Caracterização da Vulnerabilidade a Sequestros de Prefixo de Sistemas Autônomos Militares

Adriano B. Carvalho[1,2], Pedro de B. Marcos[3], Fabrício S. de Paula[4], Carlos Alberto da Silva[1], Ronaldo A. Ferreira[1]

[1] Universidade Federal de Mato Grosso do Sul (UFMS)

[2]Exército Brasileiro (EB)

[3]Universidade Federal do Rio Grande (FURG)

[4]Universidade Estadual de Mato Grosso do Sul (UEMS)

bastos.adriano@eb.mil.br, pbmarcos@furg.br, fabricio@comp.uems.br
carlos.silva@ufms.br, ronaldo.ferreira@ufms.br

Abstract. *The cyber domain has become a new front for attacks, as observed in recent conflicts. Although the military employs segregated networks for tactical communications, the use of the Internet for certain services makes them vulnerable to attacks, including prefix hijacking. Current protection tools against prefix hijacking are insufficient or can be easily bypassed. This study uses an extensive set of simulations with real-world data to characterize the vulnerability of 29 military networks to prefix hijacking, revealing that networks with higher connectivity and geographically distributed neighbors are less affected. However, up to 77% of attacks can go undetected, even with the best tool currently available for detecting forged-origin hijacks. The study also explores ways to enhance the routing system's robustness for these networks.*

Resumo. *O campo cibernético tornou-se uma nova frente de ataques, como observado em conflitos recentes. Embora os militares utilizem redes segregadas para comunicações táticas, o uso da Internet para alguns serviços os torna vulneráveis a ataques, incluindo o sequestro de prefixo. As ferramentas atuais de proteção contra sequestros de prefixo são insuficientes ou podem ser facilmente burladas. Este trabalho utiliza um conjunto extensivo de simulações, com dados reais, para caracterizar a vulnerabilidade a sequestros de prefixo de 29 redes militares, revelando que redes mais conectadas e com vizinhos distribuídos geograficamente são menos afetadas. Entretanto, até 77% dos ataques podem passar despercebidos, mesmo com a melhor ferramenta disponível para detectar sequestros com origem forjada. O trabalho também discute possibilidades para tornar o sistema de roteamento dessas redes mais robusto.*

1. Introdução

Sistemas de comunicação militares são cruciais para a segurança e soberania de uma nação. Em cenários críticos, as Forças Armadas mantêm infraestruturas segregadas e isoladas da Internet. No entanto, para oferecer serviços ou interagir com a população e seus membros, disponibilizam sistemas acessíveis pela Internet, como serviços de alistamento, gestão de informações e acesso interno via VPN para militares em missões externas. Essa exposição, contudo, os torna potenciais alvos de ataques cibernéticos. Por exemplo, conflitos globais recentes, como a guerra Rússia-Ucrânia, as tensões entre Israel e Hamas e

disputas no Oriente Médio, evidenciam essa ameaça. Recentemente, a Rússia conduziu ataques cibernéticos contra a Ucrânia antes de ações militares [Suzuki 2022]. No conflito entre Israel e Hamas, ambos os lados enfrentam ofensivas cibernéticas de grupos de *hackers* ativistas [Palmeira 2023], evidenciando um campo de batalha sem fronteiras claras. Assim, identificar e mitigar vulnerabilidades nesses sistemas é essencial para assegurar a segurança e a soberania nacionais.

Uma ameaça significativa aos sistemas militares é o ataque de sequestro de prefixo. Nesse cenário, um atacante busca interceptar o tráfego direcionado para a rede da vítima anunciando rotas falsas com o protocolo BGP (Border Gateway Protocol) [Holterbach et al. 2024], o protocolo de roteamento interdomínio da Internet [Rekhter et al. 2006]. Se o ataque for bem-sucedido, o atacante pode tanto inspecionar o tráfego destinado à vítima, atuando como *man-in-the-middle*, como também torná-lo inacessível, em um ataque de negação de serviço (DoS, *Denial of Service*).

Estudos recentes indicam que mais de uma dezena de sequestros de prefixo ocorrem diariamente, com um aumento contínuo ao longo dos anos [Moll 2020, Holterbach et al. 2024]. Porém, esse número pode ser significativamente superior, pois muitos sequestros não são visíveis nos coletores públicos de rotas BGP que são utilizados para detecção de sequestros e também não são publicamente reportados pelas vítimas. Esses incidentes são amplamente atribuídos à falta de mecanismos de segurança no protocolo BGP [Holterbach et al. 2024]. Além disso, os mecanismos de segurança propostos para BGP [Bush and Austein 2017, Lepinski and Sriram 2017, Azimov et al. 2025] possuem baixa adoção e são vulneráveis a manipulações. Por exemplo, RPKI [Bush and Austein 2017], atualmente a técnica mais implementada, cobre apenas cerca de 51% dos endereços IPv4 e IPv6 da Internet [NIST 2024] e pode ser facilmente contornada por atacantes.

Este trabalho apresenta a primeira caracterização da vulnerabilidade da infraestrutura de roteamento das redes militares das principais economias globais contra ataques de sequestro de prefixo. Para isso, três abordagens foram empregadas. A primeira consiste no desenvolvimento de um simulador para avaliar a vulnerabilidade das redes militares contra ataques de sequestro de prefixo. Já a segunda consiste na análise de dados públicos de roteamento, que também foram usados para a construção do simulador, para entender as atuais práticas de roteamento das redes militares e estimar suas vulnerabilidades. Ao longo dessas etapas, foram analisados dados coletados em 530 pontos de observação entre os meses de fevereiro e abril de 2024, que totalizam mais de 735 milhões de rotas por dia. Por fim, a terceira avalia a efetividade dos recursos existentes para detecção de sequestros em situações de ataques realistas a redes militares.

Por ser uma infraestrutura crítica para a segurança e soberania de um país, a caracterização da vulnerabilidade de uma rede militar a sequestros de prefixo contribui em várias dimensões: *(i)* compreensão da gravidade do problema; *(ii)* identificação de padrões e tendências; *(iii)* proposição de medidas de mitigação; *(iv)* avaliação da eficácia de mecanismos de segurança; *(v)* apoio à tomada de decisão; *(vi)* impacto na segurança e estabilidade da Internet. As principais contribuições deste trabalho são:

- Desenvolvimento de um simulador de sequestros de prefixo, utilizado para gerar todos os dados das análises apresentadas e disponibilizado publicamente (§ 3).

