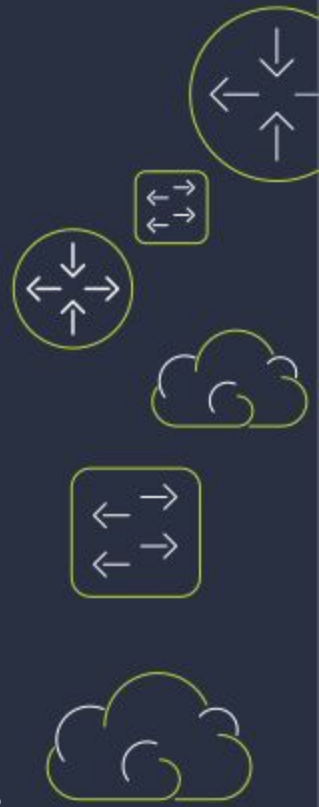
Ataques DDoS pelo IX
e suas consequências

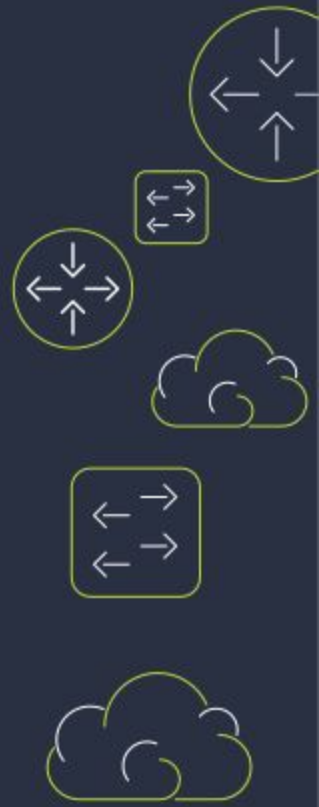


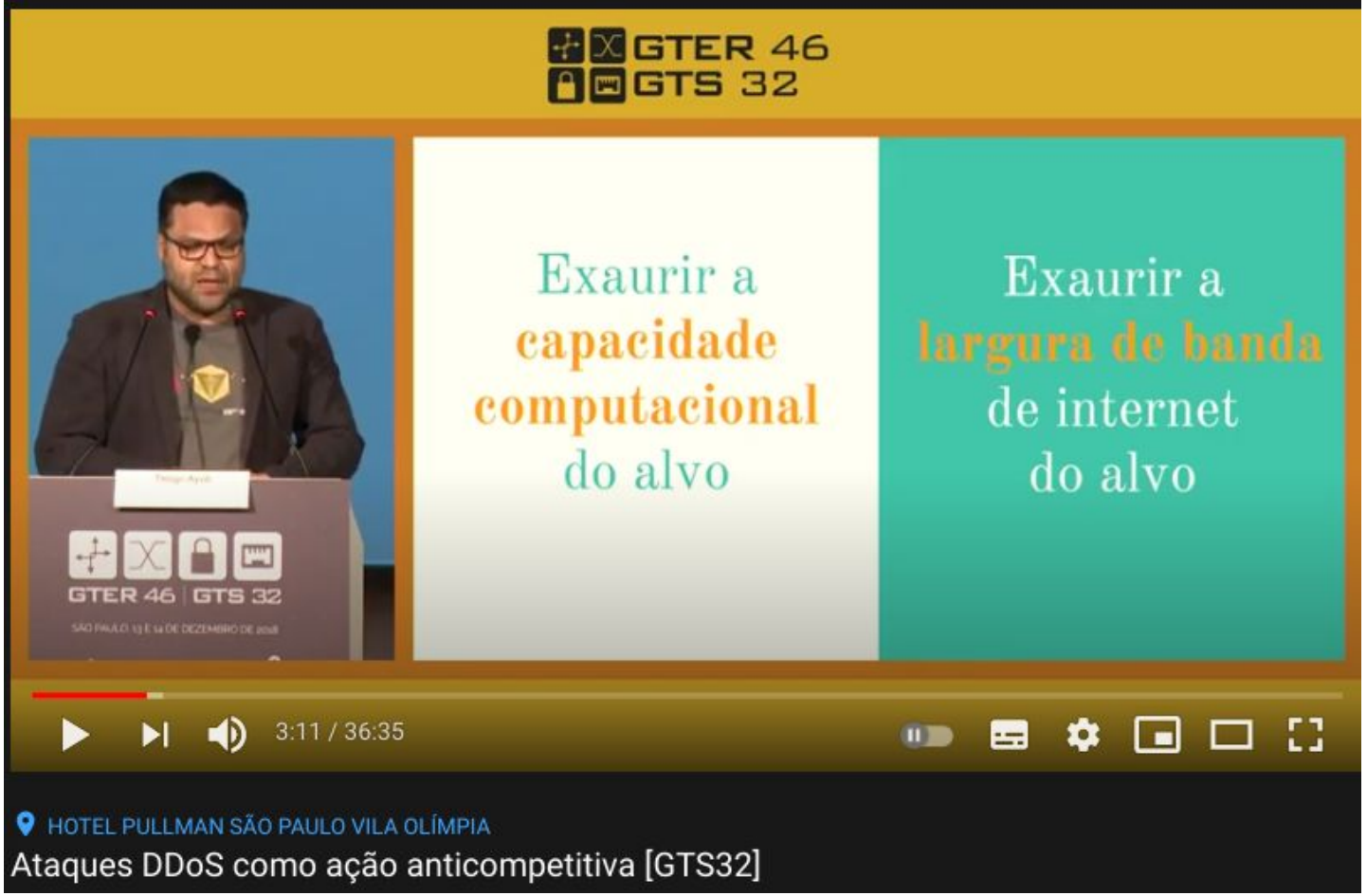
por D. Damito
Diretor de Redes

E que são ataques DDoS?

São ataques a redes dos ISPs e data centers que tem como objetivo deixá-las fora do ar ou com performance severamente degradada.

- Saturam toda a **banda** disponível com trânsitos IP e IX.
- Saturam a capacidade computacional **(CPU)** de roteadores, concentradores PPPoE e CGNAT.
