FACULDADE DE TECNOLOGIA DE AMERICANA "MINISTRO RALPH BIASI"

Curso Superior de Tecnologia em Segurança da Informação

Guilherme Antonio Souza de Melo

ASSEGURANDO A INTEGRIDADE DO ROTEAMENTO INTERDOMÍNIO COM RPKI

Americana, SP

2023

FACULDADE DE TECNOLOGIA DE AMERICANA "MINISTRO RALPH BIASI"

Curso Superior de Tecnologia em Segurança da Informação

Guilherme Antonio Souza de Melo

ASSEGURANDO A INTEGRIDADE DO ROTEAMENTO INTERDOMÍNIO COM RPKI

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Prof. Marcus Vinícius Lahr Giraldi

Área de concentração: Segurança de Roteamento

Americana, SP

2023

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana Ministro Ralph Biasi-CEETEPS Dados Internacionais de Catalogação-na-fonte

MELO, Guilherme Antonio Souza de

Assegurando a integridade do roteamento interdomínio com RPKI. / Guilherme Antonio Souza de Melo – Americana, 2023.

57f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana Ministro Ralph Biasi – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Esp. Marcus Vinícius Lahr Giraldi

1. Segurança em sistemas de informação. I. MELO, Guilherme Antonio Souza de II. GIRALDI, Marcus Vinícius Lahr III. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana Ministro Ralph Biasi

CDU: 681.518.5

Elaborada pelo autor por meio de sistema automático gerador de ficha catalográfica da Fatec de Americana Ministro Ralph Biasi.

Guilherme Antonio Souza de Melo

ASSEGURANDO A INTEGRIDADE DO ROTEAMENTO INTERDOMÍNIO COM RPKI

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Prof. Marcus Vinícius Lahr Giraldi

Área de concentração: Segurança de Roteamento

Americana, 20 de junho de 2023

Banca Examinadora:

Marcus Vinicius Lahr Giraldi (Presidente)
Especialista
Faculdade de Tecnologia de Americana - FATEC

Edson Roberto Gaseta (Membro)
Mestre
Faculdade de Tecnologia de Americana - FATEC

Mariana Godoy Vazquez Miano (Membro)
Doutora
Faculdade de Tecnologia de Americana - FATEC

RESUMO

Este trabalho aborda o tema do sequestro de prefixo como uma ameaça significativa à segurança do roteamento na Internet. O estudo percorre conceitos relacionados a arquitetura de roteadores e mecanismos de roteamento, enfatizando o protocolo BGP utilizado como padrão para o processo de roteamento interdomínio e a vulnerabilidade de implementação deste protocolo que viabiliza a ameaça de sequestro de prefixos. Em seguida, casos reais de sequestro de prefixo são apresentados, evidenciando os impactos desses incidentes na disponibilidade dos serviços de rede de grandes organizações. Através de uma abordagem conceitual e prática, este trabalho apresenta o *Resource Public Key Infrastructure* (RPKI) como proposta para mitigação da ameaça de sequestro de prefixo, utilizando de recursos de criptografia de chave pública para garantir a autenticidade dos anúncios de roteamento e evitar o sequestro de prefixo.

Palavras Chave: RPKI; BGP; Sequestro de prefixos.

ABSTRACT

This work addresses the issue of prefix hijacking as a significant threat to Internet routing security. The study covers concepts related to the architecture of routers and routing mechanisms, emphasizing the BGP protocol used as a standard for the interdomain routing process and the vulnerability of implementing this protocol that enables the threat of prefix hijacking. Then, real cases of prefix hijacking are presented, showing the impacts of these incidents on the availability of network services in large organizations. Through a conceptual and practical approach, this work presents the Resource Public Key Infrastructure (RPKI) as a proposal to mitigate the threat of prefix hijacking, using public key cryptography resources to guarantee the authenticity of the routing announcements and avoid hijacking. of prefix.

Keywords: RPKI; BGP; Prefix hijacking

SUMÁRIO

LISTA DE FIGURAS

1 INTRODUÇÃO

A infraestrutura da Internet permite a conexão de milhares de redes dispersas ao redor do mundo. A extensão global da Internet se torna possível, de acordo com Tanenbaum (2021), através da interconexão entre diversas redes conhecidas como Sistemas Autônomos, que executam o *Border Gateway Protocol 4* (BGP-4) e participam do processo de roteamento interdomínio para anunciar informações de rota para suas redes e manter a tabela de roteamento global.

O protocolo BGP, lançado oficialmente em 1995 como BGP-4 e especificado na RFC 1771 foi projetado quando ainda não se planejava a extensão que a Internet atingiria nos dias de hoje. A implementação deste protocolo prevê mecanismos que garantem a funcionalidade, mas não a segurança do serviço de roteamento da Internet. Este protocolo possui vulnerabilidades que, quando exploradas por ameaças, causam sérios impactos no comportamento do roteamento da Internet.

Ameaças como sequestro de prefixos decorrem de ações maliciosas ou de configurações incorretas no BGP e podem conduzir os dados trafegados na Internet para um destino diferente do qual ele deveria atingir, ou podem ser modificados antes de atingir o seu destino, impactando na integridade e confiabilidade desses dados ou causando indisponibilidade em rotas da Internet ao direcionar o tráfego para um destino inexistente, afetando a disponibilidade de serviços.

Recursos complementares de segurança para o roteamento na Internet foram projetados para assegurar a legitimidade dos anúncios de prefixo no BGP através da validação de origem das rotas. A *Resource Public Key Infrastructure* (RPKI), especificado na RFC 6810, garante mecanismos para mitigar a ameaça de sequestro de prefixos decorrentes de vulnerabilidades do BGP, assegurando a integridade do roteamento na Internet.

Através desta pesquisa, componentes elementares para o roteamento interdomínio serão apresentados, descrevendo e demonstrando de forma prática as vulnerabilidades do BGP em relação ao anúncio de prefixos e a forma como os

prefixos podem ser acometidos por sequestros, incorrendo no desvio de tráfego endereçado a um destino legítimo para um destino falso.

A estruturação de um ambiente de testes para demonstração de um cenário de roteamento interdomínio com o BGP permitirá a apresentação do propósito maior deste trabalho, que consiste na implementação da infraestrutura RPKI no ambiente de simulação e na comprovação prática sobre os efeitos da validação de rotas para a tomada de decisões de roteamento interdomínio provido através do BGP.

2 REFERENCIAL TEÓRICO

Neste capítulo serão apresentados os elementos e conceitos pertinentes ao roteamento na Internet implementado através do protocolo BGP, também referido como roteamento interdomínio. Em sequência, será realizada a abordagem da ameaça que explora vulnerabilidades do BGP e potencialmente resulta no incidente de sequestro de prefixos no roteamento BGP, bem como serão apresentados os impactos decorrentes deste incidente para mitigar os riscos dessa ameaça e assegurar a integridade do roteamento na Internet através da infraestrutura RPKI.

2.1 IMPORTÂNCIA E DESAFIOS PARA ASSEGURAR O ROTEAMENTO NA INTERNET

Segundo Tanenbaum (2021), a Internet é formada por conjunto de redes autônomas interconectadas que se comunicam através de protocolos formando uma infraestrutura capaz de prover serviços comuns. Essa afirmativa, válida e objetiva, remete a uma reflexão conveniente: diversas redes possuem a responsabilidade sobre a confidencialidade, integridade e disponibilidade do tráfego de dados que percorre através da Internet.

As entidades envolvidas com a ampla infraestrutura de roteamento da Internet possuem responsabilidades sobre seu funcionamento e, portanto, devem priorizar igualmente a segurança dessa infraestrutura. Desse modo, as ações para assegurar o correto funcionamento do roteamento interdomínio perpassam por responsabilidades e ações coletivas que garantem a segurança de cada rede autônoma.

Ao longo das próximas páginas, compreenderemos que funções relacionadas a anúncios de prefixos de rede executadas através do BGP, protocolo fundamental para o roteamento da Internet, apresentam vulnerabilidades que possibilitam impactos capazes de alterar o comportamento do roteamento global, com a capacidade de causar graves prejuízos para o tráfego de dados na Internet e para organizações que fornecem serviços através da Internet.

Segurança de roteamento trata-se de um assunto amplo envolvendo diversas entidades participantes do roteamento global, e, portanto, demandando boas práticas de segurança e uma mudança para a cultura de responsabilidade coletiva, conforme indicada na *Mutually Agreed Norms for Routing Security* (MANRS)[1] que também recomenda e orienta a ampla adoção de mecanismos para garantir a segurança e a performance do roteamento na Internet.

2.2 VISÃO GERAL SOBRE ROTEADORES E ROTEAMENTO

A abordagem sobre ameaças ao protocolo de roteamento BGP, ao qual se propõe esse trabalho, requer a aproximação sobre conceitos, tecnologias e processos complementares e igualmente fundamentais para o entendimento do tema. Desse modo, assimilar as funções básicas de um roteador que, por especificação executa o processo de roteamento, e caracterizar como ocorre o próprio roteamento garantirá uma base sólida para avançar em relação à compreensão sobre ameaças ao processo de roteamento na Internet.

2.2.1 Arquitetura de Roteador

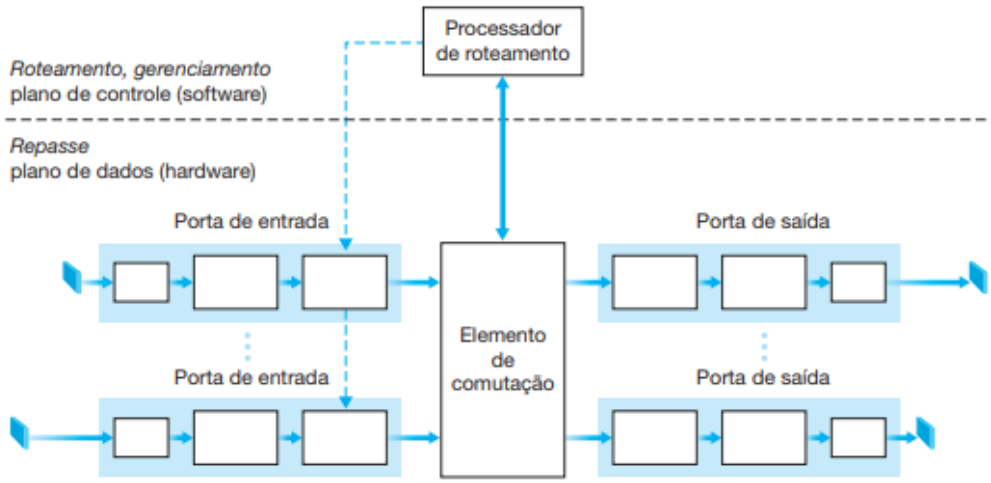
Os roteadores são equipamentos que executam, principalmente, funções relacionadas ao roteamento e ao encaminhamento de pacotes entre hospedeiros através do endereçamento lógico de origem e destino. De acordo com Furouzan (2008), esses dispositivos são capazes de prover a interconexão entre as redes locais e as redes de longa distância na Internet.

De acordo com Chao et al. (2001), um roteador é constituído por interfaces de rede, mecanismo de comutação e processador de roteamento. Uma visão detalhada sobre a arquitetura deste equipamento é ilustrada na Figura 1, onde Kurose e Ross

[1] Iniciativa liderada pela Internet Society com o objetivo de melhorar a segurança e a estabilidade do roteamento da Internet.

(2013) categorizam os componentes em quatro elementos: portas de entrada, elemento de comutação, portas de saída e processador de roteamento.

Figura 1 - Componentes de um roteador genérico



Fonte: Kurose e Ross (2013)

Portas de entrada: As portas de entrada de um roteador recebem pacotes e executam a função de examinar a tabela de encaminhamento para tomar a decisão sobre para qual porta de saída o pacote será repassado para seguir até a rede de destino. Após isso, o pacote é entregue para o elemento de comutação.

Elemento de Comutação: Corresponde a um elemento intermediário, com a função de repassar os pacotes entre a porta de entrada até a porta de saída do roteador.

