Escola Regional de Redes de Computadores (ERRC). DOI: 10.5753/errc.2024.4646


**Artigo Completo/Full Paper**

# Investigando as Implicações de Segurança da Engenharia de Tráfego e Conectividade no Roteamento da Internet

## Investigating the Security Implications of Traffic Engineering and Connectivity in Internet Routing

**Renan Barreto** • renan.barreto@furg.br
*Universidade Federal do Rio Grande (FURG)*

**Leandro Bertholdo** • leandro.bertholdo@ufrgs.br
*Universidade Federal do Rio Grande do Sul (UFRGS)*

**Pedro Marcos** • pbmarcos@furg.br
*Universidade Federal do Rio Grande (FURG)*

**resumo.** Com o crescimento da Internet, a operação do roteamento BGP tornou-se mais complexa, ao mesmo tempo que a adoção de diversas técnicas de engenharia de tráfego tem se popularizado. No entanto, técnicas como *prepend* e anúncio seletivo são associadas ao aumento da vulnerabilidade ao sequestro de prefixos — situação em que um Sistema Autônomo (AS) anuncia, de forma indevida, prefixos pertencentes a outro AS. Este artigo propõe uma metodologia para avaliar a suscetibilidade das redes a sequestros de prefixo em função do uso dessas práticas. Os resultados preliminares revelam que o uso de *prepend* pode elevar a suscetibilidade ao sequestro em uma faixa de 21,5% a 96,2%, dependendo da topologia de interconexão dos ASes. Redes com menor número de interconexões apresentaram maior probabilidade de ter seus sequestros visíveis em porções mais amplas da Internet.

**abstract.** With the growth of the Internet, the operation of BGP routing has become more complex, while the adoption of various traffic engineering techniques has gained popularity. However, techniques such as *prepend* and selective announcement are associated with an increased vulnerability to prefix hijacking—a situation in which an Autonomous System (AS) improperly announces prefixes belonging to another AS. This paper proposes a methodology to evaluate the susceptibility of networks to prefix hijacking based on the use of these practices. Preliminary results reveal that the use of *prepend* can increase the susceptibility to hijacking by a range of 21.5% to 96.2%, depending on the interconnection topology of the ASes. Networks with fewer interconnections showed a higher likelihood of having their hijacks visible across larger portions of the Internet.

**palavras-chave:** BGP • Engenharia de Tráfego • Segurança • Roteamento
**keywords:** BGP • Traffic Engineering • Security • Routing

## 1 Introdução

A Internet é a principal ferramenta de comunicação na sociedade contemporânea. Sua evolução, marcada por um crescimento vertiginoso em importância e diversidade, resultou em um aumento significativo na complexidade de sua topologia e no número de interconexões entre as diversas redes que a compõem. Esse crescimento na complexidade visa, de modo geral, proporcionar uma melhor qualidade de experiência ao usuário. Contudo, entre os desafios decorrentes dessa evolução, destacam-se a complexidade do roteamento e as vulnerabilidades de segurança.

A Internet é formada pela interconexão de diversas redes, conhecidas como Sistemas Autônomos (ASes). Cada AS possui autonomia na definição de suas estratégias de roteamento, sendo essas decisões frequentemente orientadas por acordos comerciais e interesses próprios. Diferentes classes de ASes podem ser identificadas com base em padrões de comportamento semelhantes. Por exemplo, ASes de trânsito têm como principal função fornecer conectividade global a ASes menores, geralmente operando em uma região específica. Em contraste, ASes provedores de conteúdo tendem a estabelecer conexões com o maior número possível de redes para garantir a entrega eficiente de seus serviços.

Para lidar com as relações e os diferentes objetivos dos ASes que compõem a Internet, utiliza-se o protocolo de roteamento BGP (*Border Gateway Protocol*) e seus atributos. Esse protocolo define critérios para a seleção de rotas no tráfego entre ASes; entretanto, ele não oferece a um AS controle absoluto sobre o caminho de envio e recepção de determinado tráfego.

Para superar essa limitação, são aplicadas técnicas de engenharia de tráfego, que consistem na manipula-

ção dos atributos do BGP, visando "influenciar" como um determinado prefixo será encaminhado. Os pacotes destinados para cada prefixo na Internet são, então, encaminhados com base nos anúncios de rotas recebidos, em conformidade com os critérios de seleção destes atributos. O objetivo dessas técnicas é persuadir os ASes vizinhos a adotar a rota desejada. Um exemplo desta abordagem é o *AS-path-prepend* (APP) [1].