- Exaurem o **recurso humano** de seu ISP, com jornadas longas de trabalho, filas elevadas no call center.



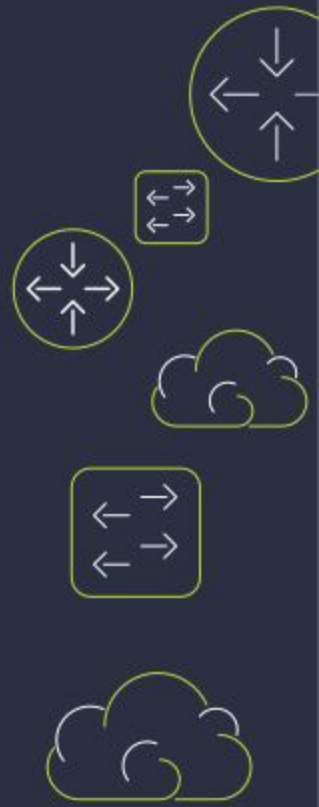


youtube.com/c/ayubio

O que a Sage Networks faz?

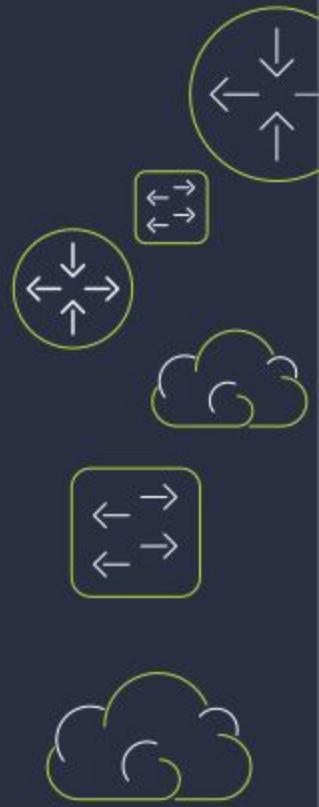
Serviços de Redes para Sistemas Autônomos e especializada em **mitigação de DDoS**.

- Implantação de sistemas de **detecção** e automação de resposta a ataques.
- **Nuvem** de mitigação por VPN, VLAN bilateral ou cross connect.
- Implantação de sistemas locais de mitigação.