- Análise da capacidade de contaminação da Internet por sequestros de prefixo em três cenários distintos, destacando características das vítimas que influenciam a contaminação (§ 4.1).
- Verificação, com dados atualizados, da capacidade dos coletores públicos de rota em observar os sequestros simulados e identificação dos tipos de sequestros mais propensos a passar despercebidos (§ 4.2).
- Identificação das características que tornam um AS mais resiliente a sequestros de prefixo (§ 4.3).
- Avaliação do impacto do uso da técnica de *prepend* na origem de rotas para engenharia de tráfego em casos de sequestro de prefixo (§ 4.4).
- Avaliação da capacidade da principal ferramenta de detecção de sequestros com origem forjada em identificar sequestros simulados para ASes militares (§ 4.5).

Aspectos éticos. As análises foram realizadas exclusivamente com dados públicos de roteamento. Os impactos de possíveis sequestros de prefixo foram avaliados por meio de simulações, sem qualquer interferência nas redes estudadas. Para preservar a privacidade e evitar a exposição de vulnerabilidades, as redes analisadas foram anonimizadas.

2. Roteamento Interdomínio e Sequestros de Prefixo

Sistemas Autônomos (AS, do inglês *Autonomous System*) trocam informações de roteamento usando o protocolo BGP [Rekhter et al. 2006]. A construção de uma rota BPG inicia quando um AS anuncia um prefixo IP aos seus vizinhos, que é propagada por meio de mensagens de atualização. O caminho até a origem é registrado no *AS path*, uma sequência de ASNs (*Autonomous System Numbers*) que é utilizada para prevenir loops de roteamento e na escolha da melhor rota. O BGP seleciona a rota com base, em ordem, na preferência local (LocalPref), comprimento do *AS path*, origem da rota e outros critérios de desempate [Rekhter et al. 2006].

Embora a Internet tenha se tornado uma infraestrutura crítica para a sociedade, ela foi concebida sem mecanismos nativos de segurança tanto no plano de dados [Fonseca et al. 2020] como no plano de controle [Holterbach et al. 2024]. BGP, por exemplo, foi concebido sem mecanismos nativos de autenticação e validação das informações de rota trocadas [Holterbach et al. 2024]. Como consequência, ele é vulnerável a manipulações arbitrárias nos anúncios de rota, incluindo mudanças no *AS path*. O sequestro de prefixo, por exemplo, é um ataque que explora essa vulnerabilidade, em que o atacante passa a divulgar um prefixo pertencente a outro AS para seus vizinhos para redirecionar o tráfego para sua rede [Holterbach et al. 2024]. Assim, o sequestrador pode tanto atuar como *man-in-the-middle* e inspecionar e/ou alterar pacotes, quanto descartá-los e ocasionar negação de serviço, possibilidades ilustradas na Figura 1.

Um sequestro de prefixo pode ser classificado como de Tipo-0 ou de Tipo-X [Sermpezis et al. 2018b]. O sequestro de Tipo-0 ocorre quando o sequestrador se passa pelo proprietário do prefixo, colocando seu AS como a origem do anúncio. Quando o sequestrador forja o *AS path*, inserindo outros ASes antes do seu no anúncio, ocorre um sequestro de Tipo-X, em que X corresponde à quantidade de ASes inseridos antes do AS do sequestrador. Por exemplo, quando o sequestrador insere no *AS path* apenas o AS proprietário do prefixo antes do seu, ocorre um sequestro de Tipo-1.

Considerando a relevância e prevalência de sequestros de prefixo, foram desen-

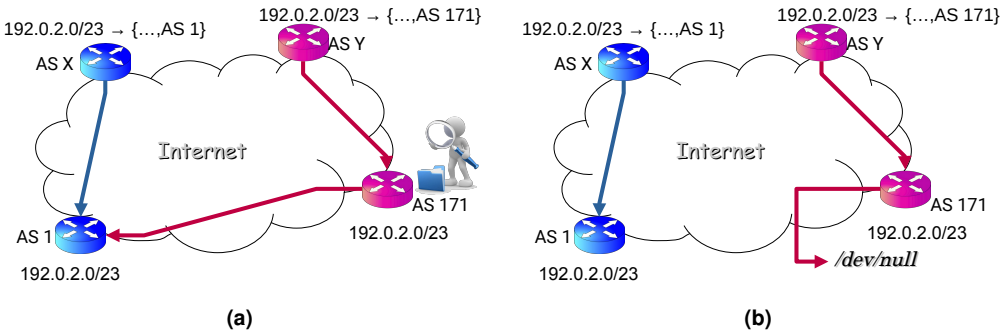

Figura 1. Ilustração de sequestros de prefixo. Em (a), o sequestrador (AS 171) recebe pacotes com destino ao prefixo sequestrado (192.0.2.0/23) da vítima (AS 1) oriundo do AS contaminado (AS Y), analisa e/ou altera os pacotes e os encaminha à vítima (*man-in-the-middle*). Em (b), o sequestrador descarta os pacotes, causando a negação do serviço.

volvidos alguns mecanismos de segurança para mitigá-los, destacando-se:

- RPKI (*Resource Public Key Infrastructure*) [Bush and Austein 2017], que é uma infraestrutura de chaves públicas para validar a origem de um prefixo. O seu funcionamento consiste em duas etapas principais: a ROA (*Route Origin Authorization*), em que um AS autoriza via assinatura digital quem pode anunciar seus prefixos; e a ROV (*Route Origin Validation*), realizada por ASes ao receber o anúncio de um prefixo, buscando validar o prefixo com sua origem no *AS path*.
- BGPSec [Lepinski and Sriram 2017], que utiliza assinatura digital para garantir a integridade do *AS path*. A implementação de BGPSec é difícil porque exige a assinatura do *AS path* por todos os ASes no caminho para garantir sua integridade.
- ASPA (*Autonomous System Provider Authorization*) [Azimov et al. 2025], que aproveita RPKI para validar as ligações entre ASes. Os ASes devem utilizar RPKI para divulgar suas conexões, permitindo que outros ASes validem as conexões presentes nos *AS paths*.

Apesar da existência desses mecanismos de segurança, a proteção efetiva de BGP só será alcançada com uma ampla implementação, algo que ainda enfrenta obstáculos significativos. Os principais desafios incluem os custos operacionais relacionados à capacitação de operadores e à atualização de equipamentos, devido ao aumento das demandas de processamento para suportar criptografia [Sermpezis et al. 2018a].

Entre as técnicas disponíveis, RPKI é atualmente a mais adotada, cobrindo 49% dos prefixos IPv4 e 51,8% dos IPv6 com ROA até abril de 2024 [NIST 2024]. No entanto, essa solução não é infalível, pois ataques que manipulam o *AS path* podem incluir o AS legítimo de forma forjada no início do caminho (sequestro do Tipo-1), levando ROV a validar incorretamente a origem do anúncio contendo o sequestro.

