com.br.

POWERED BY SAFER