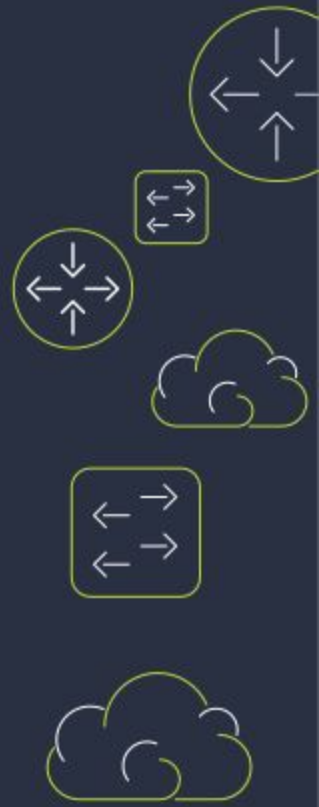
Ataques DDoS no IX SP

- De 21/04/2021 à 21/10/2021 (6 meses), registramos cerca de **1195980** episódios de ataques contra nossos clientes.
- **5%** (59799) dos ataques vieram pelo IX de São Paulo.
- Isso **não significa que o IX é inseguro.** Se você deixar de estar no IX, irá receber o ataque por outro caminho.



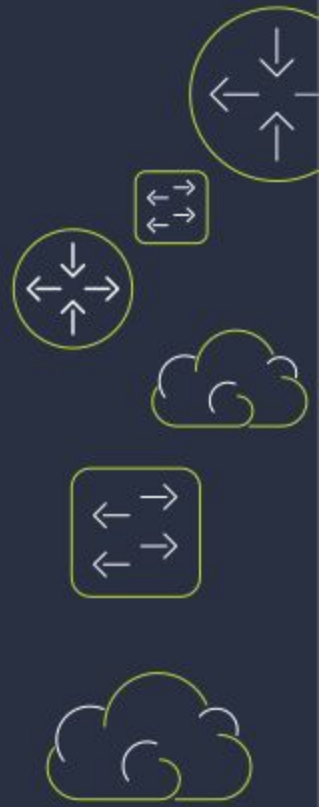
Quem são as origens de DDoS

- As **web-scales** (Google, Microsoft etc).
- Algumas **carriers** (como Claro).
- Pequenos e médios **ISPs**.



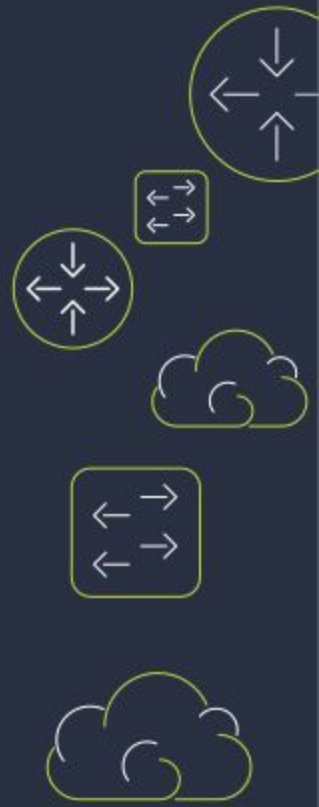
Consequências destes ataques

1. Quando o montante de ataque é grande e de muitas origens diferentes, as vezes é necessário parar de anunciar tudo para o IX e desviar o tráfego para um scrubbing center. Com isso, **deixa-se de utilizar download** do IX!



Consequências destes ataques

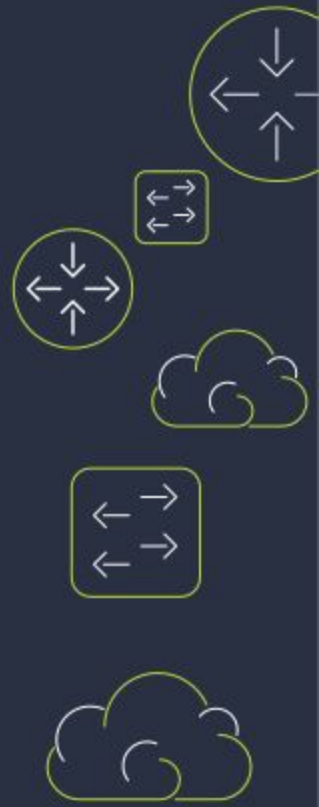
2. Se o ataque é no IP de WAN do IX, deixar de anunciar não é suficiente. É necessário desligar a interface do ATM. Com isto, **deixa-se de utilizar o download e o upload** do IX!