A maioria dos estudos sobre detecção de sequestros de prefixo baseia-se em dados de coletores públicos de rotas BGP. Os projetos Route Views [Meyer 1997] e RIPE RIS [Mcgregor et al. 2010] oferecem gratuitamente atualizações de BGP e RIBs (*Routing Information Base*) de roteadores em diversos pontos da Internet, com dados históricos e atualizações quase em tempo real. Os coletores recebem informações de BGP de diferentes ASes, que são armazenadas e disponibilizadas em sites públicos dos projetos. Este

trabalho utiliza dados de ambos os projetos.

3. Simulação de Roteamento Interdomínio e Sequestros de Prefixo

Este trabalho simula cenários de sequestro de prefixo utilizando um simulador que desenvolvemos e disponibilizamos publicamente em [Carvalho et al. 2025]. As simulações utilizam dados do grafo de relacionamentos da CAIDA [CAIDA 2015] para os meses de fevereiro, março e abril de 2024, abrangendo 76.421, 76.556 e 76.649 ASes, respectivamente. Os tipos de relacionamento entre os ASes (cliente-provedor (c2p) e *peer-to-peer* (p2p)) também são extraídos dos grafos da CAIDA. Apesar de não ser perfeito, o grafo da CAIDA é considerado a melhor fonte de relacionamento entre ASes na Internet e é frequentemente utilizado em estudos desta natureza [Milolidakis et al. 2023].

O simulador aplica uma versão simplificada, mas realista, do processo de decisão do BGP para selecionar a melhor rota para um prefixo. Cada AS escolhe a melhor rota seguindo os critérios: *(i)* maior atributo de preferência local; *(ii)* em caso de empate, a rota com o menor *AS path*; *(iii)* persistindo o empate, a primeira rota recebida. As preferências locais são determinadas pelo modelo Gao-Rexford [Gao and Rexford 2001], que reflete as relações comerciais entre ASes: rotas de clientes são preferidas sobre rotas de *peers*, que, por sua vez, têm prioridade sobre rotas de provedores. A propagação de rotas também segue o modelo Gao-Rexford: rotas recebidas de clientes são propagadas para todos os vizinhos, enquanto rotas de *peers* ou provedores são propagadas apenas para clientes.

Para melhor representar a realidade da Internet, as rotas analisadas são aquelas observadas nos ASes que exportam rotas para os coletores dos projetos RIPE-RIS [Mcgregor et al. 2010] e Route Views [Meyer 1997], que são chamados de *pontos de observação* (*vantage points*). Os ASNs desses ASes foram obtidos diretamente nos sites desses projetos, totalizando 811, 813 e 815 ASes nas simulações de fevereiro, março e abril de 2024, respectivamente. Informações adicionais sobre os ASes, como descrição e país, foram coletadas do *CIDR Report* [Philip Smith 2021] em outubro de 2024. Além disso, na análise do impacto de um sequestro envolvendo um AS vítima que implementa ROA, a validação de origem com ROV é simulada apenas para ASes com *score* superior a 0,25, conforme os dados do estudo [Li et al. 2023] na mesma data ou na mais próxima disponível dos dados utilizados. O *score* de cada AS foi obtido do mesmo estudo [Li et al. 2023] e indica a chance do AS rejeitar um anúncio inválido. Por exemplo, um AS com *score* igual a um valida com ROV todos os anúncios que possuam ROA.

3.1. Cenários das Simulações

Nas simulações, as vítimas de sequestro são ASes utilizados pelas Forças Armadas dos países do G20 ou ASes que anunciam prefixos pertencentes a essas entidades (*e.g.,* provedores de nuvem). Foram selecionados 29 ASes, distribuídos da seguinte forma: África do Sul (1), Alemanha (1), Arábia Saudita (1), Argentina (1), Austrália (2), Brasil (4), Canadá (1), China (1), Coreia (1), Estados Unidos (8), Índia (1), Indonésia (2), Itália (1), Japão (2), Rússia (1) e Turquia (1). Os ASNs desses ASes foram identificados por consultas em páginas de acesso público [Electric 2024] com os termos “Exército”, “Marinha”, “Força Aérea” e “Departamento de Defesa”, no idioma de cada país. Além disso, foi realizada a resolução de nomes de páginas oficiais dessas Forças Armadas para endereços IP e a determinação do AS dono do endereço com a ferramenta `whois`.

Tabela 1. Caracterização dos vizinhos dos ASes vítimas em abril de 2024.

	AA	AB	AC	AD	AE	AF	AG	AH	AI	AJ	AK	AL	AM	AN	AO
Vizinhos	1	1	1	1	1	1	1	1	2	2	2	2	2	2	4
Países	1	1	1	1	1	1	1	1	1	1	2	1	2	1	1
Continentes	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1
Clientes	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Peers	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Provedores	0	1	1	1	1	1	1	1	2	2	2	2	2	2	4

	AP	AQ	AR	AS	AT	AU	AV	AW	AX	AY	AZ	BA	BB	BC	
Vizinhos	5	7	7	7	16	17	31	32	40	73	276	597	1518	1765	
Países	1	1	1	1	1	1	1	10	12	3	46	31	92	142	
Continentes	1	1	1	1	1	1	1	3	4	1	5	5	5	5	
Clientes	3	4	6	1	0	15	30	0	0	70	3	389	1462	660	
Peers	0	0	0	4	15	0	0	30	25	0	226	200	56	848	
Provedores	2	3	1	2	1	2	1	2	15	3	47	8	0	257	

Os ASes vítimas variam desde aqueles com apenas um vizinho até ASes com mais de 1.700 vizinhos. A Tabela 1 apresenta as características desses ASes com base nos relacionamentos registrados pela CAIDA para abril de 2024, incluindo o número total de vizinhos, países e continentes envolvidos e vizinhos por tipo de relacionamento.[1] Entre as vítimas está o AS BC, vinculado a um grande serviço de hospedagem que também abriga sistemas de uma das Forças Armadas do G20. Essa relação foi confirmada pela resolução de nomes de páginas oficiais, cujo endereço IP é propriedade do AS BC.