Portas de Saída: As portas de saída recebem os pacotes do elemento de comutação, após a consulta realizada na porta de entrada, e repassam esse pacote para o enlace de saída correspondente a algum dispositivo conectado ao roteador.

Processador de Roteamento: Este elemento executa os protocolos de roteamento no dispositivo. Os pacotes de controle, que carregam informações de roteamento, quando recebidos nas portas de entrada do roteador são repassados até

o processador de roteamento que irá utilizar essas informações para modificar a tabela de roteamento.

As funções básicas de um roteador, portanto, são executadas utilizando este conjunto de componentes. A função correspondente ao encaminhamento de pacotes é executada entre o elemento de comutação e as interfaces de saída de um roteador. Enquanto a função respectiva ao roteamento é de responsabilidade do processador de roteamento do dispositivo.

O encaminhamento de pacotes, de acordo com Kurose e Ross (2013), trata-se de uma ação local de um roteador que repassa um pacote recebido em uma de suas portas de entrada para uma de suas portas de saída, ou seja, encaminha o pacote para o dispositivo de próximo salto conectado diretamente, através de um enlace, em alguma das interfaces do roteador.

Em relação a função de roteamento, Furouzan (2008) descreve que um roteador armazena informações de rota em uma tabela de roteamento. Essa tabela é atualizada sempre que pacotes de controle são recebidos e processados no roteador. Essa função permite que os roteadores obtenham uma visão completa da topologia de rede onde estão inseridos.

2.2.2 Protocolos de Roteamento

As funções de encaminhamento de pacotes e de roteamento executadas por um roteador são orientados por um conjunto de regras que definem como os roteadores interconectados se comunicam para obterem uma visão ampla sobre a topologia de rede em que estão inseridos. Desse modo, quando um roteador está analisando um pacote que possui um endereço de destino para outra rede, o conjunto de regras, representado por protocolos de roteamento, garante as informações sobre os melhores caminhos entre os roteadores da topologia para que o pacote chegue ao seu destino.

As informações compartilhadas entre os roteadores consistem em rotas para os seus prefixos ou endereços de destino, portanto, são informações armazenadas

em cada roteador. De acordo com Kurose e Ross (2013), as rotas são armazenadas em uma tabela de roteamento. Quando uma rede é inicializada ou ocorre qualquer alteração na topologia de rede tal como a indisponibilidade para uma determinada rota, a tabela será atualizada para estabelecer outros caminhos. Desse modo, a tabela de roteamento é consultada sempre que um roteador executa o encaminhamento de pacotes.

Existem vários protocolos de roteamento, tal como o *Routing Information Protocol* (RIP), *Open Shortest Path* (OSPF), *Border Gateway Protocol* (BGP-4) e outros. Os modelos citados referem-se a protocolos de roteamento dinâmico capazes de atender as mudanças em uma topologia de rede atualizando a tabela de rotas automaticamente. Osunade (2012) menciona que cada protocolo de roteamento se diferencia nas características, benefícios e limitações, cada um com seu próprio processo de roteamento. Portanto, segundo Masood et al. (2016), são as diferenças entre os diversos protocolos de roteamento que os torna especiais e adequados para as diferentes topologias de rede existentes.

Protocolos de roteamento são separados em duas categorias: protocolos de roteamento de *gateway* interno (*Internal Gateway Protocolos – IGP*) e protocolos de roteamento de *gateway* externo (*External Gateway Protocol – EGP*). De acordo com Furouzan (2008), os protocolos de roteamento são implementados por algoritmos que fornecem o cálculo dos caminhos mais curtos para os endereços de destino. Normalmente, um protocolo de roteamento é baseado em algoritmos de vetor de distância ou estado de link:

Algoritmos de vetor de distância: Protocolos baseados em algoritmo de vetor de distância calculam separadamente o melhor caminho para cada rede de destino, armazenando na tabela de roteamento uma lista com as distâncias referenciadas em saltos ou outros tipos de métricas para cada destino. Ao determinar o melhor caminho, o roteador encaminha o vetor de distância aos roteadores vizinhos para informar as rotas para os prefixos de rede e as métricas para alcançar esse prefixo. Como referência de implementação do algoritmo de vetor de distância temos o protocolo RIP.

Algoritmos de estado de link: Algoritmos de estado de link permitem o compartilhamento de informações sobre a topologia de rede entre os roteadores no

processo de roteamento. Essas informações incluem atributos como largura de banda, latência e carga em cada link. Diferentemente dos protocolos de roteamento de vetor de distância, no estado de link os roteadores não trocam suas tabelas de roteamento, mas compartilham informações sobre roteadores vizinhos, redes de destino e métricas relacionadas com essas conexões. O protocolo OSPF é um exemplar que implementa o algoritmo de estado de link no seu processo de roteamento

Halabi e McPherson (2000) definem o processo básico de roteamento com iniciando com a transmissão de informações de rota entre roteadores em uma topologia de rede através de protocolos de roteamento, o armazenamento e consulta dessas informações em tabelas de roteamento para encaminhar os pacotes ao seu destino considerando o melhor caminho calculado através de algoritmos de roteamento. Desse modo, um roteador encaminha o pacote para o dispositivo de próximo salto, normalmente outro roteador conectado diretamente ao enlace de saída, e essa sequência se repete até que o pacote chegue ao seu destino.

2.3 ROTEAMENTO NA INTERNET

Os roteadores são dispositivos fundamentais para movimentar pacotes entre redes, caracterizados como dispositivos encarregados do processo de roteamento. Quanto maior uma topologia de rede, mais se exige da quantidade e da capacidade de roteadores para garantir a eficiência do roteamento do tráfego dos pacotes de origem a destino. Essa exigência, conforme menciona Furouzan (2008), trata-se da quantidade de informações de roteamento a serem processadas para manter a atualização das tabelas de roteamento dos roteadores da rede. A expansão de uma rede demanda que o processamento do cálculo de rotas seja escalável.

A Internet pública interconecta milhares de hospedeiros e para essa garantir este serviço interconecta diversas redes para conduzir o tráfego de pacotes entre o hospedeiro de origem e até o de destino. Em situações frequentes, hospedeiros separados por distâncias continentais se comunicam através da Internet, exigindo a interconexão de roteadores envolvidos na rota e a convergência entre as tabelas de roteamento que serão consultadas para movimentar o tráfego até a rede de destino de forma eficiente. A solução para gerenciar a constante demanda de processamento

da Internet pública, de acordo com Kurose e Ross (2013), é garantida através do agrupamento de roteadores em Sistemas Autônomos.

2.3.1 Sistemas Autônomos

No contexto do roteamento na Internet, Sistemas Autônomos, ou *Autonomous System (*AS) são entidades autônomas que controlam um conjunto de roteadores e administram uma ou mais redes. Para que se torne mais apreensível, podemos considerar alguns modelos de organização comuns ao nosso dia a dia, a título de exemplo, os Provedores de serviço de Internet e organizações de diversos segmentos "como órgãos do governo, universidades, bancos, lojas, empresas de mídia, empresas usuárias da Internet" são organizações passíveis de administrar um Sistema Autônomo (NIC.br e CGI.br, 2022).

A autonomia dessas entidades, de acordo com Rekhter (2006) implica na livre determinação sobre como controlar os seus roteadores e quais protocolos de roteamento utilizam em seu plano de roteamento, contanto que mantenham sua rede funcional e adepta a conexão com outras redes externas. Sistemas Autônomos definem seus próprios planos de roteamento através da implementação de protocolos de roteamento e seus respectivos algoritmos, mas ao mesmo tempo devem adotar um método padrão de roteamento para se conectarem entre si e compartilhar rotas para suas redes de destino na Internet pública.

Sistemas Autônomos, portanto, atuam em uma hierarquia de roteamento segmentada em dois níveis, definidos por Tanenbaum (2021) como roteamento intradomínio e roteamento interdomínio. No roteamento intradomínio, um ou mais protocolos de gateway interno com seus respectivos algoritmos de roteamento são utilizados para garantir o roteamento de pacotes entre roteadores do mesmo domínio administrativo. Em situações em que o tráfego tem como destino uma rede que está fora do Sistema Autônomo, este deve direcionar através do roteamento interdomínio. O roteamento interdomínio compreende a conexão entre roteadores de Sistemas Autônomos distintos com o objetivo divulgar informações de alcançabilidade de seus prefixos na Internet pública.

Essas duas hierarquias de roteamento são complementares para o roteamento na Internet. Enquanto o roteamento intradomínio se ocupa de encontrar os melhores caminhos entre os roteadores da topologia interna de um Sistema Autônomo, para o

roteamento interdomínio o protocolo padrão para o processo de roteamento é o BGP, que considera os melhores caminhos entre cada Sistema Autônomo influenciados por atributos de rota e políticas de roteamento para determinar as rotas. Desse modo, hospedeiros separados a qualquer distância geográfica conseguem se comunicar através da Internet pública.

As organizações que desejam divulgar rotas para suas redes através da Internet pública necessitam de um Sistema Autônomo e, portanto, uma identificação única para o roteamento interdomínio. Essa identificação corresponde ao *Autonomous System Number* (ASN), que identifica um AS e permite que este divulgue suas rotas através do BGP-4. No início, o ASN foi projetado com 16-bits, permitindo atribuir até 65,535 ASNs e posteriormente expandido para 32-bits, correspondendo a mais de 4 bilhões de ASNs. A faixa entre 64.512 até 65.535 em 16-bit, e 4.200.000.000 até 4.294.967.294 em 32-bit correspondem a ASNs reservados para endereçamento de uso privativo.

Sistemas Autônomos utilizam o protocolo BGP para divulgar rotas até suas redes de destino, fica implícito que este domínio precisa, primeiramente, de endereços de IP para endereçar suas redes. De acordo com Butler et al. (2010), endereços de IP são atribuídos para Sistemas Autônomos em blocos contíguos de endereços de IP, ou prefixos de IP**,** identificados através do endereço de rede e do comprimento de máscara, permitindo simplificar as tabelas de roteamento. Conforme exemplifica o autor, o prefixo 192.0.2.0/24 contém todos os endereços entre 192.0.2.0 até 192.0.2.255, portanto, 256 endereços de IP. Desse modo, basta que o prefixo 192.0.2.0/24 seja divulgado no roteamento interdomínio para que todos os endereços contidos no bloco sejam alcançados através do processo de roteamento.

2.3.2 Registros Regionais da Internet

Os Recursos de Número da Internet correspondem ao conjunto formado por prefixos e ASN que são atribuídos aos Sistemas Autônomos por entidades nomeadas como Registros Regionais de Internet e registradores de nível intermediário. De acordo com Butler et al. (2010), A *Internet Assigned Numbers Authority* (IANA), instituição que ocupa o topo dessa hierarquia, faz a distribuição dos blocos de IP para cada um dos cinco Registros Regionais da Internet que atuam de forma autônoma na atribuição de recursos em diferentes regiões do mundo:

AfriNIC (África Network Information Center): Responsável pela alocação e gerenciamento de recursos de endereços IP na região da África.

APNIC (Asia Pacific Network Information Center): Responsável pela alocação e gerenciamento de recursos de endereços IP na região da Ásia-Pacífico.

ARIN (American Registry for Internet Numbers): responsável pela alocação e gerenciamento de recursos de endereços IP na região da América do Norte.

LACNIC (Latin America and Caribbean Network Information Center): Responsável pela alocação e gerenciamento de recursos de endereços IP na região da América Latina e Caribe.

RIPE NCC (Réseaux IP Européens Network Coordination Centre): Responsável pela alocação e gerenciamento de recursos de IP na região da Europa, Oriente Médio e partes da Ásia Central.

Os Registros Regionais de Internet podem endereçar os recursos diretamente para organizações que mantenedoras de Sistemas Autônomos, bem como podem delegar para registradores intermediários que representam uma região a nível nacional, chamados Registros Nacionais de Internet. O Núcleo de Informação e Coordenação do Ponto BR (NIC.br), através do Registro.br, é o Registro Nacional de Internet que possui a função de atribuir os recursos para os sistemas autônomos no Brasil (NIC.br e CGI.br, 2022).

