Universidade Federal do Rio Grande – FURG
22ª Mostra da Produção Universitária – MPU
Rio Grande/RS, Brasil, 25 a 27 de outubro de 2023
ISSN: 2317-4420

# IMPACTO DO SEQUESTRO DE PREFIXOS EM UMA REDE: COMO SE DEFENDER E REVERTER OS EFEITOS?

TRUGILLO JAEGER, Gabriel.

MARCOS, Pedro
gabriel_jaeger@furg.br
Universidade Federal do Rio Grande – FURG

**Palavras-chave:** Sequestro de Prefixo; Sistemas Autônomos; Internet; Border Gateway Protocol (BGP); Mitigação de ataques.

## 1 INTRODUÇÃO

A Internet é uma rede global de computadores interconectados, os quais se comunicam de algum modo para trocar informações entre si. Essa rede é enorme e muito complexa, tendo em vista que todos os computadores devem ter a possibilidade de se conectar a qualquer outro na rede. Para garantir que as conexões aconteçam, são necessários mecanismos que permitam que os computadores se encontrem e se comuniquem. Esses mecanismos são chamados de protocolos de comunicação, que são conjuntos de regras que definem como os computadores devem se comunicar.

Assim como as casas, que possuem endereços residenciais e que podem ser encontradas pelos correios por meio do CEP, os computadores também possuem endereços que os identificam exclusivamente na rede: os endereços IP, que, tal qual o CEP, são compostos por números e seus dígitos possuem significados específicos. Um endereço IP – considerando a versão IPv4 – é um número de 32 bits, dividido em 4 segmentos de 8 bits. Fazendo um cálculo básico, verifica-se que existem 4.294.967.296 IPs disponíveis. Ou seja, há uma vasta quantidade de endereços. Portanto, a informação deve percorrer a malha da Internet para chegar de um ponto qualquer até outro. Sendo assim, para tornar esse percurso eficiente e geral, os Sistemas Autônomos (ASes) – que são adquiridos por organizações e que recebem um número único e blocos de IPs da Internet Assigned Numbers Authority (IANA) –, com seus respectivos blocos (ou prefixos), ao se conectarem com outros ASes, por meio de acordos firmados dinamicamente entre eles, compõe a malha da Internet. Ademais, a conexão entre ASes é padronizada pelo Border Gateway Protocol (BGP), que funciona como o "sistema de navegação"da Internet. Com o BGP instalado em seus roteadores, o AS começa a receber rotas para prefixos de outros ASes, armazenando-as em sua tabela de rotas, e a compartilhar seus prefixos para seus vizinhos por meio de anúncios que vão se propagando de vizinho em vizinho, incansavelmente, distribuindo caminhos para seus endereços por toda a Internet. Por causa do modo com que as rotas se propagam e da sua quantidade de conexões, um Sistema Autônomo pode receber mais de uma rota para o mesmo prefixo e cabe ao BGP escolher a melhor rota para ele seguindo alguns critérios, que incluem, entre outros, a especificidade do prefixo, a preferência

Universidade Federal do Rio Grande – FURG
22ª Mostra da Produção Universitária – MPU
Rio Grande/RS, Brasil, 25 a 27 de outubro de 2023
ISSN: 2317-4420

local – que é definida pelo operador de rede – e o tamanho do caminho (Cisco).

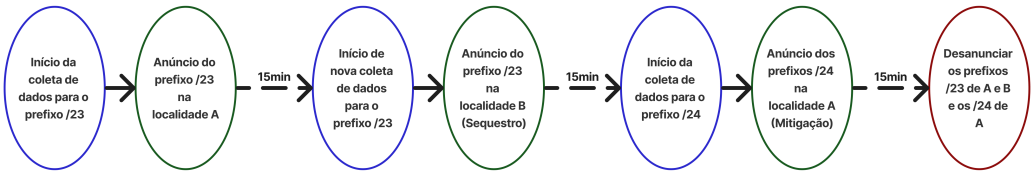
Entretanto, esta infraestrutura complexa e amplamente distribuída é suscetível a vários tipos de ataques, que incluem um evento conhecido como sequestro de prefixo (ou prefix hijacking), que ocorre quando um AS anuncia prefixos que não são seus para seus vizinhos, que, se aceitarem esses anúncios enganosos e atualizarem suas tabelas de roteamento de acordo, desviam o tráfego que deveria ir para o verdadeiro proprietário do prefixo para o AS fraudulento, podendo acarretar em consequências ruins para o AS prejudicado, como a interrupção completa do serviço, espionagem ou interceptação de dados.