Os sequestradores foram selecionados aleatoriamente, totalizando 600 ASes por data de simulação, distribuídos em quatro grupos baseados no número de vizinhos para garantir a inclusão de ASes de diferentes tamanhos. A seleção incluiu 150 ASes de cada grupo, com os sequestradores permanecendo os mesmos para todas as simulações de uma mesma data. A composição dos grupos e o número de ASes em cada um nos primeiros dias de fevereiro, março e abril de 2024 são as seguintes:

- Grupo 0 (G0): ASes com dois vizinhos (22.675, 22.782 e 22.530 ASes);
- Grupo 1 (G1): ASes com três vizinhos (7.274, 7.345 e 7.444 ASes);
- Grupo 2 (G2): ASes com quatro a dez (8.721, 8.661 e 8.807 ASes);
- Grupo 3 (G3): ASes com 11 vizinhos ou mais (9.801, 9.788 e 9.904 ASes).

Os ASes com apenas um vizinho (*stub*) não foram selecionados como sequestradores por não se observar sequestros maliciosos noticiados tendo como sequestrador um AS desse tipo. Além disso, um AS *stub* é incapaz de realizar sequestros de interceptação de tráfego por não possuir caminho alternativo para repasse dos dados para a vítima.

Por fim, todos os sequestros são realizados para prefixos com o mesmo comprimento dos da vítima, pois anúncios de prefixos mais ou menos específicos se propagariam por toda a Internet, inviabilizando análises específicas, como a visibilidade nos coletores.

4. Resultados Obtidos

Foram realizados três tipos de simulações para cada AS vítima e sequestrador: sequestros Tipo-0, Tipo-1 e Tipo-0 com ROV, simulando a validação de origem por RPKI. As simulações utilizaram dados de roteamento do primeiro dia de fevereiro, março e abril de 2024. Os resultados obtidos e suas respectivas análises são detalhados a seguir.

[1]Um AS sem provedor é Tier-1 e o outro possui ligação com um *sibling* que lhe provê trânsito.

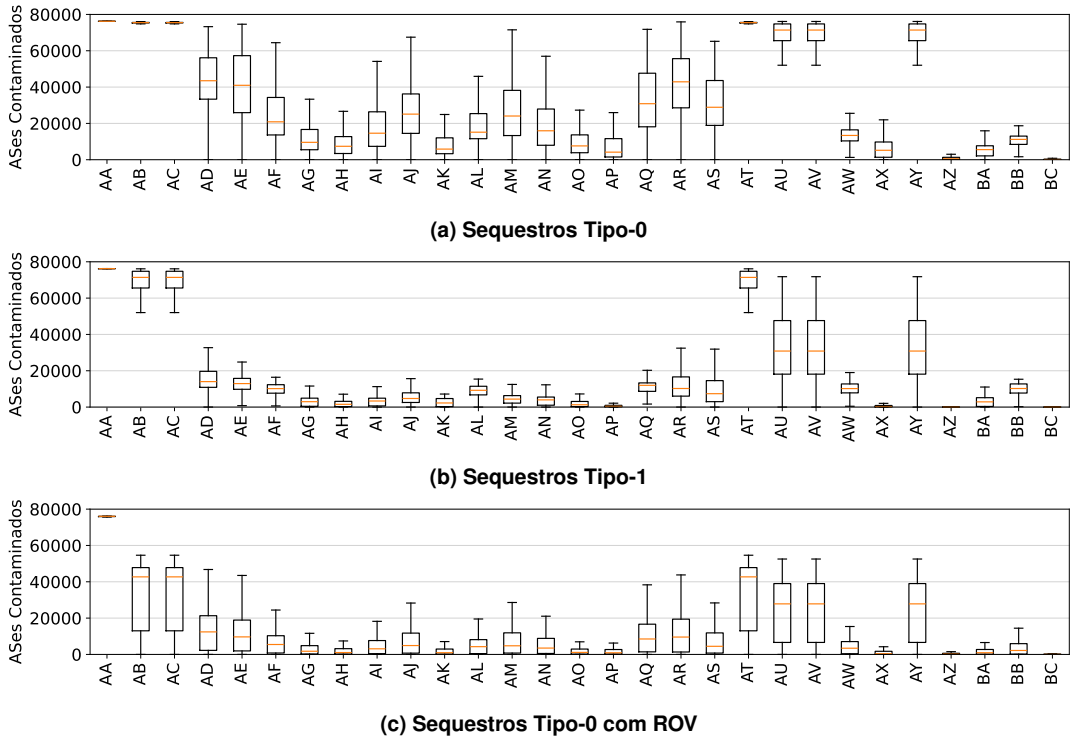

Figura 2. Quantidade de ASes contaminados para os 600 sequestros simulados por vítima para os dados referentes ao mês de abril de 2024.

4.1. Contaminação dos ASes pelo Sequestro

A primeira análise avaliou a capacidade de contaminação das tabelas de roteamento dos ASes da Internet por tipo de sequestro. A Figura 2 mostra o número de ASes afetados por sequestros de Tipo-0 (a), Tipo-1 (b) e Tipo-0 com ROV ativo (c). Os ASes estão organizados na figura pela quantidade de vizinhos, conforme a ordem da Tabela 1. Os resultados apresentados referem-se a abril de 2024, com padrões similares observados em fevereiro e março. O sequestro Tipo-0 exibiu a maior capacidade de contaminação, como esperado, contaminando uma média de 31.117 (40,7%) ASes por sequestro. Sequestros Tipo-1 contaminaram menos, pois o *AS path* maior no anúncio inicial reduz sua preferência quando o tamanho do *AS path* é usado como critério de escolha, contaminando em média 17.094 (22,3%) ASes por sequestro. O sequestro Tipo-0 com ROV teve o menor impacto, devido ao descarte da rota sequestrada por ASes que realizam validação de origem, contaminando em média 11.398 (14,9%) ASes por sequestro. Além do tipo de sequestro, fatores como o número de vizinhos do AS vítima, o tipo de conexão e a dispersão geográfica dos vizinhos influenciaram significativamente o alcance da contaminação.

Os ASes AA, AB, AC e AT foram consistentemente os mais afetados pelos sequestros. Suas características comuns incluem poucas conexões com provedores e vizinhos concentrados em um único país. Por outro lado, os ASes AZ e BC foram os menos impactados, devido à grande quantidade de vizinhos, principalmente provedores, e à diversidade geográfica desses vizinhos.

Outro fator relevante para o alcance de um sequestro é a conectividade do sequestrador. A Tabela 2 mostra que os sequestros provenientes de ASes do Grupo 3 (G3) apre-

sentaram o maior alcance, pois esses sequestradores anunciaram o prefixo sequestrado por múltiplos caminhos em diferentes pontos da Internet.

Tabela 2. Média (μ) de contaminação dos sequestros, em valores absolutos e percentuais, por data, tipo de sequestro, grupo do sequestrador e geral.