2.3.3 Border Gateway Protocol 4

O Border Gateway Protocol (BGP), especificado na RFC 1771, é atualmente o protocolo padrão para o roteamento interdomínio. A função primordial deste protocolo consiste em prover mecanismos para que Sistemas Autônomos anunciem rotas para os seus respectivos prefixos de IP de destino, de modo que estes prefixos sejam alcançáveis através da Internet.

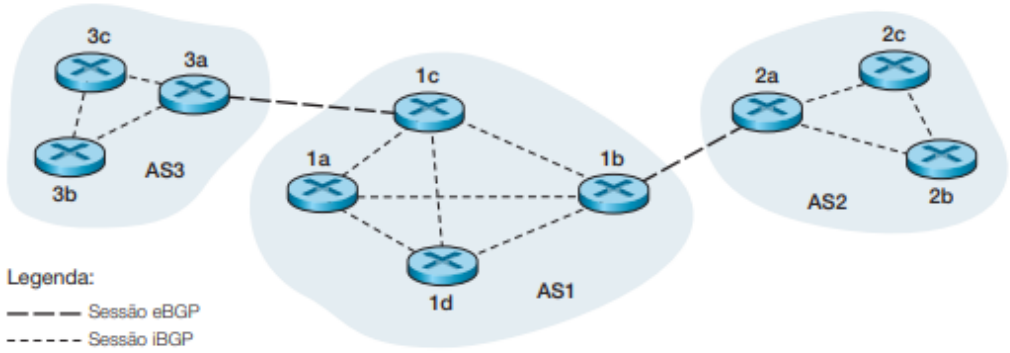
O anúncio de rotas entre dois roteadores executando BGP, conforme afirma Doyle e Carroll (2017), ocorre através de conexões TCP na porta 179. Essa conexão também é referenciada como sessão BGP e os roteadores envolvidos na sessão são considerados pares ou vizinhos BGP. Um roteador interdomínio pode formar vizinhança com um ou mais roteadores de outros domínios autônomos.

Durante as sessões BGP, as tabelas de roteamento são modificadas em duas circunstâncias. Quando um roteador envia uma mensagem de anúncio de rota aos

seus pares para comunicar uma nova rota disponível, ou quando mensagem de retirada é encaminhada aos roteadores vizinhos comunicando que uma rota deixou de existir. Esse comportamento, de acordo com Butler et al. (2010) caracteriza o BGP como um protocolo incremental.

Existem dois tipos de sessões BGP, distintas e complementares, estabelecidas entre roteadores. Quando rotas são trocadas entre dois roteadores BGP interdomínio o protocolo é referido como BGP externo (eBGP). Observando na Figura 2, os roteadores pares interdomínio 3a (AS3) e 1c (AS1), 1b (AS1) e 2a (AS2) estabelecem pares em sessões externas.

Figura 2 - Visão geral BGP



Fonte: Kurose e Ross (2013)

Uma vez que rotas para redes externas ao AS são compartilhadas em sessões eBGP, essas devem se propagar aos roteadores internos ao AS para que estes saibam para onde encaminhar o tráfego para destinos fora de seu domínio. Os roteadores interdomínio 1c e 1b (AS1), por exemplo, estabelecem sessões eBGP com roteadores 3a (AS3) e 2a (AS2), mas também estabelecem sessões iBGP para comunicarem rotas externas si e com os outros roteadores do AS.

Na topologia demonstrada na Figura 2, cada AS possui apenas uma rota para qualquer outro AS, representando um cenário resumido de execução do BGP. Entretanto, esse problema se torna menos generalista ao considerar a grandeza da Internet, onde milhares de Sistemas Autônomos formam relações de vizinhança e compartilham os prefixos de IP através do BGP. É esperado, portanto, a existência de uma ou mais rotas para o mesmo destino.

No processo de decisão de roteamento do BGP, a melhor entre duas ou mais rotas interdomínio disponíveis é determinada, de acordo com Kurose e Ross (2013), com base em políticas de roteamento e atributos do anúncio BGP. Alguns elementos do BGP são manipuláveis ou refletem as diretrizes de políticas de roteamento do Sistema Autônomo, tornando um anúncio de rota mais ou menos preferencial de acordo com os parâmetros dos atributos.

O *AS Path é* um atributo do BGP que reflete a implementação do protocolo através de algoritmos de vetor de caminho. Cada Sistema Autônomo acrescenta seu ASN no anúncio formando uma lista de todo *AS Path* para alcançar o prefixo de destino. Na topologia da Figura 2, o AS3 recebe um anúncio de rotas para o AS2 com o seguinte *AS Path*: AS1, AS2. Segundo Schiller (2013), uma rota com *AS Path* mais curto indica uma rede topologicamente mais próxima e pode atribuir maior preferência para uma rota.

A relação entre Sistemas Autônomos, muito além das conexões físicas entre roteadores interdomínio, são influenciadas por contratos de negócios ou outras relações organizacionais. Balakrishnan (2002) exemplifica que Sistemas Autônomos menores como universidades e corporações, normalmente compram conectividade com Internet *Service Providers* (ISP) e ISPs regionais menores, por sua vez, compram conectividade de ISPs maiores com grandes redes de *backbone*.

Lad et al. (2007) atribuem as classificações de cliente-provedor a relação entre pares. Na relação cliente-provedor, o Sistema Autônomo cliente paga ao Sistema Autônomo provedor o acesso para o restante da Internet. Enquanto a relação entre pares não costuma envolver custos monetários, trata-se de um acordo onde dois Sistemas Autônomos estabelecem interconexão para trocarem o tráfego de seus clientes.

As relações entre os Sistemas Autônomos, de acordo com Schiller (2013), determinam a configuração do atributo de preferência local do BGP. A preferência local é atribuída administrativamente para manipular o caminho da rota usando uma política de roteamento local. Dessa forma, os roteadores BGP escolhem as rotas com maior preferência local para encaminhar o tráfego. Este atributo é mais importante do que o *AS Path* para tomada de decisões de rota no BGP.

Acima de qualquer política de roteamento ou atributo de anúncio que influenciam nas escolhas de rotas do BGP, quando dois prefixos coexistem na tabela de roteamento os roteadores determinam o encaminhamento para a rota com

comprimento de prefixo mais específico. Segundo Kurose e Ross (2013), o prefixo mais específico é o que possui maior correspondência em bits com o endereço de destino do pacote.

Como exemplo, considere que um roteador deve endereçar um pacote para o destino 192.0.2.1 e tenha em sua tabela de roteamento dois anúncios de comprimentos distintos para o mesmo prefixo: 192.0.2.0/24 e 192.0.2.0/25. O endereço de destino 192.0.2.1 é coberto por ambos os prefixos e por isso a decisão de roteamento será para o mais específico, neste caso, o 192.168.2.0/25.

As sessões estabelecidas através do BGP são baseadas na confiança mútua, o protocolo não possui qualquer tipo de validação ou mecanismos confiáveis para atestar a autenticidade dos anúncios de prefixo originado e compartilhado entre pares (HUSTON, 2021). Um roteador BGP, de modo elementar, aceita e anexa os anúncios de prefixos IP em sua tabela de roteamento.

Um Sistema Autônomo, de acordo com Butler et al. (2010), pode anunciar no BGP um prefixo IP não atribuído por uma entidade de Registro Regional de Internet para si e pertencente a outro Sistema Autônomo. Os atributos podem ser manipulados para que esta rota se apresenta como preferencial aos Sistemas Autônomos vizinhos, que podem direcionar o tráfego para o Sistemas Autônomos ilegítimos.

2.4 SEQUESTRO DE PREFIXOS

Cada Sistema Autônomo deve configurar o BGP em seus roteadores interdomínio, também conhecidos como roteadores de borda, para anunciar as rotas respectivas ao ASN e prefixos de IP conforme atribuição do Registro Regional de Internet para que o comportamento normal do roteamento na Internet seja mantido e cada Sistema Autônomo anuncie as redes que de fato foram atribuídas para si.

A confiança implícita entre os roteadores pares e a ausência de recursos de validação no BGP possibilitam que anúncios originados de modo incorreto ou falsificado sejam aceitos, tomados como preferencial na decisão de roteamento interdomínio e propagados através da Internet. Quando isso ocorre, temos um sequestro de prefixo. Trata-se de uma das vulnerabilidades do BGP apresentadas na RFC 4272.

De acordo Schiller (2013), o sequestro de prefixo incorre em ameaças de deleção, inserção ou substituição de dados de roteamento válidos, resultando no sequestro de recursos de rede e de roteadores relacionados com esses recursos, no desvio do tráfego para destinos ilegítimos ou interrupção do tráfego destinado ao prefixo legítimo.

As ameaças capazes de explorar a vulnerabilidade no anúncio de prefixos do BGP causam riscos para as organizações mantenedoras de um Sistema Autônomo. Haag et al. (2019) apontam alguns dos principais riscos, como a indisponibilidade de serviços e responsabilidade legal, que resultam na falha de entrega de serviços e em consequentes multas previstas em contratos de entrega de serviço.

Além disso, os impactos podem se estender de forma negativa para a reputação da organização afetada. Clientes que dependem dos serviços de roteamento fornecidos por uma organização e que foram impactados por uma violação ou indisponibilidade decorrente de ataques no roteamento tendem a perder a confiança na entrega dos serviços.

A proporção dos danos, conforme complementa Haag et al. (2019), pode afetar infraestruturas críticas que dependem do serviço, provocando imposições legislativas de padronização de segurança de roteamento em organizações não regulamentadas. Por fim e igualmente preocupante, a organização é passível de perda de produtividade operacional decorrente do esforço gasto para recuperar o ambiente após ataques ao roteamento.

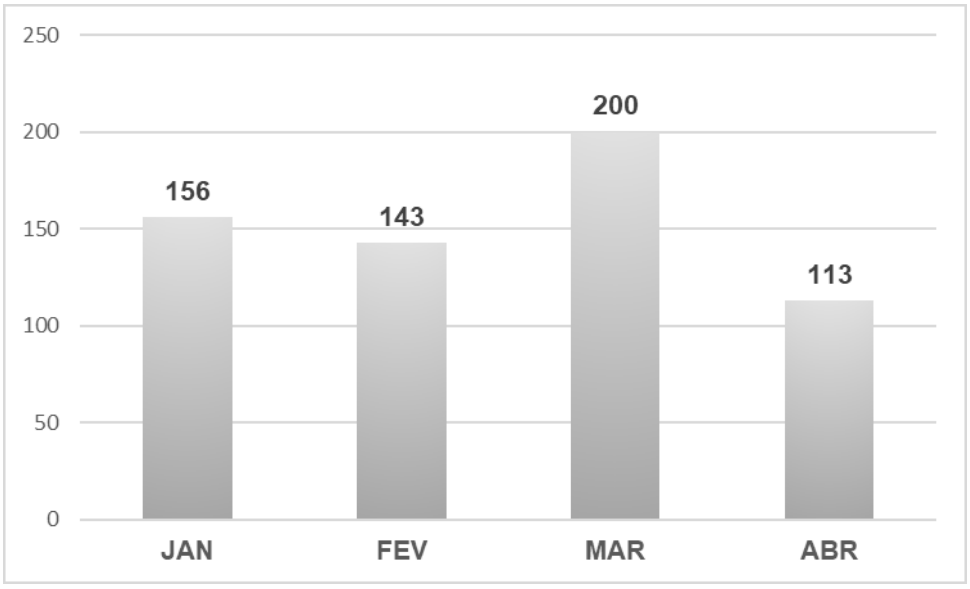
A vulnerabilidade potencialmente explorável reside na origem dos anúncios de rota compartilhados entre roteadores pares. Segundo Murphy (2006), o BGP foi concebido quando não se imaginava que a Internet se tornaria um ambiente inseguro. Portanto, recursos de proteção contra erros intencionais ou acidentais que possam causar falhas ou interrupções no roteamento interdomínio não foram incluídas no protocolo.