Os desafios relacionados à segurança também se manifestam no contexto do roteamento, sendo um dos mais críticos os eventos de sequestro de prefixo. Esses eventos ocorrem quando um AS anuncia um prefixo que não lhe pertence, sequestrando assim o tráfego de forma indevida. Esses incidentes podem causar interrupções de serviço ou ser explorados como vetores para outros tipos de ataques [2–7]. Embora existam mecanismos para mitigar o sequestro de prefixo, ainda não há um conhecimento completo sobre os fatores que aumentam a probabilidade de um prefixo ser sequestrado, nem sobre os efeitos resultantes da combinação de diferentes fatores e qual a influência das diferentes técnicas de engenharia de tráfego sobre eles. Os sequestros de prefixos são eventos diários–são contabilizados 17,5 casos suspeitos de sequestro de prefixo de origem forjada por dia [8]. Adicionalmente, 1,4% dos ASes sequestradores são recorrentes, de acordo com a análise de um classificador baseado em aprendizado de máquina [9].

Nosso objetivo neste artigo é estabelecer uma metodologia e investigar as implicações de segurança de duas técnicas de engenharia de tráfego: o *AS-path-prepend* e o uso de prefixos mais específicos. Buscamos inferir como a conectividade de um AS e a aplicação dessas técnicas afetam o sucesso potencial de um atacante no sequestro de um prefixo.

Para atingir esse objetivo complementamos as metodologias utilizadas em [1, 10] sobre a plataforma PEERING e combinando com dados do plano de controle e do plano de dados para analisar de forma sistemática os aspectos de segurança do uso de técnicas de engenharia de tráfego. A plataforma PEERING [11] é um ambiente de pesquisa que oferece acesso controlado e real ao sistema de roteamento BGP.

Este artigo está organizado da seguinte forma: na Seção 2, revisamos os trabalhos relacionados; em Seção 3, detalhamos o método e o ambiente utilizados nesta pesquisa; e em Seção 4, apresentamos os resultados iniciais. Por fim, na Seção 5, discutimos nossas conclusões e indicamos direções para trabalhos futuros.

## 2 Trabalhos Relacionados

O estudo dos impactos das técnicas de engenharia de tráfego ainda apresenta lacunas, especialmente no que se refere à segurança. O ASPP, (*AS Path Prepend*), é uma técnica previamente estudada, analisando o uso de *prepends* e propondo formas de aplicá-los de maneira eficaz [12–14]. No entanto, o impacto do ASPP na segurança só foi publicado em 2020 [1], quando se demonstrou que o uso de *prepends* longos (acima de 3 *prepends*) como alternativa de engenharia de tráfego aumentam a vulnerabilidade a sequestros de prefixo. Embora o trabalho tenha quantificado que 94% do tráfego monitorado foi sequestrado utilizando um ASPP de tamanho 3, não foram identificados quais são os ASes envolvidos e quais características eles compartilham, como, por exemplo, o nível de conectividade.

Diversas abordagens foram propostas para mitigar o sequestro de prefixos, como o *DROP* (*Don't Route Or Peer*) [15], os registros IRR (*Internet Routing Registry*) [16], e o RPKI (*Resource Public Key Infrastructure*) [17]. O *DROP* consiste em uma lista restrita de prefixos considerados uma ameaça à comunidade, abrangendo apenas um subconjunto dos prefixos maliciosos. O IRR, por sua vez, funciona como um mecanismo de defesa contra o roubo de prefixos, permitindo que ASes registrem suas rotas e validem a origem dos anúncios de prefixos. Entretanto, a falta de padronização e de controle de qualidade nos registros compromete a segurança do roteamento. Du *et al.* [18] demonstrou que registros fraudulentos podem ser inseridos nos IRRs, aparentando ser legítimos.