Considerando o exposto, o presente trabalho visa analisar o impacto de eventos de sequestro de prefixo em ASes, medindo não só a efetividade do sequestro como a efetividade da mitigação ao anunciar o prefixo desagregado (mais específico), isto é, a efetividade da recuperação dos efeitos do evento pelo AS afetado. Busca-se, também, entender como a quantidade de conexões da rede influencia nessas variáveis. Existe relação?

## 2 METODOLOGIA

Para os experimentos, foram utilizadas para a simulação de anúncios na Internet a plataforma PEERING Testbed (PEERING 2014), que permite que sejam anunciados prefixos em ASes em determinadas regiões ou ASes com configurações distintas e, para a coleta dos dados, foi utilizada a API para o serviço RIS Live da RIPE NCC, que permite visualizar a propagação dos efeitos dos anúncios na Internet em tempo real. Sendo assim, utilizou-se as 14 redes pré-prontas disponibilizadas pelo PEERING – os multiplexadores (muxes), que são pontos de conexão ao PEERING distribuídos pelo mundo em algumas regiões –, sendo elas: Amsterdam, Clemson University, Georgia Institute of Technology (Gatech), Greek Research and Technology Network (GrNet), USC Information Sciences Institute (ISI), Northeastern University (NEU), São Paulo, Stony Brook University (SBU), Seattle, Universidade Federal De Minas Gerais (UFMG), Universidade Federal de Mato Grosso do Sul (UFMS), University of Utah, University of Washington (UW) e University of Wisconsin (WISC). Foram realizados experimentos em pares para todas as combinações possíveis de muxes, totalizando 182 rodadas. Cada rodada seguiu o esquema apresentado na Figura 1:

Figura 1: Esquema das rodadas de experimentos.



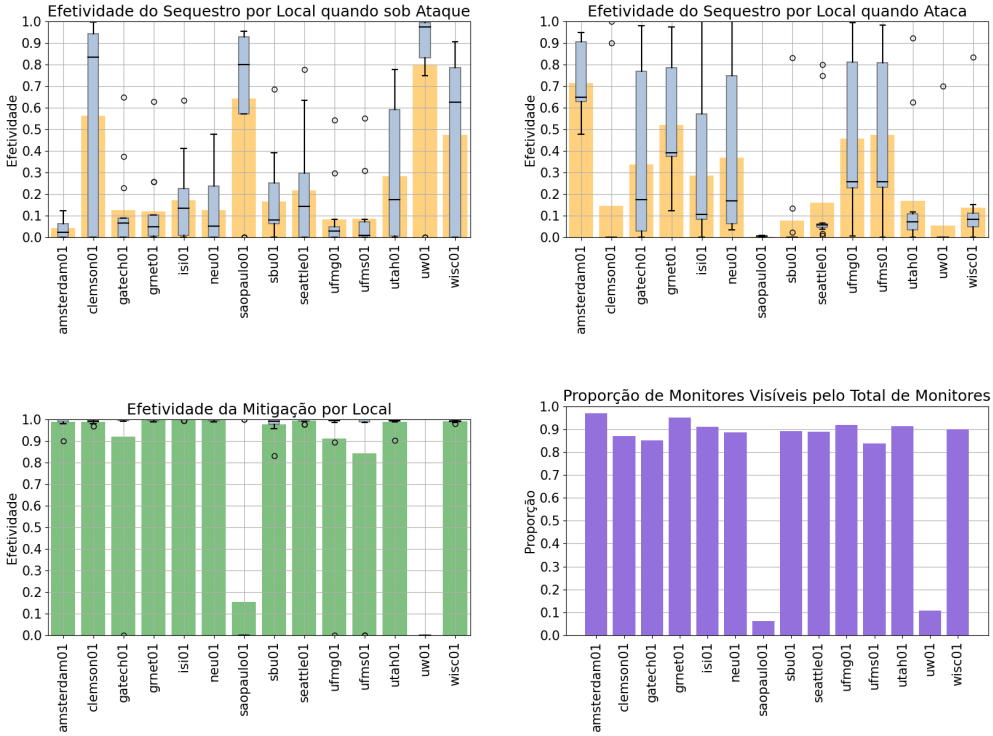

Fonte: O autor.