Consequências destes ataques

3. Quando os ASNs origem dos ataques não têm full routing, eles **não respeitam** a tua engenharia de tráfego de desviar os blocos atacados para um scrubbing center.

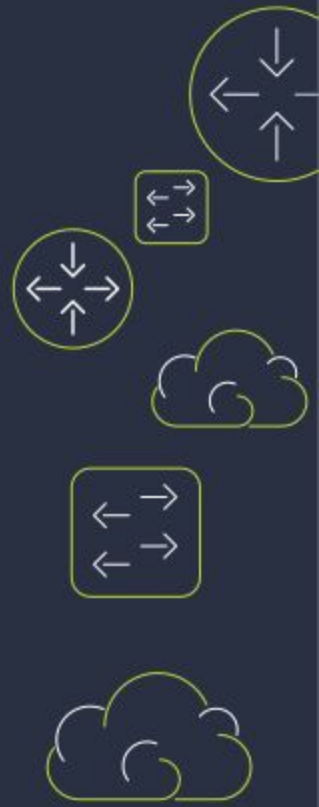
Neste caso, deixar de anunciar não resolve. Também é necessário **desligar o IX**.



Impactos da falta do IX

1. **Aumento da latência** para conteúdos que estão no IX.[1]

2. **Aumento de despesas** com trânsito IP.



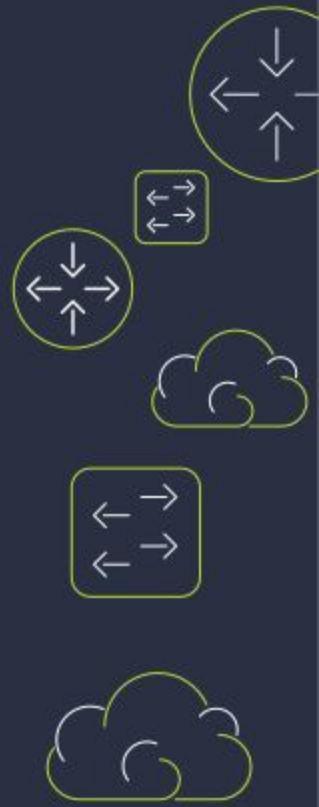
[1] Apenas em casos específicos.

Como se defender disto

1. Possua serviço de **mitigação externa** (clean pipe ou nuvem de mitigação) e/ou;

2. Tenha capacidade suficiente de trânsito IP (ainda que burstable). **IX não é trânsito.**

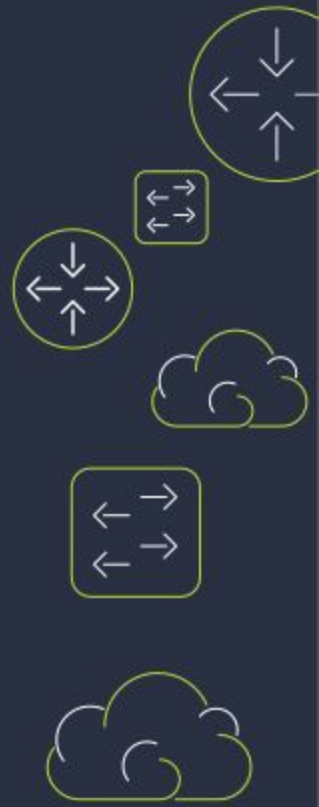
3. Colete as evidências dos ataques recebidos pelo IX e **reporte ao ASN de origem**, copiando o cert.br.