Data	Tipo-0					Tipo-1					Tipo-0+ROV				
	μ	G0	G1	G2	G3	μ	G0	G1	G2	G3	μ	G0	G1	G2	G3
Fev	30457	27128	29015	31267	34417	16549	14451	15677	17087	18979	10565	7252	9563	11526	13917
2024	39,9%	35,5%	38,0%	40,9%	45,0%	21,7%	18,9%	20,5%	22,4%	24,8%	13,8%	9,5%	12,5%	15,1%	18,2%
Mar	31517	27675	29611	32529	36254	17279	15158	16121	17880	19957	11344	8418	9432	12616	14909
2024	41,2%	36,2%	38,7%	42,5%	47,4%	22,6%	19,8%	21,1%	26,4%	26,1%	14,8%	11,0%	12,3%	16,5%	19,5%
Abr	31376	27091	29992	32183	36239	17453	15058	16562	17860	20333	12285	8113	10802	13403	16824
2024	40,9%	35,3%	39,1%	42,0%	47,3%	22,8%	19,6%	21,6%	23,3%	26,5%	16,0%	10,6%	14,1%	17,5%	21,9%
μ	31117	27298	29539	31993	35636	17094	14889	16120	17609	19756	11398	7928	9932	12515	15217
Global	40,7%	35,7%	38,6%	41,8%	46,6%	22,3%	19,5%	21,1%	23,0%	25,8%	14,9%	10,4%	13,0%	16,3%	19,9%

4.2. Visibilidade dos Sequestros nos Coletores Públicos de Rota

As simulações permitiram analisar a quantidade de sequestros que não alcançaram nenhum ponto de observação e, consequentemente, não teriam visibilidade nos coletores públicos. Os sequestros de Tipo-0 com ROV foram os que mais produziram sequestros não observados, o que ocorre por, normalmente, contaminarem menos ASes na Internet. A simulação com dados de 01/02/2024 do sequestro de Tipo-0 com ROV foi a que gerou o maior número de sequestros não visualizados, totalizando 3.255 (18,71%) de 17.400 sequestros simulados (150 sequestros por cada um dos quatro grupos e 29 vítimas). O sequestro de maior impacto não detectado contaminou as tabelas de roteamento de 2.402 ASes de um total de 76.556, representando 3,14% da Internet simulada com dados de 01/03/2024. A maior média de ASes contaminados não observados foi de 135, registrada para sequestros Tipo-0 e com dados de 01/03/2024. Os resultados detalhados por data e por tipo de sequestro estão na Tabela 3.

Tabela 3. Total de sequestros não observados por tipo e data, incluindo o sequestro com maior contaminação (percentual de ASes da Internet afetados) e a média de ASes contaminados.

Dados da Simulação	Tipo	Não Observados	Maior Contaminação	Média de Contaminados
01-02-2024	0	336 (1,93%)	2170 (2,84%)	125
01-02-2024	1	1089 (6,26%)	846 (1,11%)	47
01-02-2024	0 + ROV	3255 (18,71%)	1663 (2,18%)	38
01-03-2024	0	313 (1,80%)	2402 (3.14%)	135
01-03-2024	1	972 (5,59%)	1354 (1,77%)	32
01-03-2024	0 + ROV	3038 (17,46%)	1739 (2,27%)	29
01-04-2024	0	326 (1,87%)	842 (1,10%)	91
01-04-2024	1	926 (5,32%)	900 (1,17%)	27
01-04-2024	0 + ROV	2869 (16,49%)	925 (1,21%)	27

Segundo [Sermpezis et al. 2018b], sequestros que contaminam mais de 2% da Internet são observados nos coletores. No entanto, algumas simulações deste trabalho mostraram sequestros que afetaram mais de 3% dos ASes sem serem observados. Essa discrepância pode ser atribuída ao aumento das conexões entre ASes nos últimos anos. Comparando os dados de número de ASes e relacionamentos entre ASes, utilizados em [Sermpezis et al. 2018b], com os dados mais recentes deste trabalho de abril de 2024, observa-se que, enquanto o número de ASes aumentou em 34,4% (de 57.027 para 76.649), o número de ASes com mais de mil vizinhos aumentou em 59,3% (de 91 para

145) e o maior número de vizinhos de um AS aumentou em 50,3% (de 6.488 para 9.754). Além disso, a seleção de sequestradores com alta conectividade (Grupo 3) pode ter contribuído para a maior contaminação sem visibilidade nos coletores. Essa diferença nos resultados também reflete limitações da avaliação em [Sermpezis et al. 2018b], que não detalha os critérios de seleção de vítimas e sequestradores.

4.3. Resiliência das Vítimas ao Sequestro de Prefixo

A resiliência de um AS a sequestros de prefixo mede a proporção de tráfego destinado à vítima que permanece inalterada durante um ataque. Em termos práticos, indica a porcentagem de ASes na Internet que provavelmente não será afetada quando um determinado AS for a vítima. Conforme [Birge-Lee et al. 2022], a resiliência de um AS (R_{AS}) é calculada como a média das resiliências individuais de cada sequestro (R_s), dividindo o somatório das resiliências pelos sequestros simulados (Q_{ss}). A resiliência de um AS a um sequestro específico (R_s) é definida como:

$$R_s = \frac{\text{ASes não contaminados} - 2}{\text{Total de ASes} - 2} = \frac{ASes_{nc} - 2}{T_{ASes} - 2},$$

o valor 2 é subtraído para excluir o sequestrador e a vítima do cálculo. A resiliência total, portanto, é dada por $R_{AS} = \frac{\sum R_s}{Q_{ss}}$. Neste trabalho, a resiliência foi calculada utilizando os resultados dos três tipos de sequestros simulados: Tipo-0, Tipo-1, Tipo-0 com ROV, conforme descrito na Seção 3. A Figura 3 apresenta a resiliência por AS para as simulações com os dados de 01/04/2024.

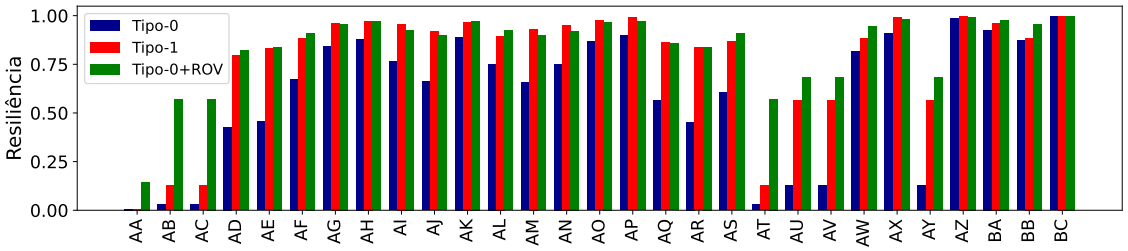

Figura 3. Resiliência de cada AS de acordo com o tipo de sequestro e com simulações realizadas com dados de abril de 2024.