Por fim, o RPKI é utilizado para validar objetos ROA (*Route Origin Authorizations*), que associam blocos de IP (*Internet Protocol*) aos ASes autorizados a anunciá-los, garantindo que o anúncio seja originado por um AS devidamente certificado. O uso de RPKI/ROA aumenta a segurança contra sequestros de prefixos, inclusive contra técnicas de engenharia de tráfego. No entanto, sua adoção permanece baixa: em 2017, apenas 10% dos ASes possuíam ROA, subindo para 15% em 2019 [19]. A resistência à adoção do RPKI deve-se a barreiras financeiras e técnicas, apesar dos riscos conhecidos de sequestro de prefixos [20]. Além disso, prefixos assinados, mas não anunciados, podem ser explorados por agentes maliciosos, como demonstrado pelo anúncio de um prefixo peruano por um AS russo, simulando uma conexão legítima [15].

O sequestro de prefixos continua a ser um desafio, com alguns ASes identificados como sequestradores reincidentes [9]. Atualmente, são registrados cerca de 17,5 casos suspeitos de sequestro de origem por dia [8], e estima-se que até 20% das rotas estabelecidas entre novos pares de ASes possam ser forjadas [21]. Além disso, sequestradores podem manipular anúncios de forma

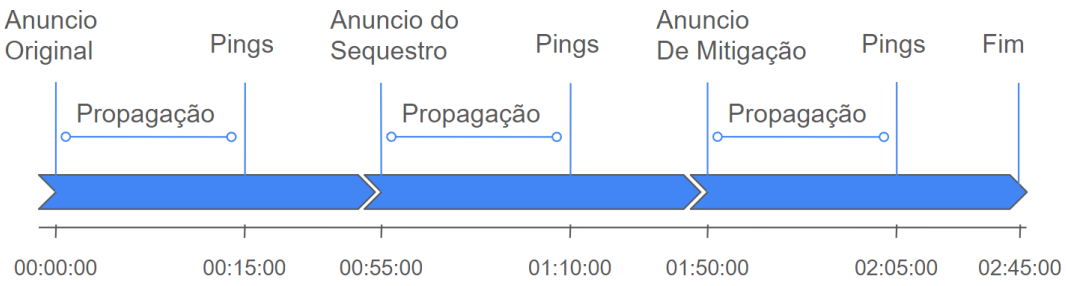


**Figura 1.** Linha do tempo de cada rodada do experimento. Após 15 minutos do anúncio do prefixo, verifica-se o RIS Live e envia-se ICMP-echo-request aos alvos para validar a alcançabilidade. Em seguida, são realizadas a tentativa de sequestro e, posteriormente, a de mitigação, com novas verificações no RIS Live e de alcançabilidade a cada fase.

invisível, evitando o registro por coletores e monitores conhecidos [22]. Diante desses desafios, e do aumento no uso de engenharia de tráfego, torna-se crucial aprofundar o entendimento sobre a segurança dos anúncios BGP, levando em consideração tanto a engenharia de tráfego quanto a conectividade dos ASes.

## 3 Metodologia

Nesta seção, detalhamos a metodologia empregada para avaliar as implicações de segurança das técnicas de engenharia de tráfego. Nossos experimentos, ilustrados na Figura 1, simulam sequestros de prefixos e suas respectivas tentativas de mitigação, utilizando blocos IPv4 especificamente designados para este fim. Utilizamos a plataforma PEERING [11], um *testbed* global para pesquisa em roteamento BGP, e coletamos dados de impacto por meio dos coletores do RIS Live [23], um serviço mantido pelo RIPE NCC que registra e armazena anúncios BGP de forma distribuída em locais estratégicos, como Internet Exchange Points (IXPs).

Embora o RIS Live possua cerca de 400 monitores, sua distribuição geográfica é concentrada no hemisfério norte, podendo limitar sua cobertura [10]. Assim, complementamos a análise com medições no plano de dados, por meio de consultas ICMP (*Internet Control Message Protocol*) utilizando a ferramenta *nping*, para gerar as requisições ICMP, enquanto as respostas são capturadas via *tcpdump* [24, 25]. Após o envio de cada *ICMP-echo-request*, as respostas são monitoradas por até dois minutos (*timeout*). São realizadas cinco tentativas de envio para cada endereço-alvo. Quando o *ICMP-echo-reply* é recebido no Mux Sequestrador, sabemos que o plano de dados dos roteadores acatou o anúncio do sequestrador.

A lista de alvos utilizada foi construída a partir da versão mais recente do *Internet address census* [26]. A lista final resultou em 127.421 endereços IP responsivos distribuídos em 40.000 ASes, limitando a cinco endereços por AS para garantir uma amostra mais equilibrada.