Como se defender disto

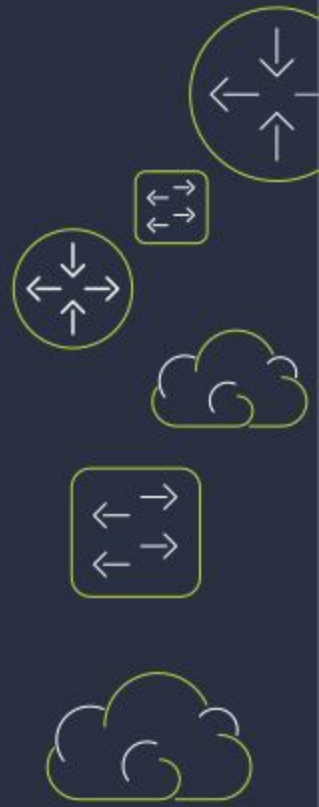
4. **Use IPv6**. Dos 1195980 ataques citados no começo desta apresentação, 0 (zero) foram em IPv6.

O IPv6 não é invulnerável a ataques DDoS, ele apenas não é interessante para os ofensores por enquanto. Então em casos extremos, você pode desligar o ATM do IX em IPv4 e continuar usando o ATM em IPv6 :)



Como o CERT e o IX poderiam nos ajudar

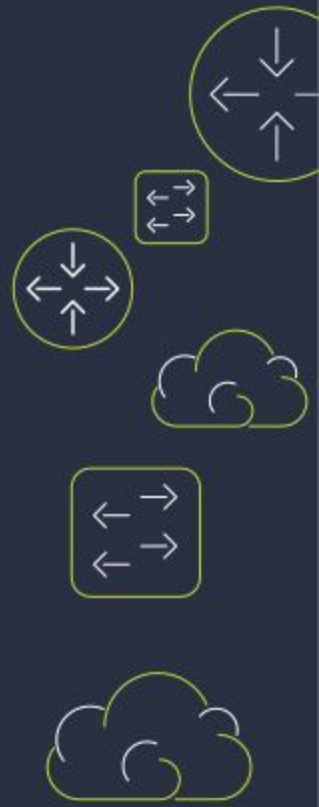
- Sendo **rígidos com os ASNs origem** que não responderem aos abuse reports de ataques DDoS, vejamos o PUA[1] do IX.BR adiante.



[1] http://old.ix.br/doc/PUA_IX.br_V1.0_30_06_2017.pdf

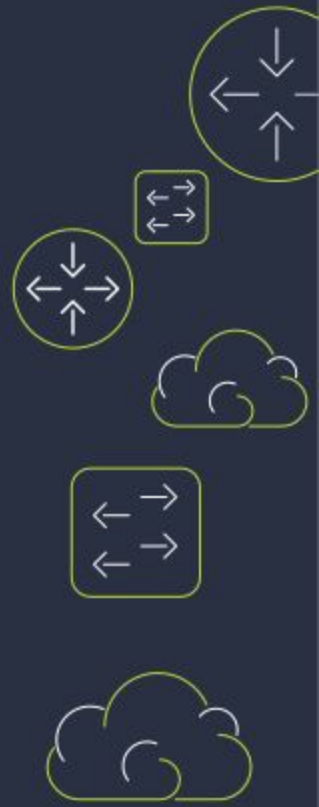
PUA do IX.BR

“Participantes são responsáveis por monitorar apropriadamente sua redes em um regime 24 x 7 (24 horas, ou sete dias da semana) para garantir que sua utilização do IX.br não pretenda ou provoque inundação da rede (flooding) ou ataques de negação de serviço.”



