Analisando o impacto e a capacidade de mitigação de sequestro de prefixos com base na conectividade

Gabriel Trugillo Jaeger[1], **Pedro Marcos**[1]

[1]Universidade Federal do Rio Grande (FURG)
Rio Grande – RS – Brasil

{gabriel_jaeger,pbmarcos}@furg.br

Abstract. *In this study, the influence of connections with tier-1 providers on the performance of networks when subjected to prefix hijacking events is investigated. Through experiments, it evaluates how different connectivity configurations impact their success. It was revealed that the removal of strategic connections with tier-1s increases the impact of the hijacking. Furthermore, temporal analysis show that the absence of connections with tier-1s speeds up the propagation of hijacking announcements. Finally, the importance of understanding the interactions between network architecture and its vulnerabilities is highlighted, as well as the need for more holistic approaches to network security and the necessity for more platforms that facilitate controlled experiments on the Internet.*

Resumo. *Neste estudo, investiga-se a influência das conexões com provedores de tier-1 no desempenho de redes quando submetidas a eventos de sequestro de prefixos, por meio de experimentos que avaliam como diferentes configurações de conectividade impactam seu sucesso. Desse modo, revelou-se que a remoção de conexões estratégicas com tier-1s aumenta o impacto do sequestro. Ademais, análises temporais demonstram que a ausência de conexões com esses provedores acelera a propagação de anúncios de sequestro. Por fim, destaca-se não só a importância de compreender as interações entre arquitetura de redes e suas vulnerabilidades e da necessidade de abordagens mais holísticas à segurança de redes, mas também a demanda por mais plataformas que facilitem experimentos controlados na Internet.*

1. Introdução

A Internet consiste em redes de computadores interconectadas globalmente por meio de enlaces e, para que a informação chegue de um ponto a outro, é preciso seguir padrões de comunicações entre as redes para garantir uma troca de tráfego o mais otimizada possível.

Em geral, cada rede é um Sistema Autônomo (AS), que possui um número de registro único (ASN) e detém uma coleção de prefixos IP. Sendo assim, é possível estabelecer conexões e trocas de informação entre ASes padronizadas pelo Border Gateway Protocol (BGP), o qual permite que um AS anuncie prefixos para outros com alguns atributos para propagar rotas até si para as tabelas de roteamento das redes vizinhas, que selecionarão a melhor rota até os prefixos de destino tendo, por base, a sua política de roteamento.

Apesar da padronização, não há garantias de autenticidade dos prefixos anunciados, resultando em riscos como sequestros de prefixos, que podem causar interrupções e

desvios de tráfego. Nesse sentido, evidenciando a recorrência do problema atualmente, o Crosswork BGPStream da [Cisco 2023] registrou 1169 possíveis sequestros entre fevereiro e setembro de 2023, como verificado em uma breve visita à plataforma.

Em trabalhos recentes, buscou-se iniciar o estudo do impacto do sequestro de prefixos em redes de diferentes configurações, medindo a eficácia do evento e da mitigação de seus efeitos com o uso de prefixos mais específicos, relatadas em um artigo da Mostra de Produção Universitária da FURG [Gabriel Trugillo Jaeger 2023], no qual se evidenciou a necessidade de uma pesquisa mais aprofundada a fim de entender por que cada rede se comporta de tal modo quando é submetida a sequestros de prefixos.

Assim, o presente trabalho quer expandir a compreensão do assunto, por meio de medições com parâmetros mais controlados visando trazer uma perspectiva mais detalhada em como a conectividade de uma rede afeta a efetividade do sequestro de seus prefixos e como os diferentes atores que compõem a Internet se comportam nesses eventos. Para isso, serão utilizadas comunidades BGP para manipular a exportação de tráfego para os provedores tier-1 de um AS na plataforma *PEERING Testbed* [PEERING 2014].

2. Contextualização das Relações entre Sistemas Autônomos

O modo como ASes interagem entre si se reflete na eficiência, na resiliência e na segurança do tráfego na Internet. Considerando que a associação entre eles é, em grande parte, motivada por contratos e interesses econômicos, é evidente que uns terão mais conexões que outros e que suas relações irão variar em complexidade e natureza.