As ações para mitigar os riscos de ocorrência dos eventos de sequestro de prefixo demandam a adoção de mecanismos complementares ao BGP, que fornecem uma camada de segurança através de validações criptográficas para garantir que um roteador apenas aceite anúncios de rota caso esses sejam válidos, ou seja, de fato pertencem ao Sistema Autônomo responsável pelo anúncio.

Os incidentes de sequestro de prefixo acontecem com frequência no roteamento interdomínio da Internet como podemos observar nos registros de

incidentes do BGP Stream apresentados na Figura 3. No primeiro quadrimestre de 2023 foram registradas 612 alertas de incidentes relacionados a possíveis roubos de prefixo no mundo, equivalente a 5 incidentes por dia.

Figura 3 - Sequestro de prefixo 1º quadrimestre de 2023



Fonte: Dados do BGP Stream (2023)

Os impactos no tráfego, frequentemente, são de pequena escala, conforme menciona a Internet Society (2020). No entanto, há registro de ocorrências de sequestro de prefixos que causaram interrupções em parte expressiva do roteamento interdomínio, resultando na indisponibilidade de serviços fornecidos através da Internet. A seguir, algumas situações de sequestro serão apresentadas.

2.4.1 Sequestro de prefixos do Youtube

O provedor de conteúdos Youtube mantém um Sistema Autônomo (AS36561) para divulgar rotas para seus prefixos de origem no roteamento da Internet. No ano de 2008 o ministério das telecomunicações do Paquistão ordenou ao provedor de serviços de Internet, Pakistan Telecom (AS17557), para bloquear o acesso ao Youtube. De acordo com estudo de caso da RIPE NCC (2008), o Paquistão ordenou o bloqueio do site do Youtube a partir dos endereços de IP 208.65.153.238, 208.65.153.251 e 208.65.153.253 respectivos ao DNS do site. Na tentativa de cumprir

as ordens, o Pakistan Telecom anunciou de forma não autorizada o prefixo 208.65.153.0/24, cobrindo todos os endereços de 208.65.153.0 até 208.65.153.255.

O provedor de serviços de Internet PCCW Global (AS3491), através de sessões BGP com o AS vizinho, Pakistan Telecom, recebeu e anexou em sua tabela de roteamento BGP o anúncio de origem de rota para o prefixo 208.65.153.0/24. A PCCW Global encaminhou este anúncio para outros Sistemas Autônomos com os quais mantinha sessões BGP, divulgando este o anúncio falso para o restante da Internet. Dois anúncios de rota para os prefixos do Youtube coexistiam no roteamento da Internet. Um, sendo o legítimo e originado pelo próprio Youtube (AS36561) para o prefixo 208.65.152.0/22, e outro, falso e não autorizado, originado de origem da Pakistan Telecom (AS17557) para o prefixo 208.65.152.0/24.

Quando dois prefixos de comprimentos diferentes coexistem na tabela de roteamento, os roteadores determinam o encaminhamento através do endereço do prefixo mais longo. O anúncio legítimo dos prefixos do Youtube, 208.65.152.0/22 corresponde ao intervalo de endereços 208.65.152.0 - 208.65.155.255. No entanto, o prefixo 208.65.152.0/24 representa especificamente os endereços no intervalo 208.65.152.0 até 208.65.155.255, recebendo preferência no roteamento quando o destino é para a rede 208.65.152.0.

Essa ação resultou em um sequestro de prefixo, desviando o tráfego destinado aos endereços de DNS do Youtube através da rota não autorizada originado pelo AS da Pakistan Telecom. Como consequência, o tráfego endereçado ao Youtube foi encaminhado para outra rede de destino, provocando a indisponibilidade dos serviços do provedor de conteúdo por aproximadamente duas horas. Além disso, Balakrishnan (2002) ressalta que o Youtube é um site popular com alto índice de tráfego, portanto, ao originar os prefixos desse site, a Pakistan Telecom provocou um ataque de tráfego contra si e ao provedor PCCW Global.

2.4.2 Sequestro de prefixos da Apple

Em julho de 2022 a organização Rostelecom (AS12389) anunciou no BGP o prefixo 17.70.96.0/19. Este prefixo, contudo, não foi atribuído à Rostelecom, e faz parte de um bloco de endereços atribuídos para a empresa Apple, mantenedora do AS714. O comprimento do prefixo 17.70.96.0/19 anunciado pela Rostelecom é completamente coberto pelo prefixo 17.0.0.0/8 da Apple, e em razão disso o anúncio

do AS12389 desviou o tráfego destinado ao AS714 por apresentar um comprimento de prefixo mais específico.

Este caso, semelhante à situação de sequestro de prefixo ocorrida com o AS do Youtube em 2008, também resultou em sequestro de prefixo baseado na regra de prefixo mais específico. O prefixo 17.0.0.0/8 anunciado através do AS714 corresponde a todos os endereços entre 17.0.0.0 até 17.255.255.255. Enquanto o anúncio da Rostelecom, 17.70.96.0/19, cobre especificamente os endereços de IP na faixa 17.70.127.0 até 17.70.127.255 que também estão contidos no anúncio do AS714.

De acordo com Siddiqui (2022), durante 12 horas, em partes específicas da Internet, alguns usuários que tentaram acesso aos serviços da Apple podem ter sido direcionados para as redes correspondentes ao prefixo do anúncio da Rostelecom. Para reduzir os impactos, a engenheiros de rede da Apple anunciaram o 17.70.96.0/21. Desse modo, as decisões de roteamento do BGP novamente seriam influenciadas por um anúncio mais específico em relação ao anúncio da Rostelecom.

2.5 RESOURCE PUBLIC KEY INFRASTRUCTURE (RPKI)

O *Resource Public Key Infrastructure* (RPKI), proposto na RFC 6480, corresponde a uma infraestrutura hierárquica de chaves públicas capaz de vincular os Recursos de Número da Internet atribuídos por Registros Regionais ou Nacionais de Internet aos Sistemas Autônomos, com chaves públicas, através de certificados digitais e de uma hierarquia de certificação[2]. Segundo Chung et al. (2019), as chaves privadas associadas aos certificados são usadas para que os titulares dos certificados, neste contexto representado por Sistemas Autônomos, declarem que os Recursos de Numeração da Internet de fato foram atribuídos a si.

Essa tecnologia permite a validação de anúncios de rota através do protocolo BGP (REGISTRO.BR, 2009). Portanto, com a implementação do RPKI, roteadores em sessões BGP, ao receberem um anúncio de origem de rota, não se orientam apenas pela confiança implícita aos seus pares para anexar a rota em sua tabela, mas dispõe de recursos e informações para validar se os Recursos de Número da Internet relacionados ao anúncio de rota recebido de fato pertencem ao Sistema Autônomo

[2] Lepinski, M. and Kent, S. (2012). **An Infrastructure to Support Secure Internet Routing.** RFC 6480.

que está originando este anúncio, evitando sequestro de prefixos. Atualmente, essa tecnologia faz parte das recomendações para segurança de roteamento previstas no MANRS.

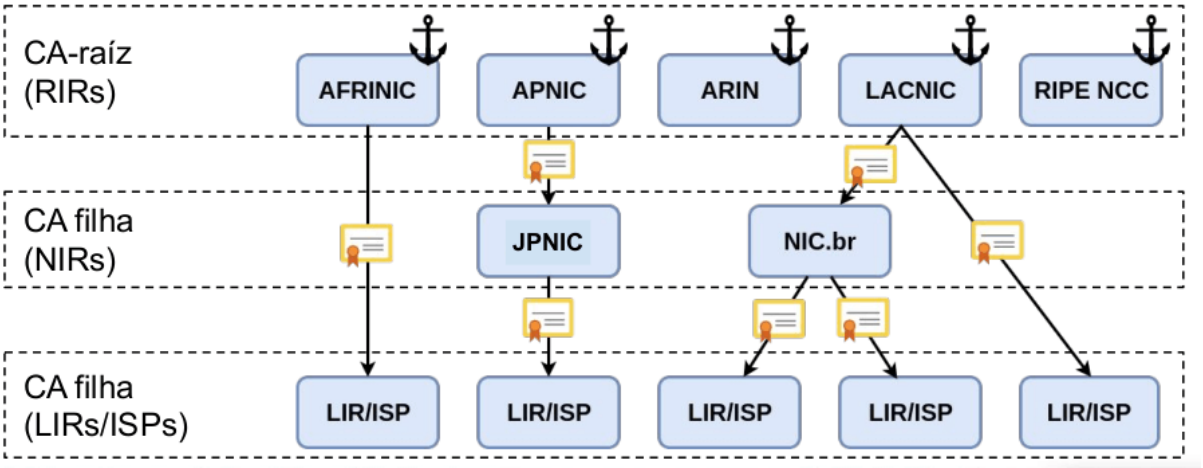
2.5.1 Certificados e Hierarquia de Certificação

O RPKI possui as funções fundamentais de uma infraestrutura de chaves pública, ou *Public Key Infrastructure* (PKI): certificação e validação. Segundo Albarqi et al. (2015), uma PKI utiliza um sistema de criptografia assimétrico, onde as chaves públicas são utilizadas para verificar a legitimidade de uma assinatura digital e as chaves privadas servem para as autoridades certificadores assinarem digitalmente os certificados.

Através do RPKI, os Recursos de Número da Internet de um Sistema Autônomo são vinculados a certificados digitais de padrão X.509, possibilitando verificar a legitimidade dessa entidade sobre esses recursos através da chave pública. E as chaves privadas, portanto, serão utilizadas por autoridades certificadores do RPKI para assinar os certificados de seus membros (REGISTRO.BR, 2009).

Conforme ilustrado na Figura 4, os cinco Registros Regionais de Internet assumem a posição de Âncora de Confiança, equivalente a uma Autoridade Certificadora (C.A) de uma PKI, com a atribuição de emitir certificados para cada uma de suas regiões de representação na hierarquia de chaves de certificação do RPKI.

Figura 4 - Hierarquia de certificado RPKI



Fonte: Registro.br

De acordo com Phooker (2013), As Âncoras de Confiança assinam certificados para cada um de seus membros. Esses membros podem ser níveis intermediários de registros de Internet como os Registros Nacionais de Internet, ou podem ser os clientes de um registrador, como Provedores de Serviço de Internet ou qualquer outra organização que mantenha um Sistemas Autônomo.

Cada âncora de confiança assina os certificados de CA, referenciados como certificados de recursos, com a chave privada para seus respectivos membros. Esse certificado será utilizado para atestar a legitimidade dos detentores de Recursos de número da Internet alocados para si por seus respectivos Registros de Internet.

2.5.2 Validação de Origem baseada em RPKI

A validação de origem, segundo Phooker (2013), remete a um dos principais problemas do roteamento interdomínio. Esse problema demanda uma solução onde os participantes do roteamento interdomínio utilizem de mecanismos capazes de validar a autenticidade dos anúncios de prefixo que seus roteadores pares encaminham nas sessões BGP. A solução para o problema do roteamento interdomínio é proposta a partir de um objeto categorizado por Autorização de Origem de Rota, ou *Route Origin Authorization* (ROA).

2.5.3 Autorização de Origem de Rota

Chung et al. (2019) descrevem um ROA como um objeto contendo um único ASN, um ou mais prefixos de IP com seus respectivos comprimentos de prefixo respectivos a um Sistema Autônomo. De modo complementar, Phooker (2013) afirma que a função de um ROA, é assegurar que um Sistema Autônomo foi autorizado pelo detentor do bloco de recursos, ou seja, um Registro de Internet, a originar os prefixos no BGP. ROAs, portanto, não asseguram o roteamento na interdomínio, mas, de acordo com o autor, fornece objetos criptograficamente verificáveis utilizados para filtros confiáveis no BGP.