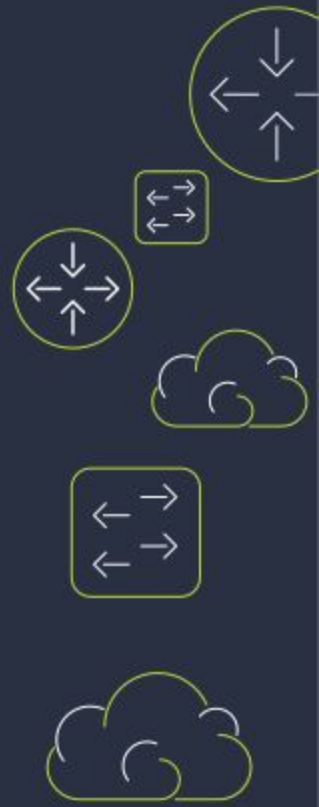
PUA do IX.BR

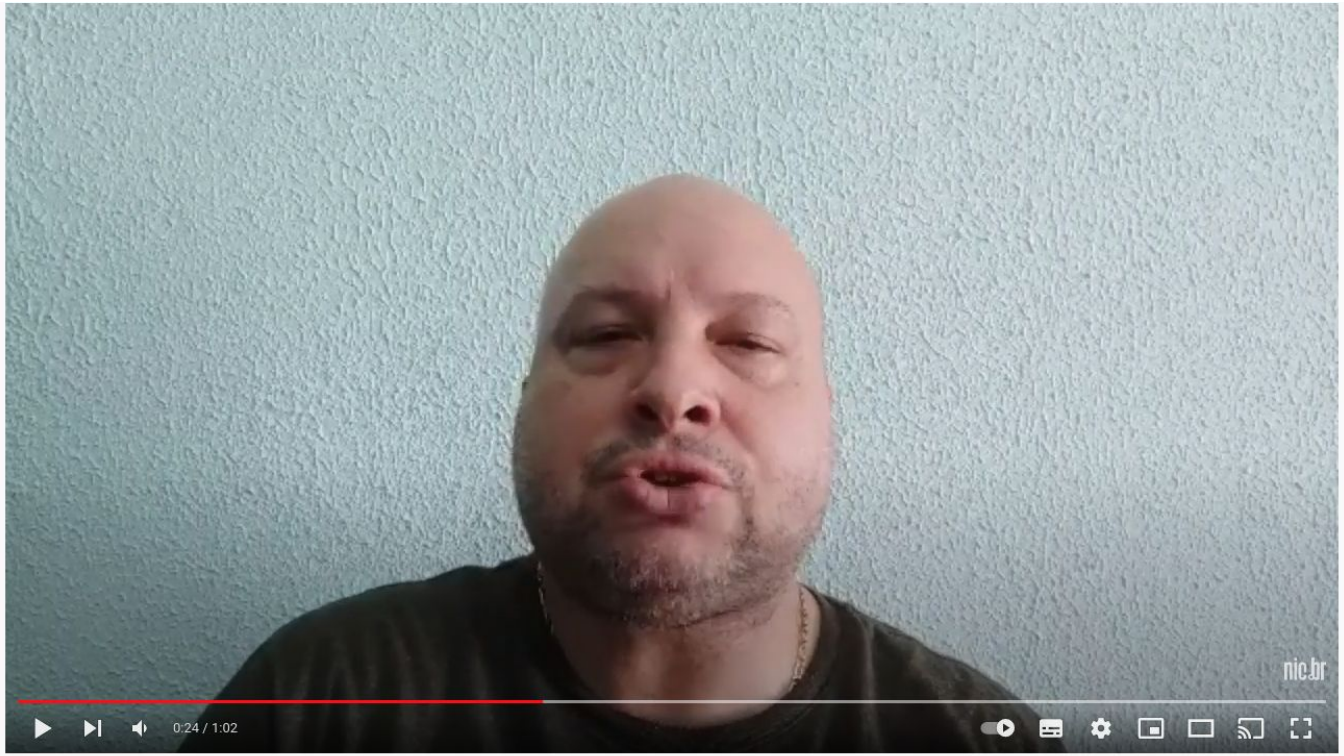
“O NIC.br se reserva o direito de desconectar todas as portas envolvidas em atividades maliciosas, e/ou varredura de portas.”



Como não ser origem destes ataques

- **Monitorar** variações significativas de **upload** na rede.
- Aplicar **BCP38.**
- Manter serviços de rede (como DNS, NTP etc) com **restrições de acesso e de consulta** externas.
- Manter serviços e equipamentos de rede **atualizados**.
- Aderir ao **MANRS.**





[9ª Semana de Infraestrutura] Objetivos e vantagens de se obter o selo MANRS para o Sistema Autônomo

217 visualizações • 14 de nov. de 2019

9 0 COMPARTILHAR SALVAR ...

NICbrvideos
63,3 mil inscritos

INSCRITO

youtube.com/user/NICbrvideos/

Dúvidas?

E-mail:
daniel.damito@sagenetworks.com.br

Site: sagenetworks.com.br
Telefone: (19) 3500-6269