A Figura 2 ilustra um exemplo de como é configurada a plataforma PEERING com seus múltiplos *muxes* para os testes realizados. São realizadas várias combinações de *muxes* no papel de sequestrador (atacante) e de originador buscando entender implicações como conectividade e diversidade geográfica. Utilizamos os seguintes *muxes* do PEERING: `amsterdam01`, `gatech01`, `grnet01`, `ufmg01`, `vultrjohannesburg`, `vultrseoul`.

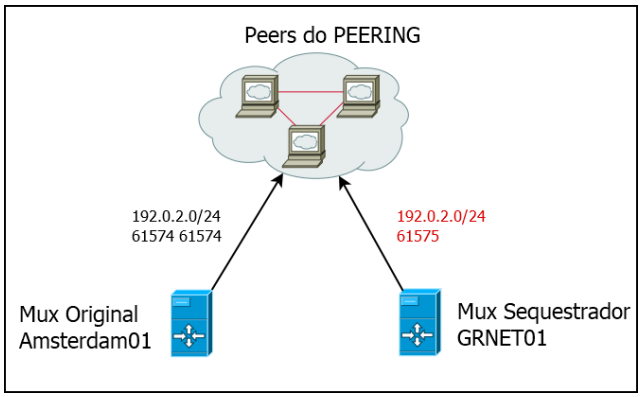


**Figura 2.** AS original (Mux `Amsterdam01`) anuncia seu prefixo `192.0.2.0/24` com prepend 1, enquanto o sequestrador (`GRNET01`) anuncia sem prepend, criando um caminho mais curto e falso para o destino.

Os testes foram conduzidos a partir de uma máquina localizada em Rio Grande ou em uma máquina virtual em Porto Alegre. Tanto o PEERING quanto os *scripts* utilizados estão versionados no *GitHub*. A configuração de cada experimento é especificada por um arquivo de texto, que define a vítima, o atacante e as opções de engenharia de tráfego.

Cada experimento é executado de forma isolada, sem paralelismo, para evitar interferências. A comunicação entre o cliente PEERING e os *muxes* define dinamicamente as configurações de anúncio de cada experimento, permitindo testar diferentes cenários e avaliar o impacto das técnicas de engenharia de tráfego

sobre a segurança dos anúncios BGP.

## 4 Resultados

Conforme apresentado na Seção 1, o primeiro objetivo deste trabalho é identificar as características dos ASes mais suscetíveis a ataques de roubo de prefixo, utilizando uma metodologia adequada.

Durante os testes, enfrentamos desafios com *muxes* da plataforma PEERING que não propagavam anúncios ou filtravam *prepends*, além de coletores do RIS que não registravam os anúncios legítimos, mas capturavam os de tentativa de roubo de prefixo. Também identificamos filtros em provedores. Alguns comportamentos foram classificados como *bugs* na plataforma, enquanto outros resultaram de ajustes em filtros de provedores e a descoberta de proteções implementadas por grandes operadoras (*Tier-1*). A metodologia atual, descrita na Seção 3, está em sua sétima versão. Foram incorporadas medições ativas, ajustes no tempo de propagação, na quantidade de *ICMP-echo-requests*, e na lista de alvos, entre outros. A seguir, apresentamos os resultados preliminares obtidos com esta metodologia.

O primeiro teste realizado utilizou a técnica ASPP com um prefixo IPv4 /23. Na Figura 3, `amsterdam01` realiza o anúncio original com 2 *prepends*, sendo observado por 376 dos 400 coletores globais do RIS. Em seguida, `grnet01` realiza o mesmo anúncio do prefixo /23 sem nenhum *prepend*, conseguindo sequestrar o prefixo, que foi registrado por 134 dos 400 coletores. Posteriormente, foi realizada uma mitigação comumente usada por provedores, na qual o prefixo mais específico possível (/24) foi anunciado em `amsterdam01` sem nenhum *prepend*. Nesse cenário, 122 dos 134 coletores que haviam registrado o sequestro foram recuperados em menos de 30 segundos.