A segunda parte do processo do RPKI, portanto, utilizará dos certificados e ROAs para executar o processo de validação. Isso permitirá a roteadores interdomínio, através do sistema RPKI a consultarem a autenticidade dos anúncios de rota recebidos através do BGP. Para isso, esses objetos devem ser publicados em

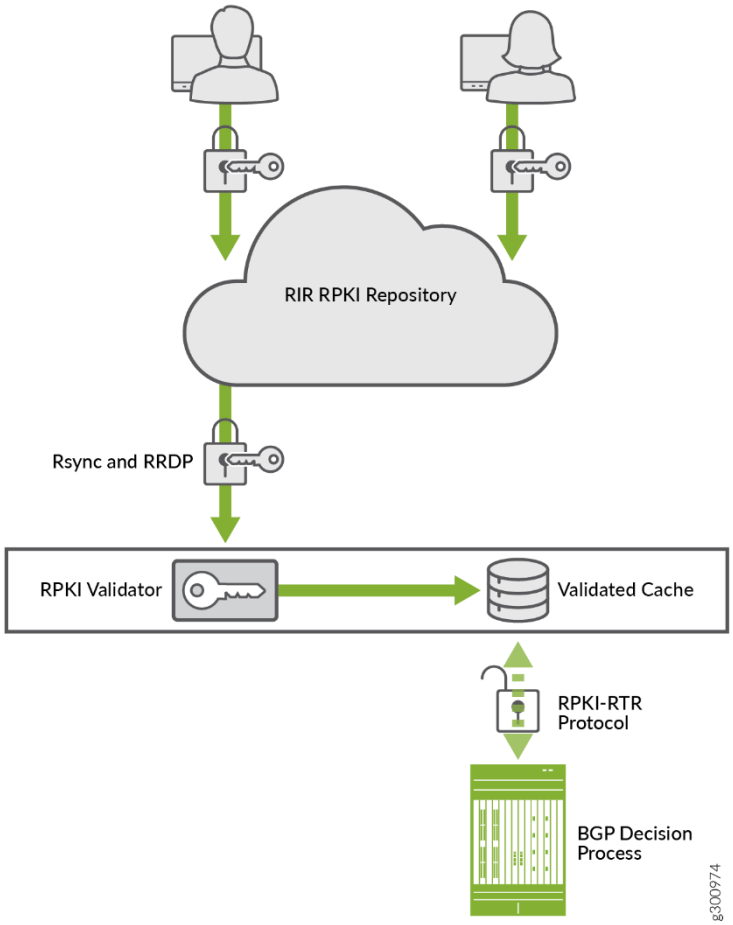
repositórios que serão consultados sempre que uma parte confiável necessita validar o anúncio recebido.

Segundo o Registro.br (2009), existem dois modelos de repositório. O modelo de C.A corresponde a um repositório fornecido através dos Registros de Internet. O próprio Registro.br fornece acesso a um repositório para publicação de certificados e ROAs. No entanto, há o modelo classificado como delegado, onde as organizações têm como opção utilizarem repositórios próprios caso essas mantenham uma autoridade de certificação.

2.5.4 Validação de Origem de Rota

Os repositórios permitem que os objetos criptográficos como certificados e ROAs se tornem acessíveis para um propósito. Esses objetos, de algum modo, devem se tornar legíveis por roteadores para serem utilizados como filtros de rota no BGP durante o processo de roteamento interdomínio. Para essa ocasião, os Sistemas Autónomos, de acordo com Chung et al. (2019), utilizam um software de parte confiável, ou Relying *Party* (RP). Esses softwares, através do utilitário *rsync*, sincronizam com os repositórios para acessar e validar os ROAs, produzindo objetos de ROAs validados e armazenando esses objetos em cache.

Figura 5 - Visão geral do RPKI ao BGP



Fonte: Juniper Networks Tech Library (2020)

O processo de validação do RPKI, ilustrado na Figura 5, portanto, mantém ROAs validados em um cache local. Parte importante desse processo, o protocolo RPKI-RTR especificado na RFC 6810, permite que roteadores recebam as ROAs validadas e utilizem para seu processo de decisão do BGP no roteamento interdomínio[3]. De acordo com Phooker (2013), a proposta do protocolo RPKI-RTR é se ocupar de toda carga de validação, determinando se um anúncio de rota recebido é legítimo ao AS anunciantes ou não. Os roteadores que utilizam dos objetos de validação do RPKI para as tomadas de decisão do BGP, portanto, não precisam dispor de nenhum processamento adicional para validações criptográficas.

[3] R. Bush (2013). **The Resource Public Key Infrastructure (RPKI) to Router Protocol.** RFC 6810

2.5.5 Estados de validação RPKI

Os mecanismos de validação fornecem meios para que roteadores consultem objetos RPKI durante o processo de roteamento interdomínio. Esses objetos fornecem direcionamentos que influenciam diretamente as decisões de roteamento no BGP, com a finalidade de garantir maior confiabilidade neste processo. Em um sistema RPKI, quando um roteador recebe um anúncio de rota no BGP, ele irá validar esse anúncio através do conjunto de ROAs validados disponíveis no cache.

De acordo com Chung et al. (2019), a validação consiste em determinar se o prefixo IP anunciado no BGP é coberto por alguma ROA validado. Portanto, o prefixo, comprimento do prefixo e o ASN, atributos contidos em um anúncio de rota BGP, serão comparados com os mesmos atributos contidos em uma ROA validado, caso essa exista no cache validador. De acordo com a correspondência ou divergência entre o anúncio recebido e um ROA validado, o anúncio recebido por um roteador através do BGP será classificado com algum dos seguintes estados:

Válido: Este estado é aplicado ao anúncio de rota do BGP quando o anúncio corresponde em todos os atributos com o de uma ROA, ou seja, o prefixo e comprimento são anunciados por um AS autorizado por um ROA existente.

Inválido: Um anúncio no BGP recebe esta classificação quando o prefixo e comprimento do prefixo são cobertos por um ROA, no entanto, o AS não corresponde ao AS autorizado no ROA e não existe nenhum outro ROA que cubra o anúncio.

Não identificado: Não há nenhum ROA que cubra o prefixo, portanto, nenhum ROA a ser validado.

É esperado, portanto, que as rotas classificadas com estado válido sejam aceitas para o roteamento BGP, enquanto operadores de rede tendem a descartar as rotas inválidas em sua política de roteamento. Anúncios validados como não identificados podem representar anúncios legítimos, mas que não foram publicados em um repositório RPKI. Cada uma das partes confiáveis, segundo Phooker (2013) deve definir suas regras, direcionando a políticas com maior austeridade ou mais flexibilidade em relação a validação RPKI.

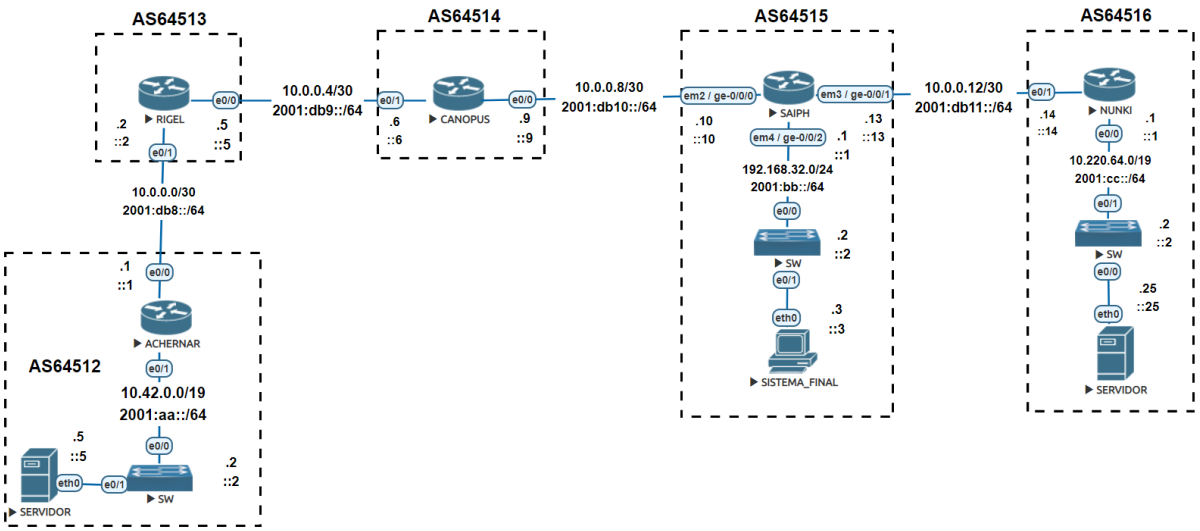
3 DESENVOLVIMENTO

Nessa seção será demonstrada uma topologia de rede baseada em um modelo de roteamento interdomínio utilizando protocolo BGP. Em seguida, será apresentada de forma prática a ocorrência de um sequestro de prefixo no roteamento da topologia. Por fim, uma proposta de solução para mitigar a ameaça de sequestro de prefixo aos serviços do protocolo BGP será apresentada, com o objetivo de expor os resultados decorrentes da aplicação do RPKI para validação de rotas no BGP.

3.1 AMBIENTE DE TESTE

O ambiente de teste foi criado no emulador de redes EVE-NG, utilizando roteadores, *switches* e servidores virtualizados implementados na plataforma de virtualização VM-Ware Workstation 17. 0.0 build-20800274. Neste escopo de rede foram utilizados três *hosts* implementados através de *Virtual PC*, dois *Switches* Cisco com IOS 15.2 e cinco roteadores virtuais, sendo quatro emulados com IOS 15.4 e um Juniper vMX com Junos IOS 14.1R1.10 adaptável ao protocolo RPKI-to-Router. O software de *Relying Party* utilizado para validação do RPKI foi FORT Validator versão 1.5.4, instalado em um servidor virtualizado de sistema operacional FreeBSD 12.3.

Figura 6 - Topologia de Rede



Fonte: De autoria própria

A topologia de rede do ambiente de testes é demonstrada na Figura 6, sendo composta por cinco Sistemas Autônomos envolvidos no roteamento interdominio, atribuídos de ASN privados e prefixos de IPv4 reservados e IPv6 global unicast, interconectados através de sessões externas do BGP. A abordagem para este escopo de rede descreve os Sistemas Autônomos através da sigla AS e pressupõe a legitimidade dos prefixos atribuídos para cada entidade apenas para testes do ambiente, permitindo a posterior simulação de um sequestro de prefixo e a aplicação do RPKI no processo de validação dos anúncios de rota. Os blocos de IPv4 atribuídos para os Sistemas Autônomos correspondem a endereços reservados e, portanto, não roteáveis na Internet pública.