Essas diferentes relações têm implicações na robustez da conectividade das redes: **Resiliência** – ASes com mais conexões de peering e de trânsito são, em geral, mais resilientes, pois têm múltiplas rotas para envio de tráfego caso uma falhe; **Velocidade** – Conexões diretas, como as de peering, tendem a ser mais rápidas e confiáveis, oferecendo mais eficiência aos ASes com muitos peers; **Segurança** – Dependendo da relação, certos ASes podem ser mais suscetíveis a ameaças e, se eles não têm um controle rigoroso das rotas que anunciam ou aceitam, podem alavancar os danos relativos às ameaças.

2.1. Relações de Peering

Acontecem quando há um acordo mutualístico entre ASes, onde a troca de tráfego ocorre com baixo ou nenhum custo, a fim de otimizar a velocidade e a eficiência do serviço, evitando o encaminhamento através de várias redes intermediárias.

2.2. Relações de Trânsito ou Cliente-Provedor.

Em geral, esse tipo de relação ocorre quando ASes menores ou os Provedores de Serviço Internet (ISPs) regionais, que atuam como clientes nessa relação, pagam a outros ASes fornecedores de trânsito de maior capacidade para alcançarem mais partes da Internet e para que carreguem seu tráfego, tendo em vista que os provedores, em teoria, têm mais conexões que o cliente, podendo oferecer esse maior alcance à Internet. [CAIDA 2013]

2.3. Tier-1 Peering

Redes de tier-1 ocupam uma posição especial na hierarquia da Internet, podendo acessar toda a rede via relações de peering sem custos entre elas. Comumente descritas como a espinha dorsal da Internet, ainda que haja argumentos sobre o achatamento da rede [Arnold et al. 2020], sua importância para manter a estabilidade e eficiência é inegável.

2.4. Comunidades BGP

As comunidades BGP acrescentam uma camada de complexidade e personalização do anúncio de rotas na comunicação entre ASes, permitindo sinalizar informações ou influenciar decisões de roteamento ao anunciar prefixos, utilizando atributos disponibilizados pelo AS vizinho que tratará o anúncio recebido conforme a sua política de roteamento.

3. Metodologia

Neste estudo será explorado, usando o atributo Comunidades do BGP, como a relação de uma rede com seus provedores tier-1 afeta o seu desempenho quando submetida a sequestros de prefixos originados por diferentes redes. Para tal, utiliza-se o *PEERING Testbed* para fazer experimentos em um ambiente controlado para simular anúncios na Internet, junto à ferramenta de coleta de dados em tempo real *RIS Live* [RIPE NCC 2015].

Logo, selecionou-se da lista de Peering Sessions do PEERING Testbed o peer com ID de sessão 60, pertencente à rede Bit BV (AS12859), a qual é provedora de trânsito e foi escolhida por possuir como provedores 3 redes tier-1 – *Arelion Sweden AB*, *NTT America, Inc* e *Zayo Bandwidth* – e por oferecer comunidades específicas para sinalizar a não exportação do tráfego para os tier-1: 12859:2240 (NO-OUT-NTTVERIO), 12859:2250 (NO-OUT-ZAYO) e 12859:2260 (NO-OUT-ARELION).

Sendo assim, construiu-se 8 modelos de experimentos de modo a estudar o desempenho de Bit BV em diferentes configurações. Primeiro, fez-se o experimento sem comunidades. Depois, 3 experimentos, cada um com uma delas, para que a rede tivesse apenas duas conexões com tier-1s. Após, mais 3 experimentos combinando as comunidades em pares únicos, deixando a rede com só uma conexão de tier-1. Por fim, usou-se as três comunidades para não enviar trânsito a nenhum tier-1. A adição das comunidades, para todos os modelos, ocorre nas etapas de índices 2, 4, 6 e 7 na Figura 1.

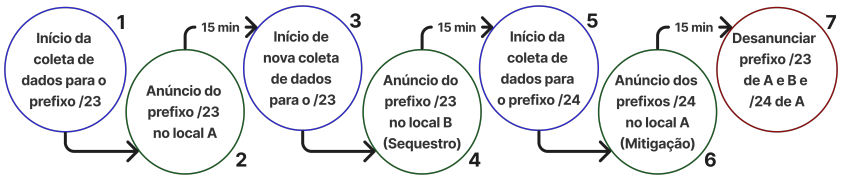

Figura 1. Esquema das rodadas de experimentos de sequestro de prefixos. Fonte: Os autores.