Atualmente, não existe uma técnica amplamente implementada capaz de bloquear a propagação de sequestros com *AS path* forjado. No entanto, como mostrado na Figura 3, os ASes demonstram maior resiliência a sequestros de Tipo-1 em comparação aos de Tipo-0. Essa maior resiliência ocorre porque o *AS path* em um sequestro de Tipo-1 é mais longo no início pela adição do ASN da vítima como origem, o que o coloca em desvantagem no critério de desempate baseado no comprimento do *AS path*.

O uso correto de ROA+ROV pode aumentar significativamente a resiliência de um AS contra sequestros de Tipo-0, como observado em [Madory 2022]. Por exemplo, a resiliência dos ASes AU, AV, e AY aumenta de 0,1271 para 0,6817, um incremento de 0,5546. O menor aumento foi observado no AS BC, com resiliência subindo de 0,9948 para 0,9978. Entre os 29 ASes analisados, apenas 13 possuem ROA configurada, e apenas oito a aplicam para todos os seus prefixos. Em 01/04/2024, cerca de 49% dos prefixos IPv4 e 51,8% dos IPv6 eram validados pela ROV [NIST 2024], indicando a necessidade

de maior adoção. Com base na resiliência dos ASes (Figura 3) e nas características dos seus vizinhos (Tabela 1), pode-se concluir que:

- ASes bem conectados: Aqueles com mais provedores e maior distribuição geográfica são mais resilientes, como AZ, BA, BB e BC;
- ASes com poucos provedores: Mesmo com muitos enlaces *peer-to-peer*, tendem a ser menos resilientes, como o AS AT;
- ASes com baixa conectividade: Dependem da conectividade dos vizinhos, especialmente provedores, para maior resiliência. Por exemplo, o AS AH, com apenas um provedor, alcança uma resiliência de 0,8792 para o sequestro Tipo-0 porque seu provedor possui 2.992 vizinhos em 112 países diferentes.

4.4. Impacto de *Prepend* em Sequestros

Os resultados das Seções 4.1-4.3 basearam-se em simulações de rotas propagadas sem técnicas de engenharia de tráfego. Analisando as RIBs disponibilizadas pelos coletores em 01/04/2024, observou-se o uso significativo de *prepend* nas rotas anunciadas pelos ASes vítimas. Esta técnica consiste em aumentar artificialmente o comprimento do *AS path* repetindo uma ou mais vezes o ASN do AS realizando *prepend* [Barreto et al. 2024]. Essa técnica é usada para priorizar ou despriorizar determinados vizinhos na entrada do tráfego, mas pode facilitar sequestros de prefixo, já que anúncios legítimos com *prepend* tendem a ser preteridos devido ao maior *AS path* [Marcos et al. 2020].

Em 01/04/2024, todos os ASes militares da Tabela 1 tinham anúncios com *prepend*, e alguns aplicavam a técnica na origem. As rotas do AS AD foram as que mais apresentaram *prepend*, com 79,76% dos anúncios. Entre os ASes que implementaram *prepend* na origem, destacam-se AO (68,82% dos anúncios), seguido por AJ, AZ, BC, AF, AX, AI, e AP, com percentuais variando de 2,27% a 62,96%.

Para avaliar o impacto de *prepend* na resiliência e contaminação, foram analisados os ASes que aplicaram *prepend* na origem, o número de vezes que o ASN estava repetido e os vizinhos afetados. Os dados das RIBs de 01/04/2024 foram usados nas simulações, e os resultados comparando resiliência com e sem *prepend* estão nas Figuras 4a e 4b.

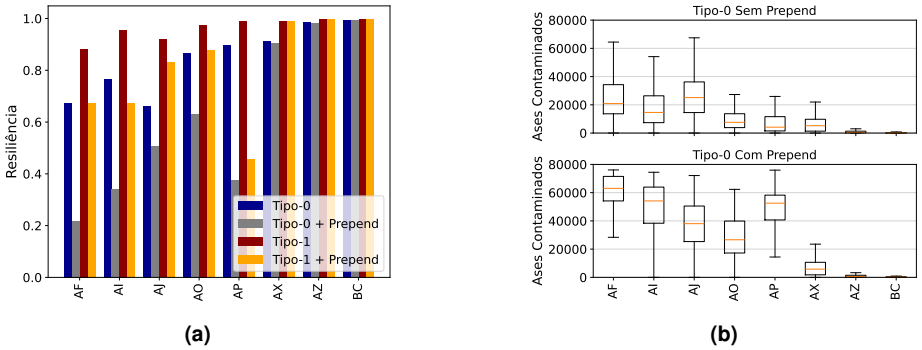

Figura 4. Em (a) a comparação dos valores de resiliência obtidos para os sequestros com e sem o uso de *prepend*. Em (b) na parte superior estão os valores de ASes contaminados para o sequestro Tipo-0 quando não há o uso de *prepend*, e na parte inferior quando há o uso do *prepend*.

Os resultados mostram que o uso de *prepend* pode reduzir significativamente a resiliência. Por exemplo, para o AS AP, a resiliência caiu de 0,8985 para 0,3770 (Tipo-0)

e de 0,9899 para 0,4564 (Tipo-1). No entanto, ASes com vizinhos geograficamente distribuídos, como AX, AZ, e BC, foram menos impactados. Entre eles, a maior queda de resiliência foi no AS AX, com reduções de apenas 0,0077 (Tipo-0) e 0,0012 (Tipo-1), demonstrando que conexões diversificadas ajudam a manter a resiliência contra sequestros.

4.5. Capacidade de Identificação dos Sequestros

Com a crescente adoção de RPKI, que mitiga sequestros de Tipo-0, sequestros maliciosos têm forjado a origem de prefixos para contornar a validação, resultando em um número maior de sequestros de Tipo-1. Um exemplo recente envolveu um sequestro que resultou no roubo de criptomoedas [Siddiqui 2022]. O DFOH (***D**etect **F**orged-**O**rigin BGP **H**ijacks*) [Holterbach et al. 2024] é atualmente o estado da arte na detecção de sequestros com origem forjada. Ele identifica conexões forjadas entre ASes analisando novos enlaces observados no dia, comparando-os a um grafo de conexões na Internet coletado nos 300 dias anteriores. DFOH utiliza 28 *features* para inferência derivadas de informações topologicas, padrões de conexão entre ASes no *AS path*, informações geográficas onde os ASes se conectam e bidrecionalidade de enlaces. Essas *features* alimentam uma floresta aleatória (*random forest*) treinada com enlaces legítimos extraídos do grafo e enlaces forjados gerados sinteticamente. Para garantir representatividade, os enlaces são selecionados com base em agrupamentos de ASes criados pelo sistema. Para informações adicionais sobre DFOH, veja [Holterbach et al. 2024].