3.1.1 Análise das sessões BGP

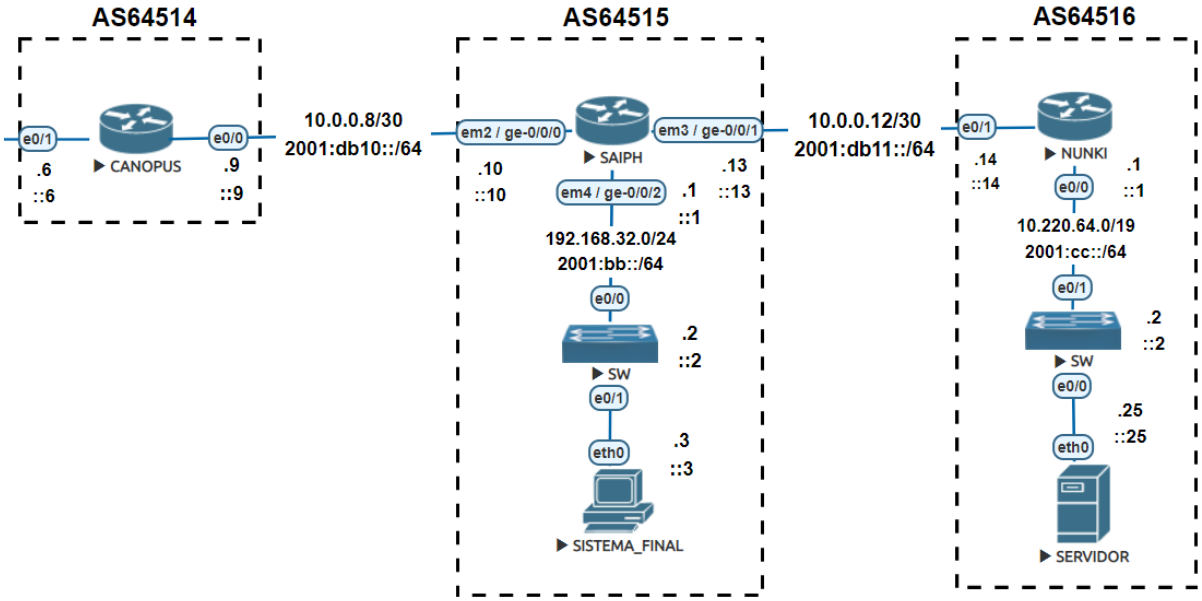
Através de sessões externas do BGP com os roteadores adjacentes, um AS compartilha anúncios de rotas para seus prefixos de destino. Cada roteador possui rotas para qualquer prefixo de destino pertencente aos Sistemas Autônomos dessa topologia. Desse modo, o AS64515 será utilizado como modelo para a descrição do contexto BGP apresentado neste escopo de rede, ressaltando que o processo de

roteamento interdomínio ocorrido entre este AS e seus pares diretamente conectados são aplicados a todos os roteadores deste cenário e seus respectivos pares.

O roteador Saiph (AS6515), como é possível observar na Figura 7, possui conexão com o roteador Canopus (AS64514) e ambos fazem parte da rede 10.0.0.8/30, possibilitando o estabelecimento de conexão lógica entre os roteadores. O roteador Saiph (AS6515) está endereçado com o IPv4 10.0.0.9 e o Canopus (AS64514) com o endereço IPv4 10.0.0.10. Os pares também possuem comunicação lógica através do IPv6 na rede 2001:db9::/64, onde o Saiph está endereçado com 2001:db10::9 e o roteador Canopus com 2001:db10::6

A topologia também apresenta uma conexão estabelecida entre os roteadores Saiph (AS64515) e Nunki (AS64516). Os roteadores fazem parte da rede 10.0.0.12/30, sendo o primeiro endereçado com 10.0.0.13 e o segundo com o endereço 10.0.0.14. Seguindo o padrão desta topologia, os roteadores adjacentes também possuem conexão através da rede IPv6 2001:db11::/64, onde o roteador Saiph está endereçado com 2001:db11::13 e o roteador Nunki recebe o endereçamento 2001:db11::14.

Figura 7 - Conexão entre ASes



Fonte: De autoria própria

A conexão entre os roteadores Saiph e Canopus e Saiph e Nunki permite o estabelecimento de sessões BGP entre os roteadores pares e a formação de vizinhança entre AS64515 e AS64514, e entre 64515 e 64516. A Figura 8 demonstra o resumo das conexões BGP estabelecidas no roteador Saiph (AS64515) com os roteadores adjacentes de ASes vizinhos. Há duas sessões para cada vizinho, sendo uma respectiva ao estabelecimento através do endereçamento IPv4 e a outra estabelecida em IPv6.

Figura 8 - Sumário BGP do roteador Saiph (AS64515)

```
AS64515@SAIPH> show bgp summary
Groups: 2 Peers: 4 Down peers: 0
Table          Tot Paths  Act Paths Suppressed    History Damp State    Pending
inet.0
                       5          4          0          0          0          0
inet6.0
                       6          4          0          0          0          0
Peer                     AS      InPkt     OutPkt    OutQ   Flaps Last Up/Dwn State|
..
10.0.0.9              64514         77         77       0       0       33:07 Establ
  inet.0: 3/3/3/0
10.0.0.14             64516         75         78       0       0       33:03 Establ
  inet.0: 1/2/2/0
2001:db10::9          64514         79         76       0       0       32:44 Establ
  inet6.0: 3/4/4/0
2001:db11::14         64516         74         81       0       0       32:51 Establ
  inet6.0: 1/2/2/0
```

Fonte: De autoria própria

A única relação de vizinhança BGP que o AS64516 estabelece, conforme observado na Figura 7, é com o AS64515 através da conexão entre os roteadores Nunki e Saiph respectivamente. O AS64516 possui as redes IPv4 10.0.0.12/30, IPv6 2001:db11::/64 e IPv4 10.220.64.0/19, IPv6 2001:cc::/64, que exporta ao seu vizinho AS64515 durante as sessões BGP entre os roteadores pares. A Figura 9 mostra os anúncios recebidos no roteador Saiph (AS64515) durante sessão com seu par Nunki (AS64516).

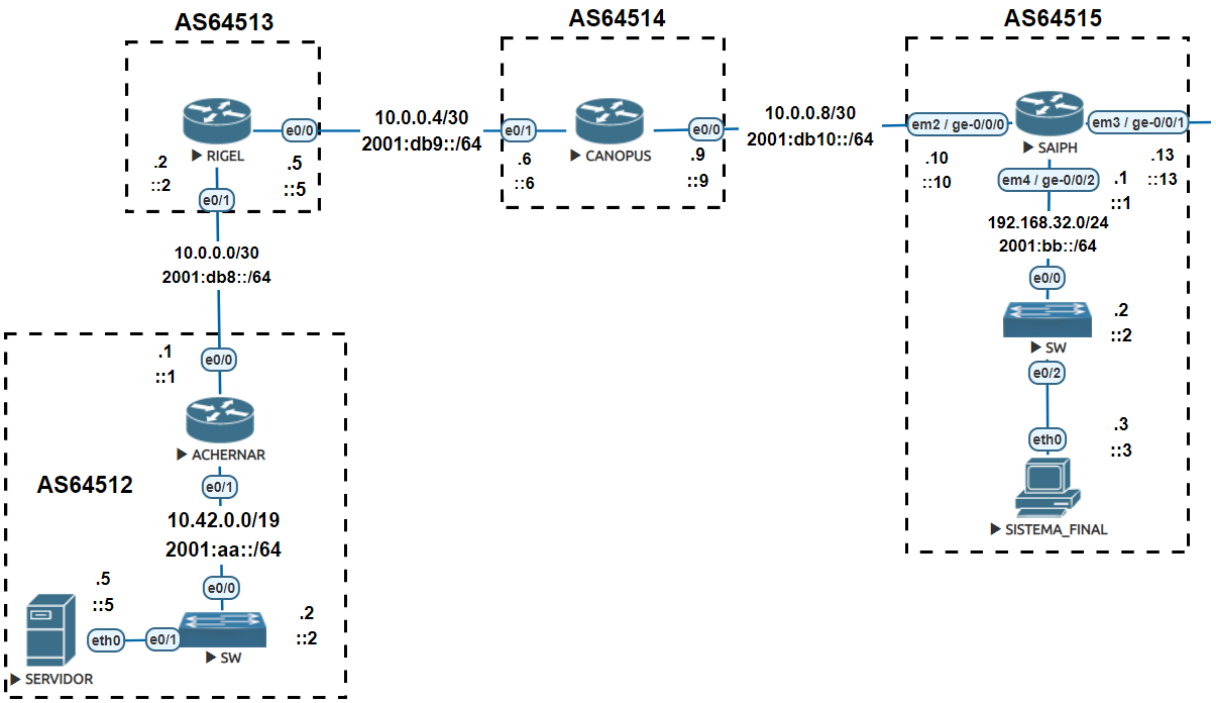
Figura 9 - Rotas BGP do AS64515 recebidos do AS64516

```
AS64515@SAIPH> show route receive-protocol bgp 10.0.0.14

inet.0: 10 destinations, 11 routes (10 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
  10.0.0.12/30            10.0.0.14            0                  64516 I
* 10.220.64.0/19          10.0.0.14            0                  64516 I

inet6.0: 13 destinations, 17 routes (13 active, 0 holddown, 0 hidden)

AS64515@SAIPH> show route receive-protocol bgp 2001:db11::14

inet.0: 10 destinations, 11 routes (10 active, 0 holddown, 0 hidden)

inet6.0: 13 destinations, 17 routes (13 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 2001:cc::/64            2001:db11::14        0                  64516 I
  2001:db11::/64          2001:db11::14        0                  64516 I
```

Fonte: De autoria própria

O roteador Saiph (AS64515) receberá uma quantidade maior de prefixos durante as sessões BGP com o roteador Canopus (AS64514). Isso ocorre devido a vizinhança estabelecida entre o AS64514 e AS64513 e entre AS64513 e AS64512, conforme Figura 10. Os prefixos do AS64512, 10.42.0.0/19, 2001::aa::/64, 10.0.0.4/30 e 2001:db8::/64 são anunciados ao AS64513. O AS64513, por sua vez, anuncia os prefixos do AS64512 mais os prefixos 10.0.0.8/30 e 2001:db9::8 ao AS64514.

Figura 10 - Topologia Parcial



Fonte: De autoria própria

O roteador Canopus (AS64514), por fim, compartilha todos prefixos recebidos anteriormente, somado aos seus prefixos 10.0.0.12/30 e 2001:db10::/64 em sessão BGP com o roteador Saiph (AS64515). Ao final deste processo, o roteador Saiph (AS64515) obtém as rotas para todas as redes de destino correspondente aos ASes 64514, 64513 e 64512, conforme demonstrado na **Erro! Fonte de referência não encontrada.**.

Figura 11 - Rotas BGP do AS64515 recebidos do AS64514

```
AS64515@SAIPH> show route receive-protocol bgp 10.0.0.9

inet.0: 10 destinations, 12 routes (10 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 10.0.0.0/30             10.0.0.9                                64514 64513 I
* 10.0.0.4/30             10.0.0.9                                64514 64513 I
  10.0.0.8/30             10.0.0.9             0                  64514 I
* 10.220.64.0/20          10.0.0.9                                64514 64513 64512 I

inet6.0: 14 destinations, 18 routes (14 active, 0 holddown, 0 hidden)

AS64515@SAIPH> show route receive-protocol bgp 2001:db10::9

inet.0: 10 destinations, 12 routes (10 active, 0 holddown, 0 hidden)

inet6.0: 14 destinations, 18 routes (14 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 2001:cc::/96            2001:db10::9                            64514 64513 64512 I
* 2001:db8::/64           2001:db10::9                            64514 64513 I
* 2001:db9::/64           2001:db10::9         0                  64514 I
  2001:db10::/64          2001:db10::9         0                  64514 I
```

Fonte: De autoria própria

O roteador Saiph (AS64515), através do protocolo BGP, adquire rotas para todas as redes de destino da topologia, bem como exporta os seus prefixos aos seus pares durante as sessões. Portanto, todos ASes também possuem rotas para qualquer destino deste escopo de rede. Periodicamente os roteadores BGP trocam mensagens para informar alterações na topologia e sincronizar as tabelas de roteamento.

3.1.2 Demonstração de sequestro de prefixo

Todo processo de compartilhamento de rotas no BGP ocorre sem nenhum tipo de apresentação entre os pares. As sessões BGP são baseadas na confiança mútua, o que significa que cada par de roteadores envolvidos em sessões BGP considera para o seu processo de seleção de rotas, sem nenhuma análise prévia da autenticidade do anúncio, as informações recebidas de seus vizinhos.

O AS64515, por exemplo, possui o prefixo de rede 192.168.32.0/24. Para que o tráfego originado nesta rede seja endereçado a rede 10.220.64.0/30 do AS64516, em um cenário de roteamento interdomínio integro, os pacotes serão encaminhados

em apenas um salto até o destino, haja vista que o roteador Saiph do AS64515 está diretamente conectado ao roteador Nunki correspondente AS64516 de destino.