A Tabela 1 apresenta os resultados das medições realizadas nos planos de controle e dados. Nessas análises, foram considerados apenas os monitores e alvos

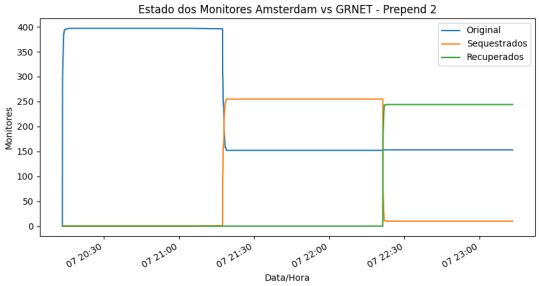


**Figura 3.** Resultados da propagação do anúncio com 2 prepends entre `amsterdam01` (Vítima) e `grnet01` (Sequestrador). Monitores que aceitaram o anúncio original estão em azul, os que aceitaram o sequestro em laranja, e os recuperados pela mitigação em verde.

que responderam de forma consistente em todas as etapas de cada experimento. Por exemplo, ao originar o prefixo em `amsterdam01`, observou-se que o tamanho do *prepend* está diretamente relacionado ao impacto do sequestro de prefixo, tanto no plano de controle quanto no plano de dados.

Em outro caso, quando `grnet01` origina o prefixo, dois aspectos são particularmente relevantes. Primeiro, o impacto do sequestro mostrou-se pouco sensível ao tamanho do *prepend*, sugerindo que `amsterdam01` tem caminhos mais curtos para os alvos, o que dificulta o sequestro e ressalta a importância da conectividade para a segurança do roteamento. Segundo, aproximadamente 20% dos monitores ou alvos não foram sequestrados, indicando que esses, ou outros ASes no caminho, podem selecionar rotas com base em preferências locais. Esses casos serão investigados em trabalhos futuros. Além disso, observou-se que o uso de prefixos mais específicos é uma estratégia eficaz de mitigação.

O impacto de um sequestro realizado com um anúncio mais específico, sem o uso de *prepend* pela vítima, também foi avaliado. A Tabela 2 apresenta os resultados em que o *anúncio original* utilizou o prefixo /23,

| Configuração dos Experimentos | | | Monitores no Plano de Controle | | | Alvos no Plano de Dados | | |
|---|---|---|---|---|---|---|---|---|
| Originador | Atacante | Tamanho do *Prepend* | Total | Sequestrados | Recuperados | Total | Sequestrados | Recuperados |
| Amsterdam | GRNET | 0 | 395 | 85 (21.52%) | 75 (88.24%) | 1682677 | 356119 (21.16%) | 356119 (100%) |
| Amsterdam | GRNET | 1 | 397 | 142 (35.77%) | 132 (92.96%) | 1679636 | 762282 (45.38%) | 762282 (100%) |
| Amsterdam | GRNET | 2 | 397 | 255 (64.23%) | 244 (95.69%) | 1678404 | 1282353 (76.40%) | 1282353 (100%) |
| Amsterdam | GRNET | 3 | 396 | 381 (96.21%) | 368 (96.59%) | 1680564 | 1680564 (100%) | 1680564 (100%) |
| GRNET | Amsterdam | 0 | 381 | 320 (83.99%) | 296 (92.50%) | 1646449 | 1228879 (74.64%) | 1228879 (100%) |
| GRNET | Amsterdam | 1 | 382 | 328 (85.86%) | 305 (92.99%) | 1635977 | 1313934 (80.31%) | 1313934 (100%) |
| GRNET | Amsterdam | 2 | 382 | 329 (86.13%) | 305 (92.71%) | 1653106 | 1321587 (79.95%) | 1321587 (100%) |
| GRNET | Amsterdam | 3 | 381 | 330 (86.61%) | 306 (92.73%) | 1664218 | 1333532 (80.13%) | 1333532 (100%) |

**Tabela 1.** Resultados preliminares para medições no Plano de Controle e Plano de Dados sem utilizar prepend no anúncio original e então utilizando prepend de tamanho 1 até tamanho 3. O sequestro ocorre sem prepend e com prefixo de mesmo tamanho.