Para verificar a capacidade de detecção dos sequestros em ASes militares pelo DFOH, os *AS paths* sequestrados nas simulações observados pelos coletores foram convertidos para o formato do DFOH, simulando novos enlaces. Foram realizados 17.400 sequestros de Tipo-1 para cada data analisada. No entanto, como destacado na Seção 4.2, uma porcentagem considerável de sequestros não chega aos coletores, o que impossibilita análises desses sequestros com DFOH e que não seriam, portanto, identificados. Para os enlaces observados pelos coletores, o DFOH identificou ∼94% como suspeitos. Quando considerados todos os sequestros simulados, a taxa de identificação foi de ∼89%. Os resultados detalhados para cada data estão na Tabela 4.

Tabela 4. Taxa de acerto das inferências realizadas pelo DFOH para os enlaces observados pelos coletores e em relação ao total de simulações.

Data da Simulação	Total de Sequestros	Observados	Detectados	% dos Observados	% do Total
01-02-2024	17.400	16.311	15.399	94,41%	88,50%
01-03-2024	17.400	16.428	15.502	94,36%	89,09%
01-04-2024	17.400	16.474	15.497	94,07%	89,06%

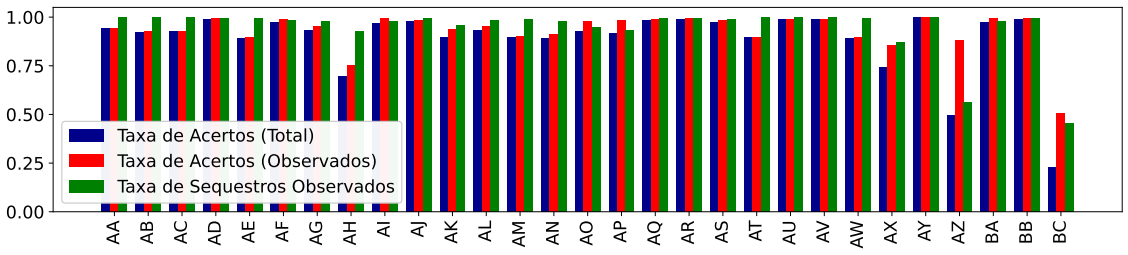

Figura 5. Taxa de acerto do DFOH por AS com dados de 01/04/2024, considerando o total de sequestros e os observados pelos coletores. Também é mostrada a taxa de sequestros observados por coletores para cada AS.

A Figura 5 apresenta as taxas de acerto do DFOH com base no total de sequestros simulados por AS e nos sequestros observados pelos coletores, além da taxa de enlaces observados. Muito embora a Seção 4.3 mostre que os ASes AZ e BC sejam os mais resilientes, eles também são mais suscetíveis a sequestros invisíveis, ou seja, sequestros não observados nos coletores ou detectados pelo DFOH.

Como conclusão deste estudo, mais de 10% de sequestros Tipo-1 não seriam detectados pela melhor ferramenta existente atualmente, sendo que alguns ASes teriam mais de 77% de sequestros não identificados ou visíveis nos coletores públicos de rota.

5. Trabalhos Relacionados

O sequestro de prefixo é um problema grave na Internet. Como ainda não há uma solução eficaz para evitá-lo, muitos estudos focam em sua detecção rápida para mitigar impactos [Lad et al. 2006, Xiang et al. 2011, Liu et al. 2012, Sermpezis et al. 2018b, Shapira and Shavitt 2022, Qin et al. 2022, Bühler et al. 2023, Holterbach et al. 2024]. As abordagens existentes empregam o plano de dados, o plano de controle ou ambos.

A detecção no plano de dados analisa o fluxo de pacotes na rede, geralmente em provedores. A premissa básica é que, durante um sequestro, o provedor do AS da vítima observa queda no volume de dados. Métodos baseados em variações no fluxo, como em [Liu et al. 2012], ou no tempo de ida e volta (RTT), como em [Bühler et al. 2023], podem detectar sequestros, mas não conseguem identificar o sequestrador.

A detecção no plano de controle utiliza rotas coletadas por monitores BGP [Meyer 1997, Mcgregor et al. 2010]. Por exemplo, o PHAS [Lad et al. 2006] analisa mudanças de origem em anúncios BGP e emite alertas para as redes. O Artemis [Sermpezis et al. 2018b] usa dados locais e de coletores para detectar sequestros de Tipo-0 e Tipo-1 com precisão, enquanto tipos mais complexos requerem dados adicionais.

Técnicas de aprendizado de máquina também são usadas para melhorar a detecção. O AP2Vec [Shapira and Shavitt 2022] utiliza representações vetoriais (*embeddings*) dos *AS paths* para identificar alterações suspeitas. Já o DFOH [Holterbach et al. 2024] emprega um modelo de floresta aleatória (*random forests*) com 28 *features*, incluindo padrões de *AS path* e topologia, para inferir sequestros com base em dados históricos e conexões dos ASes no grafo de conectividade da Internet.

Abordagens que combinam os dois planos usam o plano de controle para identificar suspeitas e o plano de dados para confirmar, geralmente com testes de conectividade (*e.g.,* `ping`). Exemplos incluem o Argus [Xiang et al. 2011] e o Themis [Qin et al. 2022], que aprimora o Argus com IA para distinguir anúncios com origens distintas para o mesmo prefixo entre legítimos e ilegítimos.

O estudo de [Milolidakis et al. 2023] analisa como a engenharia de tráfego pode ajudar sequestradores a evitarem a detecção por coletores públicos. Ele compara sequestradores ingênuos, que anunciam rotas sequestradas a todos os vizinhos, com sequestradores avançados, que tentam evadir esses sistemas. Neste trabalho, simula-se um sequestrador que não busca evadir a detecção, resultando em estimativas conservadoras de impacto. Também são avaliadas redes estratégicas nacionais, o uso de *prepend* e a eficácia da ferramenta de detecção mais avançada disponível.

6. Conclusão e Discussão

Este trabalho mostra a gravidade dos sequestros de prefixo para ASes militares do G20, que podem causar negação de serviço ou ataques *man-in-the-middle*, comprometendo a segurança e estabilidade da Internet. Embora sequestros Tipo-0 tenham maior alcance, as simulações mostram que a adoção de RPKI reduz significativamente a vulnerabilidade, sendo uma das formas mais eficazes de mitigação — desde que amplamente adotada.