Para todos os modelos, o local "A"é a rede Bit BV, que é submetida aos sequestros de prefixo. Já os locais de ataque, "B", de onde partem os anúncios falsos, são as redes dos multiplexadores do PEERING, que são pontos globais de conexão à plataforma que dão acesso às redes usadas, que são: Clemson University, Georgia Institute of Technology, Greek Research and Technology Network, USC Information Sciences Institute, Northeastern University, São Paulo, Stony Brook University, Seattle, Universidade Federal De Minas Gerais, University of Utah e University of Wisconsin. Já na execução dos experimentos, que ocorreu de 02 a 08 de agosto de 2023, usou-se os prefixos 184.164.226.0/23, 184.164.226.0/24 e 184.164.227.0/24. Ademais, os ASNs de origem, para distinguir os locais A e B no AS-Path das mensagens do RIS, são 47065 e 263842, respectivamente.

4. Resultados e Discussão

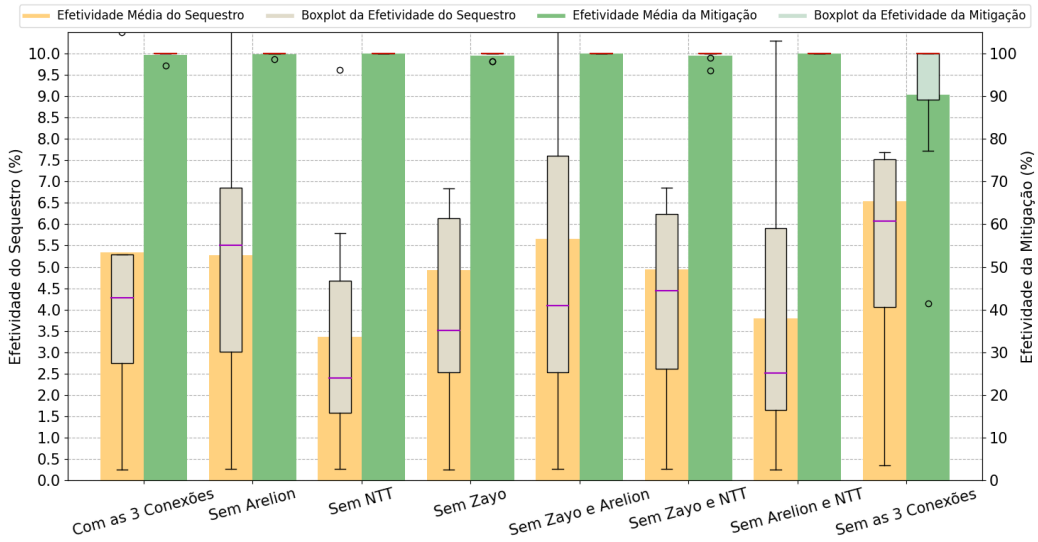

Figura 2. Comparação das efetividades de sequestro e de mitigação para as diferentes configurações dos experimentos. Fonte: Os autores.

Os dados coletados permitiram o cálculo das efetividades do sequestro e da mitigação para todas as rodadas de todos os modelos de experimentos, usando relações derivadas das mensagens dos monitores do RIS Live. Portanto, na Figura 2, são apresentados os resultados para os modelos e os dados de cada rodada das diferentes redes estão agrupados em *boxplots*. Segue o cálculo da efetividade:

- m: Monitor genérico do conjunto total de monitores observados no RIS Live e é definido como a tupla $m = (\text{peer}, \text{peer\_asn})$, onde peer é o endereço IP único do monitor e peer_asn é o ASN dele, garantindo a unicidade do monitor.

- C_i: Coleta de mensagens recebidas exclusivamente da API do RIS Live, correspondente ao índice i na Figura 1, tendo sido filtradas as repetições da tupla m mantendo apenas os dados da mensagem com timestamp mais recente.