ISSN: 2317-4420

As rodadas de experimentos foram executadas do dia 15/06/2023 ao 21/06/2023 para cada um dos pares, com exceção dos pares que envolviam as regiões de São Paulo e da UFMS, que foram realizadas mais tarde, de 17/07/2023 a 19/07/2023. Ademais, Os prefixos utilizados foram: 184.164.226.0/23 e 184.164.226.0/24. E, o AS Number de origem do atacante é 263842 e do atacado é 47065.

## 3 RESULTADOS E DISCUSSÃO

Figura 2: Efetividade média e boxplots do sequestro de prefixos por Mux.




Fonte: O autor.

Os gráficos da Figura 2 mostram que diferentes regiões apresentaram resultados diferentes. Observa-se que em Amsterdam, por exemplo, quando a região tinha seu prefixo sequestrado, ou seja, estava sob "ataque", a efetividade do sequestro foi baixa e, quando o evento se originava em Amsterdam e afetava as outras regiões, a efetividade média foi a mais alta em comparação com outras regiões. Portanto, Amsterdam se defende bem e causa grandes danos se sequestrar um prefixo.

As diferenças observadas entre as regiões sugerem que diversos fatores podem estar influenciando a efetividade do sequestro de prefixos. Estes, supõe-se, podem incluir a configuração específica da rede, o número e a natureza das conexões que ela possui e, possivelmente, outros fatores ainda não identificados. Para responder a essa questão, serão necessárias análises adicionais. Sendo assim, planejamos examinar não só a relação entre a efetividade do sequestro de prefixos e as medidas de co-

ISSN: 2317-4420

nectividade de rede: número de provedores, de pares e de consumidores dos ASes, bem como a distribuição dessas conexões e, possivelmente, outras características de rede. Espera-se que análises futuras ajudem a esclarecer o comportamento das redes quando submetidas a eventos de sequestro de prefixos.

Por outro lado, os dados mostram que a efetividade de mitigação não variou significativamente entre as regiões. Como esperado, com a técnica de anúncio de prefixo mais específico, a maioria das regiões demonstrou uma efetividade de mitigação acima de 90%, com a exceção notável das regiões de São Paulo e da University of Washington, que apresentaram efetividades de 15,4% e 0%, respectivamente, o que parece estar relacionado com a visibilidade média dos monitores durante a captura. Nessas redes, a visibilidade média dos monitores foi de apenas 6,1% e 10,6%, respectivamente, significativamente menor do que nas outras regiões, o que reduz a confiabilidade dos dados apresentados para essas localidades específicas.

## 4 CONSIDERAÇÕES FINAIS

Por fim, embora os resultados até agora sejam preliminares, eles destacam a complexidade do problema do sequestro de prefixos e a necessidade de mais pesquisas para entender e combater tal problema, garantindo a segurança da Internet, que é uma preocupação constante, tendo em vista o avanço contínuo das tecnologias e das ameaças de segurança de redes. Espera-se que em futuros trabalhos se possa contribuir ainda mais na compreensão e na busca de soluções para problemas envolvendo a segurança de redes. Ademais, é importante reparar que o uso de prefixos mais específicos no combate a eventos de sequestro de prefixos já foi explorado em outros trabalhos, como em (Sermpezis et al. 2016), que reforçam que, apesar de efetiva, a desagregação de prefixos mais específicos que /24 faz com que sejam filtrados pela maioria dos roteadores. Além de que, para acomodar um prefixo mais específico, é necessário ocupar mais espaço na tabela de rotas, podendo sobrecarregar o AS em questão.

## REFERÊNCIAS

Cisco. **Select BGP Best Path Algorithm**. Acessado em: 28 de julho de 2023. Disponível em: <https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13753-25.html>.

PEERING. **PEERING The BGP Testbed**. 2014. Acessado em: 17 de julho de 2023. Disponível em: <https://peering.ee.columbia.edu/>.

RIS Live. **Routing Information Service (RIS)**. Acessado em: 17 de julho de 2023. Disponível em: <https://ris-live.ripe.net/>.

SERMPEZIS, P. et al. Monitor, detect, mitigate: Combating bgp prefix hijacking in real-time with artemis. 2016. Acessado em: 25 de julho de 2023. Disponível em: <https://arxiv.org/pdf/1609.05702.pdf>.