No entanto, não há impedimento algum para que um roteador de um AS compartilhe no BGP os prefixos correspondentes a outro AS. Nesta ocasião, trata-se de um anúncio falso, e caso este possua atributos que o eleve como rota preferencial em relação ao anúncio legítimo para a rede e seja selecionado para o roteamento interdomínio, o tráfego para a rede de um determinado AS pode ser desviada para um destino ilegítimo em outro AS.

Para demonstração dessa ameaça, considerando a topologia de rede abordada neste ambiente de testes, o AS64512 será utilizado como agente de ameaça. Desse modo, o roteador Achernar (AS64512) encaminha no BGP o anúncio para o prefixo 10.220.64.0/20, sendo mais específico que o prefixo legitimo 10.220.64.0/19 de origem do AS64516.

O roteador Achernar (AS64512), conforme Figura 12, encaminha o anúncio para o prefixo 10.220.64.0/20 e 2001:cc::/96 ao roteador adjacente Rigel (AS64513). O AS64513 possui vizinhança com o AS64514, e, por fim, o anúncio para o prefixo de destino falso originado no AS64512 chegará ao AS64515 devido a sessões BGP que mantém seu par AS64514.

Figura 12 - Anúncios de prefixo do AS64512 no BGP

```
ACHERNAR#show ip bgp neighbors 10.0.0.2 advertised-routes
BGP table version is 8, local router ID is 10.220.64.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  10.0.0.0/30      0.0.0.0                  0         32768 i
 *>  10.220.64.0/20   0.0.0.0                  0         32768 i

Total number of prefixes 2
ACHERNAR#show bgp ipv6 neighbors 2001:db8::2 advertised-routes
BGP table version is 11, local router ID is 10.220.64.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  2001:CC::/96     ::                       0         32768 i
 *>  2001:DB8::/64    ::                       0         32768 i

Total number of prefixes 2
```

Fonte: De autoria própria

Ao verificar as entradas da tabela de roteamento no AS64515, representado na Figura 13, identificamos duas rotas para a rede 10.220.64.0. A rota legítima correspondente ao prefixo 10.220.64.0/19 de apenas um salto até AS64516 de destino, e outra 10.220.64.0/20 correspondente ao anúncio falso, que percorre o *AS Path* de AS64514, AS64513 até chegar ao destino ilegítimo AS64512.

Figura 13 - Entradas da tabela de roteamento AS64515

```
AS64515@SAIPH> show route 10.220.64.0/19

inet.0: 10 destinations, 11 routes (10 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.220.64.0/19     *[BGP/170] 01:01:02, MED 0, localpref 100
                      AS path: 64516 I, validation-state: unverified
                    > to 10.0.0.14 via em3.0
10.220.64.0/20     *[BGP/170] 01:00:31, localpref 100
                      AS path: 64514 64513 64512 I, validation-state: unverified
                    > to 10.0.0.9 via em2.0
```

Fonte: De autoria própria

Conforme demonstrado nos casos reais de sequestro de prefixo nas seções anteriores, organizações como Youtube e Apple foram acometidas por sequestro de seus prefixos de seus respectivos ASes no roteamento BGP. Ambos os casos foram condicionados através de anúncios falsos com comprimento de prefixo mais específico do que os anúncios legítimos dos ASes correspondentes às organizações.

O prefixo mais específico possui maior prioridade na seleção de rotas do BGP em relação ao nível de preferência local ou *AS Path* mais curto que possa tornar a rota preferível. Dessa forma, ao escolher entre duas rotas para rede de destino 10.220.64.0 ou 2001:db11::/64 através do BGP, o roteador Saiph (64515) determinará o caminho respectivo ao anúncio do prefixo 10.220.64.0/20 ou 2001:db11::/96 do AS64516, conforme exposto na Figura 14.

Figura 14 - Melhor rota do AS64515 para o AS64516

```
AS64515@SAIPH> show route best 10.220.64.0

inet.0: 10 destinations, 11 routes (10 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.220.64.0/20     *[BGP/170] 00:48:28, localpref 100
                      AS path: 64514 64513 64512 I, validation-state: unverified
                    > to 10.0.0.9 via em2.0

AS64515@SAIPH> show route best 2001:cc::

inet6.0: 14 destinations, 18 routes (14 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

2001:cc::/96       *[BGP/170] 00:00:52, localpref 100
                      AS path: 64514 64513 64512 I, validation-state: unverified
                    > to 2001:db10::9 via em2.0
```

Fonte: De autoria própria

A ausência de mecanismos de validação inerentes ao BGP viabiliza incidentes dessa categoria, uma vez que as rotas são inseridas nas tabelas de roteador sem uma validação prévia da origem do anúncio. Contudo, mecanismos de validação complementares ao BGP, como a infraestrutura RPKI, permite mitigar esse tipo de ameaça assegurando a verificação da autenticidade dos prefixos anunciados, conforme será demonstrado na seção seguinte.

3.1.3 Influências do RPKI no BGP

O sequestro de prefixos deflagrado na topologia de testes representa um incidente resultante da exploração de uma vulnerabilidade na origem do anúncio de prefixos do BGP. Ao receber dois anúncios de prefixos de ASes distintos para a mesma rede, como ocorrido com o roteador Saiph do AS64515, o roteador poderá endereçar o tráfego para um destino ilegítimo caso o anúncio respectivo a este destino possua atributos que eleve sua preferência no roteamento do BGP.

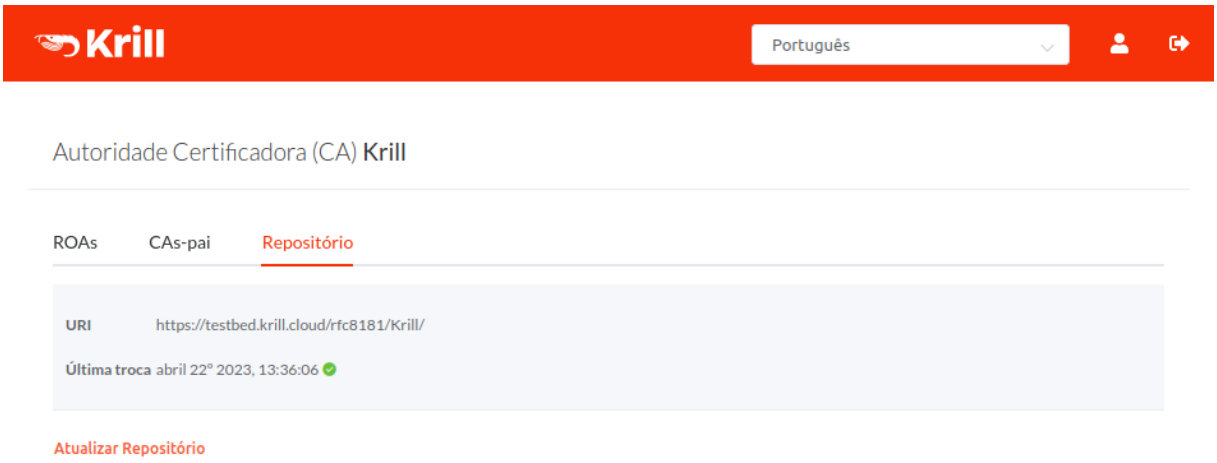
Na falta de mecanismos de validação de origem intrínsecos ao BGP, a infraestrutura RPKI apresenta a resolução para este problema provendo mecanismos para que os roteadores envolvidos em sessões BGP validem os anúncios de rotas recebidos. Em conjunto com políticas de roteamento, a validação de rotas resguarda

os anúncios legítimos na tabela de roteamento BGP de um roteador, ao passo que pode descartar os anúncios de rotas ilegítimas.

Ao levar esta implementação para o contexto apresentado no ambiente de testes, o AS64516 deve certificar seus Recursos de Número da Internet com a Autoridade Certificadora do qual é membro e publicar seus recursos em repositórios RPKI. Na Internet, como descrito na seção 5.1, os Registros Regionais de Internet assumem a posição de Âncoras de Confiança e fornecem serviços de certificação e publicação dos recursos para os Sistemas Autônomos.

No ambiente de testes, o software Krill foi instalado em um servidor virtualizado e será utilizado como C.A e executará a publicação dos objetos RPKI em repositórios. O repositório de publicação, de acordo com a Figura 15, é fornecido por uma plataforma de experimentos (*testbed*) do software Krill. Desse modo, os objetos assinados para os membros deste C.A serão publicados e armazenados no repositório correspondente ao C.A

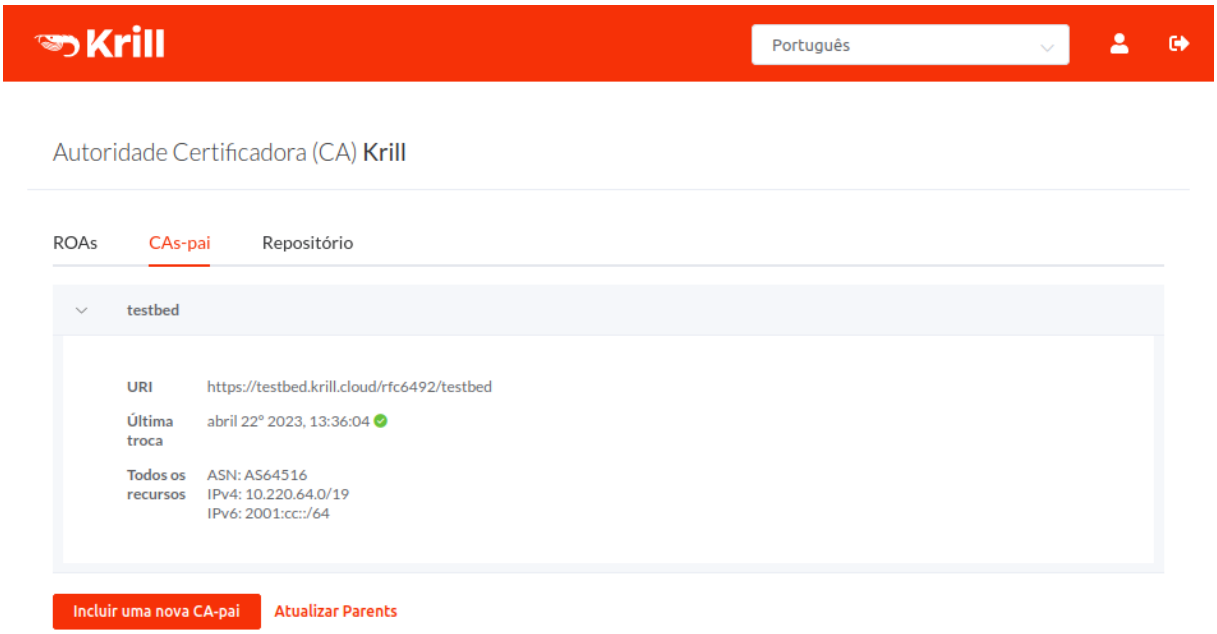
Figura 15 - Repositório RPKI



Fonte: De autoria própria

Um CA-raíz também fornecido através da plataforma de *testbed* do Krill, assume a posição de Âncora de Confiança, portanto, assina os certificados para a CA-filha correspondente a instância implementada no servidor virtualizado do ambiente. Dessa forma, a CA-filha será responsável por certificar os Recursos de Número da Internet de seu membro AS64516. Para esta abordagem, a C.A-filha já se encontra configurada ao respectivo C.A-pai, conforme demonstrado na Figura 16.