- M_{23A} é extraído de C_1 e é definido como:

$$M_{23A} = \{m \in C_1 \mid m \text{ tem ASN 47065 de origem no AS-Path para } /23\}$$

- M_{23B} é subconjunto de M_{23A} e é extraído de C_3, sendo definido como:

$$M_{23B} = \{m \in C_3 \cap M_{23A} \mid m \text{ tem ASN 263842 de origem no AS-Path para } /23\}$$

- M_{24A} é subconjunto de M_{23B} e é extraído de C_5, sendo definido como:

$$M_{24A} = \{m \in C_5 \cap M_{23B} \mid m \text{ tem ASN 47065 de origem no AS-Path para } /24\}$$

$$\text{E. do Sequestro (\%)} = \left(\frac{|M_{23B}|}{|M_{23A}|}\right) \times 100 \qquad \text{E. da Mitigação (\%)} = \left(\frac{|M_{24A}|}{|M_{23B}|}\right) \times 100$$

Dito isso, observa-se um aumento da efetividade do sequestro de 5,34% para 6,54% quando a Bit BV perde todas as três conexões. É complexo identificar um padrão ao retirar uma ou duas conexões devido à irregularidade dos valores. Ao remover um tier-1, o impacto não é consideravelmente maior, e os dois restantes parecem preservar a estabilidade da rede. Com duas conexões retiradas, o resultado sobe levemente, mas a rede se mantém próxima aos valores iniciais.

Quanto à efetividade de mitigação, não há uma relação clara com a remoção de conexões com tier-1s, uma vez que 7 dos 8 casos apresentaram eficácia próxima de 100%. Porém, com a retirada das 3 conexões, essa efetividade média caiu para 90,35%. Adicionalmente, é importante notar que a Figura 2 mostra desvios-padrão elevados, que são consequência das diferentes configurações das redes do PEERING usadas nos sequestros.

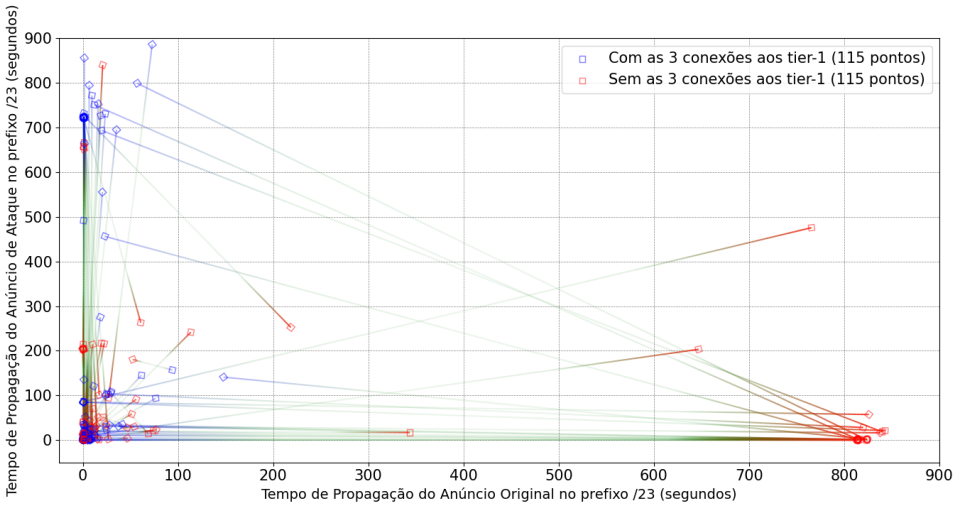

Figura 3. Transição dos tempos de propagação entre as etapas com as 3 conexões aos tier-1s e sem elas. Fonte: Os autores.

A fim de compreender a propagação dos anúncios, estabeleceram-se relações entre os tempos que cada monitor do RIS levou para recebê-los. Tendo em vista o caso mais extremo evidenciado nas efetividades da Figura 2, a Figura 3 ilustra os monitores (pontos quadrados) quando o local atacado possuía 3 conexões e, posteriormente, quando sem as conexões. As linhas representam a transição de um momento para o outro. É importante mencionar que, dos monitores que oferecem sua tabela de rotas completa ao RIS, somente 115 aparecem nos dois cenários, por motivos de visibilidade e alcance de propagação.