Sequestradores podem forjar *AS paths* para contornar RPKI, como em [Siddiqui 2022], e ainda não há solução definitiva para prevenir esses ataques. Aumentar a resiliência e melhorar a detecção são, portanto, estratégias essenciais. Este trabalho mostra que a contratação de provedores bem conectados e distribuídos geograficamente é crucial, enquanto o uso de *prepend* na origem do anúncio deve ser evitado, especialmente em ASes com poucos provedores, pois reduz a resiliência. A detecção também é crítica, mas mais de 10% dos sequestros simulados não foram identificados pela ferramenta mais avançada ou não foram observados por coletores públicos.

Como medidas de mitigação, os ASes podem ampliar sua conectividade, aumentando a resiliência e reduzindo os impactos do ataque. Além disso, o aumento de coletores em regiões estratégicas pode aumentar a capacidade de detecção dos sequestros.

Agradecimentos

O presente trabalho foi realizado com apoio da CAPES – Código de Financiamento 001, do CNPq – Procs. 420934/2023-5, 308101/2022-7 e 465446/2014-0, e da FAPESP – Procs. 2023/00812-7, 2023/00811-0, 2020/05192-9 e 2020/05183-0.

Referências

Azimov, A. et al. (2025). BGP AS_PATH Verification Based on Autonomous System Provider Authorization (ASPA) Objects. Internet-draft, IETF. Work in Progress.

Barreto, R. P. et al. (2024). Poster: Traffic engineering security implications. In *Proc. of ACM IMC'24*, page 771–772.

Birge-Lee, H. et al. (2022). Creating a Secure Underlay for the Internet. In *USENIX Security' 22*, pages 2601–2618.

Bühler, T. et al. (2023). Oscilloscope: Detecting BGP Hijacks in the Data Plane. *arXiv preprint arXiv:2301.12843*.

Bush, R. and Austein, R. (2017). The Resource Public Key Infrastructure (RPKI) to Router Protocol, Version 1. RFC 8210.

CAIDA (2015). AS Relationships (Serial-2). `https://catalog.caida.org/dataset/as_relationships_serial_2`.

Carvalho, A. B. et al. (2025). Material Suplementar - Código Fonte e Dados. `https://github.com/Bastos-abc/prefix_hijack_simulator`.

Electric, H. (2024). Hurricane Electric Internet Services. `https://bgp.he.net/`.

Fonseca, O. et al. (2020). Tracking Down Sources of Spoofed IP Packets. In *Proc. of 2020 IFIP Networking Conference (Networking)*, pages 208–216.

Gao, L. and Rexford, J. (2001). Stable Internet Routing Without Global Coordination. *IEEE/ACM Transactions on Networking*, 9(6):681–692.

Holterbach, T., Alfroy, T., Phokeer, A. D., Dainotti, A., and Pelsser, C. (2024). A System to Detect Forged-Origin Hijacks. In *Proc. of the 21th USENIX NSDI*.

Lad, M., Massey, D., Pei, D., Wu, Y., Zhang, B., and Zhang, L. (2006). PHAS: A Prefix Hijack Alert System. In *USENIX Security Symposium*, volume 1, page 3.

Lepinski, M. and Sriram, K. (2017). BGPsec Protocol Specification. RFC 8205.

Li, W. et al. (2023). RoVista: Measuring and Analyzing the Route Origin Validation (ROV) in RPKI. In *ACM IMC 2023*, page 73–88, New York, NY, USA.

Liu, Y., Su, J., and Chang, R. K. (2012). LDC: Detecting BGP Prefix Hijacking by Load Distribution Change. In *2012 IEEE 26th IPDPS Workshops*, pages 1197–1203.

Madory, D. (2022). BGP Hijack of Twitter by Russian ISP. `https://www.kentik.com/analysis/bgp-hijack-of-twitter-by-russian-isp/`.

Marcos, P. et al. (2020). AS-Path Prepending: There Is No Rose Without a Thorn. In *Proc. ACM IMC ´20*, page 506–520.

Mcgregor, T., Alcock, S., and Karrenberg, D. (2010). The RIPE NCC Internet Measurement Data Repository. In *Int. Conf. on Passive and Active Network Measurement*.

Meyer, D. (1997). University of Oregon Route Views Archive Project.

Milolidakis, A. et al. (2023). On the Effectiveness of BGP Hijackers That Evade Public Route Collectors. In *IEEE Access*, volume 11, pages 31092–31124.

Moll, O. (2020). Border Gateway Protocol Hijacking - Examples and Solutions. `https://www.anapaya.net/blog/border-gateway-protocol-hijacking-examples-and-solutions`.

NIST (2024). NIST RPKI Monitor. `https://rpki-monitor.antd.nist.gov/`.

Palmeira, C. (2023). Hackers entram na guerra e atacam governos da Palestina e de Israel. `https://www.tecmundo.com.br/seguranca/272527-hackers-entram-guerra-atacam-governos-palestina-israel.htm`.

Philip Smith (2021). BGP Routing Table Analysis. `https://thyme.apnic.net/`.

Qin, L. et al. (2022). Themis: Accelerating the Detection of Route Origin Hijacking by Distinguishing Legitimate and Illegitimate MOAS. In *USENIX Security‘ 22*.

Rekhter, Y. et al. (2006). A Border Gateway Protocol 4 (BGP-4). RFC 4271.

Sermpezis, P. et al. (2018a). A Survey among Network Operators on BGP Prefix Hijacking. In *Proc. ACM SIGCOMM'18*, page 64–69.

Sermpezis, P. et al. (2018b). ARTEMIS: Neutralizing BGP Hijacking Within a Minute. In *IEEE/ACM Transactions on Networking*, volume 26, pages 2471–2486.

Shapira, T. and Shavitt, Y. (2022). AP2Vec: An Unsupervised Approach for BGP Hijacking Detection. *IEEE Trans. on Network and Service Management*, 19(3):2255–2268.

Siddiqui, A. (2022). KlaySwap – Another BGP Hijack Targeting Crypto Wallets. `https://manrs.org/2022/02/klayswap-another-bgp-hijack-targeting-crypto-wallets/`.

Suzuki, S. (2022). A guerra cibernética paralela entre Rússia e Ucrânia. `https://www.bbc.com/portuguese/internacional-60551648`.

Xiang, Y. et al. (2011). Argus: An Accurate and Agile System to Detecting IP Prefix Hijacking. In *19th IEEE ICNP*, pages 43–48.