| Configuração dos Experimentos | | | Monitores no Plano de Controle | | | Alvos no Plano de Dados | | |
|---|---|---|---|---|---|---|---|---|
| Originador | Atacante | Tamanho do Prefixo Original | Total | Sequestrados | Recuperados | Total | Sequestrados | Recuperados |
| amsterdam01 | ufmg01 | /23 | 398 | 374 (93.97%) | 259 (69.25%) | * | * (*%) | * (*%) |
| amsterdam01 | ufmg01 | /24 | 400 | 93 (23.25%) | N/A | 99901 | 34237 (34.27%) | N/A |
| amsterdam01 | vultrjohannesburg | /23 | 401 | 391 (97.51%) | 247 (63.17%) | * | * (*%) | * (*%) |
| amsterdam01 | vultrjohannesburg | /24 | 400 | 128 (32%) | N/A | 90512 | 33381 (36.88%) | N/A |
| amsterdam01 | vultrseoul | /23 | 399 | 372 (93.23%) | 296 (79.57%) | * | * (*%) | * (*%) |
| amsterdam01 | vultrseoul | /24 | 403 | 71 (17.61%) | N/A | 89996 | 19685 (21.87%) | N/A |
| ufmg01 | amsterdam01 | /23 | 372 | 397 (106.72%) | 94 (23.68%) | * | * (*%) | * (*%) |
| ufmg01 | amsterdam01 | /24 | 375 | 314 (83.73%) | N/A | * | * (*%) | N/A |
| ufmg01 | vultrjohannesburg | /23 | 372 | 391 (105.11%) | 149 (38.11%) | * | * (*%) | * (*%) |
| ufmg01 | vultrjohannesburg | /24 | 374 | 227 (60.69%) | N/A | * | * (*%) | N/A |
| ufmg01 | vultrseoul | /23 | 372 | 371 (99.73%) | 229 (61.72%) | * | * (*%) | * (*%) |
| ufmg01 | vultrseoul | /24 | 374 | 137 (36.63%) | N/A | * | * (*%) | N/A |

**Tabela 2.** Resultados para medições no plano de controle e plano de dados dos experimentos envolvendo prefixos mais específicos sem prepend, onde o anúncio original varia de /23 a /24 enquanto os sequestros são realizados utilizando /24.

enquanto o *anúncio do sequestro* usou prefixos /24. Nos casos em que os *muxes* vítimas foram `amsterdam01` ou `ufmg01`, também realizamos experimentos com ambos os anúncios usando prefixos /24. Os experimentos envolvendo `gatech01` falharam na propagação dos anúncios e foram removidos da tabela, enquanto outros experimentos com falhas estão indicados com asterisco. Cabe ressaltar que, em vários casos, ocorreram falhas na coleta de dados no plano de dados.

Os resultados do plano de controle mostram que um sequestro utilizando um prefixo mais específico captura a maioria dos monitores. No caso de `amsterdam01` sequestrando o prefixo de `ufmg01`, o primeiro consegue capturar mais monitores do que no anúncio original. Isso de deve ao fato do peer entre PEERING e alguns ISP permitir somente prefixos /24. Então consideramos que 100% dos prefixos foram capturados.

Quando o anúncio original é desagregado em prefixos /24, o impacto é reduzido, semelhante ao observado com prefixos /23 sem *prepend* (vide Tabela 1). Entretanto, nesse cenário, não haveria uma medida de mitigação viável, pois um prefixo /25 provavelmente seria filtrado. Assim, a conectividade do *mux* permanece um fator crítico. As falhas nas medições do plano de dados continuam sob investigação, sendo possível que requisições tenham sido filtradas durante o processo.

## 5 Conclusão e Trabalhos Futuros

Nossas avaliações preliminares indicam que a conectividade de um AS é relevante para a segurança de seus anúncios. Um AS menos conectado teve 83,99% dos monitores sequestrados sem uso de engenharia de tráfego, e o uso de *prepend* aumentou a suscetibilidade de sequestro de 21,52% para 96,21%. Além disso, o uso de prefixos mais específicos por ASes bem conectados resultou na totalidade dos monitores sequestrados.

Este trabalho, ainda em andamento, buscará avaliar outros *muxes* e o impacto de diferentes técnicas de engenharia de tráfego, bem como a conectividade dos monitores e alvos. Aproximadamente 20% dos monitores não foram sequestrados, possivelmente devido a preferências locais de roteamento, conforme mostrado na Tabela 1.

Após avaliar individualmente as técnicas de engenharia de tráfego, investigaremos a interação entre múltiplas técnicas. Como contribuição, ampliamos a lista de alvos de *ping*, geograficamente distribuídos, e resolvemos problemas relacionados ao uso de ASN em anúncios nos *muxes* da rede Vultr, complementando as metodologias de [1, 10].