Avaliando o gráfico da Figura 3, percebe-se que uma parcela (27,83%) dos monitores em azul está acima de 400 segundos no eixo que mostra o tempo de propagação do anúncio do sequestro e que os mesmos monitores, ao serem retiradas as 3 conexões de tier 1, vão para valores entre 0 e 250 segundos, mostrando que o anúncio do sequestrador chegou mais rápido aos monitores quando Bit BV não tinha conexões com provedores tier-1. Além disso, para o tempo de atraso do anúncio original – ou seja, o anúncio do /23 do local sob ataque – nota-se que 21 monitores que recebiam o anúncio entre 0 e 150 segundos recebem após 800 segundos, totalizando 18,26%.

Os resultados mostram a significância das conexões de tier-1 no impacto do se-

questro de prefixos e na propagação de anúncios pela Internet. Na Figura 3 se vê que, sem conexões com tier-1s, a disseminação de anúncios falsos pode acelerar e a variabilidade no tempo de atraso sugere impactos na estabilidade da rede. Assim, é vital considerar a natureza e o número das conexões que um AS mantém em análises de resiliência.

É relevante destacar a importância de estudos sobre o impacto dos sequestros de prefixos e as contramedidas. Segundo [Sermpezis et al. 2021], pesquisas foram feitas usando o PEERING Testbed e o RIS para avaliar o impacto desses sequestros, determinando qual porcentagem da Internet é afetada. Há, no entanto, uma carência de atenção a esse tema na literatura. Os autores enfatizam a necessidade de pesquisas voltadas às redes que trocam tráfego com um subconjunto específico dos ASes na Internet. Isso se relaciona ao objetivo deste artigo, que busca entender como as configurações e conexões de um AS podem influenciar no sucesso de um sequestro de prefixos.

5. Considerações Finais

Nesta pesquisa, explorou-se a interação entre o sequestro de prefixos e as conexões de um AS com seus provedores de tier-1. Identificou-se, assim, uma relação direta entre a natureza das conexões entre ASes e o desempenho de um AS sob ataque. Em uma era em que a segurança cibernética é crucial, compreender as vulnerabilidades das estruturas de conexão da Internet é essencial. Nesse contexto, destaca-se a relevância de uma visão holística da segurança de redes para o entendimento do impacto de sequestros de prefixos.

Um obstáculo deste estudo foi a escassez de plataformas para simulações. Trabalhou-se com o único provedor de trânsito que oferecia as comunidades de não exportação aos seus peers de tier-1. Esta situação sublinha a demanda por mais plataformas de experimentação em segurança de redes. Para o futuro, visa-se investigar mais sobre o sequestro de prefixos e abordar estratégias de mitigação através de ajustes de rede.

Referências

Arnold, T. et al. (2020). "Cloud Provider Connectivity in the Flat Internet". Em: Acessado em: 11 de outubro de 2023. URL: https://dl.acm.org/doi/10.1145/3419394.3423613.

CAIDA (2013). *AS Relationships*. Acessado em: 11 de setembro de 2023. URL: https://www.caida.org/catalog/datasets/as-relationships/.

Cisco (2023). *BGPStream - A free resource for receiving alerts about BGP events*. Acessado em: 09 de setembro de 2023. URL: https://bgpstream.crosswork.cisco.com/.

Gabriel Trugillo Jaeger, P. d. B. M. (2023). "Impacto do Sequestro de Prefixos em uma Rede: Como se Defender e Reverter os Efeitos?" Em: 22ª Mostra da Produção Universitária da Universidade Federal do Rio Grande - FURG. URL: https://gabrieltjaeger.github.io/papers/furg_2023_22a_mpu.pdf.

PEERING (2014). *PEERING The BGP Testbed*. Acessado em: 05 de setembro de 2023. URL: https://peering.ee.columbia.edu/.

RIPE NCC (2015). *Routing Information Service Live (RIS-Live)*. Acessado em: 05 de setembro de 2023. URL: https://ris-live.ripe.net/.

Sermpezis, P. et al. (2021). "Estimating the Impact of BGP Prefix Hijacking". Em: Acessado em: 11 de outubro de 2023. URL: https://arxiv.org/pdf/2105.02346.pdf.