Como contribuições para complementar as metodologias utilizadas em [1, 10] na plataforma PEERING, apresentamos uma nova lista de alvos ICMP responsivos, distribuídos geograficamente, com limitação de ASes para evitar vieses causados por grandes ASes com múltiplos alvos. Além disso, contribuímos para melhorias na plataforma PEERING pela identificação de um problema relacionado ao anúncio de prefixos com ASN de origem nos *muxes* utilizando a estrutura do provedor de nuvem Vultr.

## Declarações complementares

### Disponibilidade de dados e materiais adicionais

Os dados e/ou materiais adicionais serão publicados após a expansão do trabalho e então poderão ser disponibilizados mediante solicitação.

## Referências

1 Botelho Marcos, P. de *et al.* AS-Path Prepending: There is No Rose without a Thorn. *In*: ACM IMC 2020. Virtual Event, USA, 2020. ISBN 9781450381383. DOI: 10.1145/3419394.3423642. Disponível em: https://doi.org/10.1145/3419394.3423642.

2 Turba, T. *Amazon once again lost control (for 3 hours) over the IP pool in a BGP hijacking attack*. Nov. 2022. Disponível em: https://research.securitum.com/amazon-once-again-lost-control-for-3-hours-over-the-ip-pool-in-a-bgp-hijacking-attack/.

3 Madory, D. *BGP hijack of Amazon DNS to steal crypto currency*. Oracle Developers, mai. 2018. Disponível em: https://medium.com/oracledevs/bgp-hijack-of-amazon-dns-to-steal-crypto-currency-a90dd29cb3ab.

4 Kacherginsky, P. *Celer Bridge incident analysis*. 2022. https://www.coinbase.com/pt-br/blog/celer-bridge-incident-analysis. Disponível em: https://www.coinbase.com/pt-br/blog/celer-bridge-incident-analysis. Acesso em: 20 ago. 2024.

5 Miao, S. *Yet another BGP hijacking towards AS16509*. 2022. https://mailman.nanog.org/pipermail/nanog/2022-August/220320.html. Disponível em: https://mailman.nanog.org/pipermail/nanog/2022-August/220320.html. Acesso em: 20 ago. 2024.

6 Siddiqui, A. *Not just another BGP Hijack*. 2020. https://manrs.org/2020/04/not-just-another-bgp-hijack/. Disponível em: https://manrs.org/2020/04/not-just-another-bgp-hijack/. Acesso em: 20 ago. 2024.

7 Siddiqui, A. *KlaySwap – Another BGP Hijack Targeting Crypto Wallets*. 2022. https://manrs.org/2022/02/klayswap-another-bgp-hijack-targeting-crypto-wallets/. Disponível em: https://manrs.org/2022/02/klayswap-another-bgp-hijack-targeting-crypto-wallets/. Acesso em: 20 ago. 2024.

8 Holterbach, T. *et al.* A System to Detect Forged-Origin Hijacks. *In*: 21TH USENIX Symposium on Networked Systems Design and Implementation (NSDI 24). USENIX Association, 2024.

9 Testart, C. *et al.* Profiling BGP Serial Hijackers: Capturing Persistent Misbehavior in the Global Routing Table. *In*: PROCEEDINGS of the Internet Measurement Conference. Amsterdam, Netherlands: Association for Computing Machinery, 2019. (IMC '19), p. 420–434. ISBN 9781450369480. DOI: 10.1145/3355369.3355581. Disponível em: https://doi.org/10.1145/3355369.3355581.

10 Bertholdo, L. M. *et al.* On the Asymmetry of Internet eXchange Points -Why Should IXPs and CDNs Care? *In*: 2022 18th International Conference on Network and Service Management (CNSM). 2022. P. 73–81. DOI: 10.23919/CNSM55787.2022.9964817.

11 Schlinker, B. *et al.* PEERING: virtualizing BGP at the edge for research. *In*: PROCEEDINGS of the 15th International Conference on Emerging Networking Experiments And Technologies. Orlando, Florida: Association for Computing Machinery, 2019. (CoNEXT '19), p. 51–67. ISBN 9781450369985. DOI: 10.1145/3359989.3365414. Disponível em: https://doi.org/10.1145/3359989.3365414.

12 Chang, R.; Lo, M. Inbound traffic engineering for multihomed ASs using AS path prepending. *IEEE Network*, v. 19, n. 2, p. 18–25, 2005. DOI: 10.1109/MNET.2005.1407694.

13 Battista, G. D. *et al.* Towards Optimal Prepending for Incoming Traffic Engineering. *In*. Disponível em: https://api.semanticscholar.org/CorpusID:62039321.

14 Rizvi, A. S. M. *et al.* Anycast Agility: Network Playbooks to Fight DDoS. *In*: 31ST USENIX Security Symposium (USENIX Security 22). Boston, MA: USENIX Association, ago. 2022. P. 4201–4218. ISBN 978-1-939133-31-1. Disponível em: https://www.usenix.org/conference/usenixsecurity22/presentation/rizvi.

15 Oliver, L. *et al.* Stop, DROP, and ROA: Effectiveness of Defenses through the Lens of DROP. *In*: PROCEEDINGS of the 22nd ACM Internet Measurement Conference. Nice, France: Association for Computing Machinery, 2022. (IMC '22), p. 730–737. ISBN 9781450392594. DOI: 10.1145/3517745.3561454. Disponível em: https://doi.org/10.1145/3517745.3561454.

16 Rekhter, Y. *Routing in a Multi-provider Internet*. RFC Editor, abr. 1995. 8 p. RFC 1787. (Request for Comments, 1787). DOI: 10.17487/RFC1787. Disponível em: https://www.rfc-editor.org/info/rfc1787.

17 Bush, R.; Austein, R. *The Resource Public Key Infrastructure (RPKI) to Router Protocol*. RFC Editor, jan. 2013. 27 p. RFC 6810. (Request for Comments, 6810). DOI: 10.17487/RFC6810. Disponível em: https://www.rfc-editor.org/info/rfc6810.

18 Du, B. *et al.* IRRegularities in the Internet Routing Registry. *In*: PROCEEDINGS of the 2023 ACM on Internet Measurement Conference. Montreal QC, Canada: Association for Computing Machinery, 2023. (IMC '23), p. 104–110. ISBN 9798400703829. DOI: 10.1145/3618257.3624843. Disponível em: https://doi.org/10.1145/3618257.3624843.

19 Chung, T. *et al.* RPKI is Coming of Age: A Longitudinal Study of RPKI Deployment and Invalid Route Origins. *In*: PROCEEDINGS of the Internet Measurement Conference. Amsterdam, Netherlands: Association for Computing Machinery, 2019. (IMC '19), p. 406–419. ISBN 9781450369480. DOI: 10.1145/3355369.3355596. Disponível em: https://doi.org/10.1145/3355369.3355596.

20 Sermpezis, P. *et al.* A Survey among Network Operators on BGP Prefix Hijacking. *SIGCOMM Comput. Commun. Rev.*, Association for Computing Machinery, New York, NY, USA, v. 48, n. 1, p. 64–69, abr. 2018. ISSN 0146-4833. DOI: 10.1145/3211852.3211862. Disponível em: https://doi.org/10.1145/3211852.3211862.

21 Cho, S. *et al.* BGP hijacking classification. *In*: 2019 Network Traffic Measurement and Analysis Conference (TMA). 2019. P. 25–32. DOI: 10.23919/TMA.2019.8784511.

22 Milolidakis, A. *et al.* On the Effectiveness of BGP Hijackers That Evade Public Route Collectors. *IEEE Access*, v. 11, p. 31092–31124, 2023. DOI: 10.1109/ACCESS.2023.3261128.

23 NCC, R. *RIS Live*. 2024. https://ris-live.ripe.net/. Disponível em: https://ris-live.ripe.net/. Acesso em: 10 jul. 2024.

24 Garcia, L. M.; Fyodor. *Nmap*. 2024. https://nmap.org/. Disponível em: https://nmap.org/. Acesso em: 20 ago. 2024.

25 Group, T. T. *TCPDUMP and LIBPCAP*. 2024. https://www.tcpdump.org/. Disponível em: https://www.tcpdump.org/. Acesso em: 20 ago. 2024.

26 Fan, X.; Heidemann, J. Selecting representative IP addresses for Internet topology studies. *In*: ACM. ACM IMC 2010. 2010. (IMC '10). ISBN 9781450300575. DOI: 10.1145/1879141.1879195.