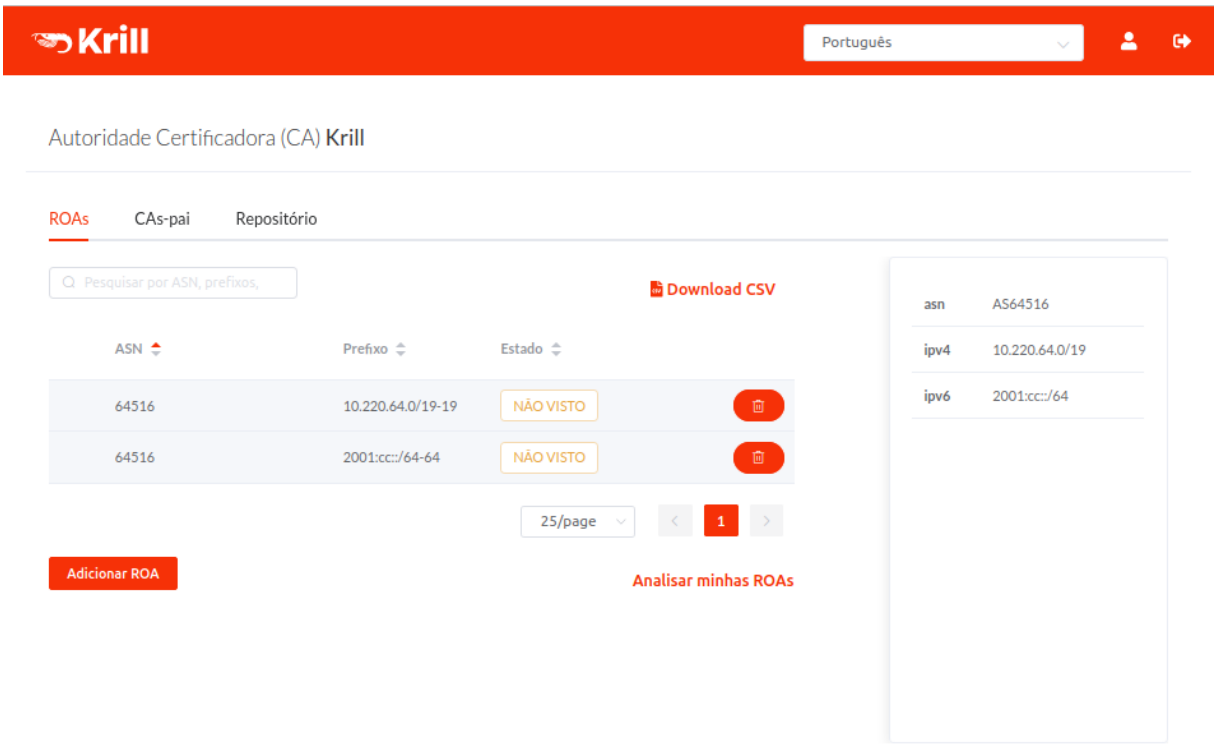
Figura 16 - Associação entre C.A-filha e C.A-pai



Fonte: De autoria própria

A associação do C.A e do repositório de publicação permite ao AS64516 criar e gerenciar *Route Origin Authorization* (ROAs) para os seus prefixos. Os ROAs criados conforme Figura 17 serão publicados no repositório de *testbed* do Krill. Por padrão, o Krill obtém informações dos anúncios BGP do repositório RIPE NIS para atribuir um Estado aos ROAs. Os prefixos utilizados neste ambiente são para finalidade de testes e, portanto, não compartilham informações com o RIPE NIS.

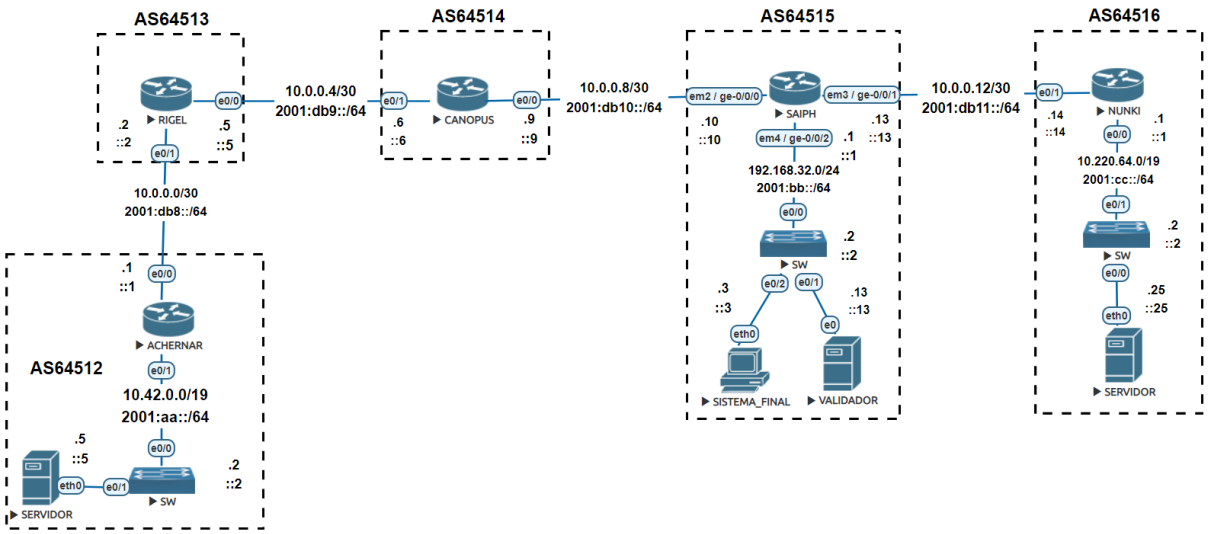
Figura 17 - ROAs criadas no Krill



Fonte: De autoria própria

Com os ROAs correspondentes aos prefixos IPv4 e IPv6 do AS64516 publicados no repositório de teste da autoridade certificadora, esses objetos precisam, de algum modo, chegar ao roteador Saiph do AS64515 que deve utilizá-los como recurso de decisão no roteamento interdomínio do BGP caso necessite encaminhar o tráfego para uma de duas rotas para a rede 10.220.64.0 existentes em sua tabela de roteamento.

Figura 18 - Topologia de rede com validador



Fonte: De autoria própria

Para este propósito, o software *Relaying Party* Fort Validator, executando em um servido nomeado como Validador localizado no domínio do AS64515, conforme ilustra Figura 18, estabelece conexão com repositórios RPKI para obtenção dos ROAs. A Figura 19 exibe os ROAs obtidos no repositório de testes do Krill e armazenadas no cache do servidor de validação. Observe que os dois primeiros registros se referem aos prefixos do AS64516 publicados no repositório de teste do Krill.

Figura 19 - ROAs armazenadas no cache do servidor validação

```
root@validador:/usr/local/etc/fort # jq . roas.json

  "roas"

      "asn"  "AS64516"
      "prefix"  "2001:cc::/64"
      "maxLength"  64


      "asn"  "AS64516"
      "prefix"  "10.220.64.0/19"
      "maxLength"  19


      "asn"  "AS111"
      "prefix"  "192.168.1.0/24"
      "maxLength"  24


      "asn"  "AS23596"
      "prefix"  "1.18.127.0/24"
      "maxLength"  24
```

Fonte: De autoria própria

Os ROAs válidos obtidos do repositório serão fornecidos aos roteadores em sessões de validação providas através do protocolo *RPKI-to-Router* (RTR). Após o estabelecimento da sessão, o roteador estará suscetível a receber as ROAs válidas do cache do servidor de validação. A Figura 20 mostra uma sessão de validação estabelecida no roteador Saiph (AS64515) com o servidor de validação endereçado com o IPv6 2001:bb::13.

Figura 20 - Seção de validação do roteador Saiph

```
AS64515@SAIPH> show validation session
Session                                 State    Flaps     Uptime #IPv4/IPv6 records
2001:bb::13                             Up           0   00:06:04 8/7
```

Fonte: De autoria própria

A Figura 21 mostra que, após o estabelecimento da sessão, ao consultar a base de dados de validação é possível identificar os ROAs válidos e correspondentes aos prefixos IPv4 10.220.64.0/19 e IPv6 2001:cc::/64. Estes são os prefixos legítimos atribuídos ao AS64516 dentro dessa topologia e serão utilizados como filtro para endereçamento do tráfego do AS64515 para a rede 10.220.64.0.

Figura 21 - ROAs validos do AS64516 utilizados no AS64515

```
AS64515@SAIPH> show validation database origin-autonomous-system 64516
RV database for instance master

Prefix                Origin-AS Session                                   State
 Mismatch
10.220.64.0/19-19          64516 2001:bb::13                              valid
2001:cc::/64-64            64516 2001:bb::13                              valid

  IPv4 records: 1
  IPv6 records: 1
```

Fonte: De autoria própria

Para esta topologia foi definida uma política de roteamento que determina ao AS64515 atribuir o status de válido para uma rota quando há um ROA respectivo ao prefixo e comprimento de prefixo dessa rota. Em situações adversas, caso o prefixo e o comprimento de prefixo de uma rota de sua tabela de roteamento seja incondizente

com o prefixo de um ROA válido, a rota será declarada como inválida e descartada na decisão de roteamento BGP.

Como o roteador Saiph possui em sua tabela de roteamento dois prefixos de rotas para a rede 10.220.64.0, mas apenas um deles correspondendo aos critérios de um ROA válido, o prefixo 10.220.64.0/19 do AS64516 será classificado como rota válida. Enquanto o prefixo falso 10.220.64.0/20, que possui correspondência de prefixo, mas não de comprimento de prefixo, será determinado como inválido, conforme exposto na Figura 22.

Figura 22 - Rotas do AS64515 para o prefixo 10.220.64.0/19 após validação

```
AS64515@SAIPH> show route 10.220.64.0/19 all

inet.0: 10 destinations, 11 routes (9 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

10.220.64.0/19     *[BGP/170] 00:08:48, MED 0, localpref 110
                      AS path: 64516 I, validation-state: valid
                    > to 10.0.0.14 via em3.0
10.220.64.0/20      [BGP ] 00:08:53, localpref 9
                      AS path: 64514 64513 64512 I, validation-state: invalid
                    > to 10.0.0.9 via em2.0
```

Fonte: De autoria própria

A influência dos filtros obtidos do RPKI para o roteamento do BGP no AS64515 é visível ao repetir a consulta de melhor rota para a rede 10.220.64.0. O resultado esperado desse comando, ao final desse processo de validação, conforme mostrado na Figura 23, é a indicação de preferência para a rota de prefixo 10.220.64.0/19, representando a rota legítima e pertencente ao AS64516.

Figura 23 - Melhor rota para os prefixos do AS64516

```
AS64515@SAIPH> show route best 10.220.64.0

inet.0: 10 destinations, 11 routes (9 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

10.220.64.0/19     *[BGP/170] 00:07:35, MED 0, localpref 110
                      AS path: 64516 I, validation-state: valid
                    > to 10.0.0.14 via em3.0
```

Fonte: De autoria própria

Podemos concluir, portanto, que ao assinar ROAs para os seus Recursos de Número da Internet, o AS64516 assegurou a legitimidade de seus prefixos. Uma vez que esses ROAs foram publicados em repositório e ficaram disponíveis para serem utilizados como filtro de roteamento, o AS64515 foi capaz de identificar, entre duas rotas para a mesma rede em sua tabela, qual anúncio correspondia ao prefixo legítimo e, consequentemente, descartar o anúncio falso de suas decisões de roteamento.

4 CONSIDERAÇÕES FINAIS

O roteamento na Internet envolve a interação entre diversos Sistemas Autônomos e este trabalho buscou apresentar os sequestros de rota como uma ameaça constante para a segurança e para a estabilidade do roteamento interdomínio. Incidentes dessa categoria podem afetar as mais diversas organizações que dependem da Internet para operar com seus serviços, provocando desde vazamentos ou modificações de dados até indisponibilidade de serviços de rede, resultando em prejuízos financeiros ou de reputação para as organizações acometidas por sequestro de prefixos.

Neste contexto, o RPKI assume grande importância para os Sistemas Autônomos e para todo o roteamento na Internet devido a sua proposta em fornecer uma camada de segurança para o roteamento interdomínio. Ao permitir que um Sistema Autônomo ateste a sua legitimidade sobre os seus recursos através de objetos criptográficos e permitir que esses objetos sejam acessados para consulta e utilização de outros Sistemas Autônomos em suas decisões de roteamento, o RPKI resulta em benefícios sólidos para a integridade do roteamento interdomínio.

Na perspectiva da Segurança da Informação, as soluções providas através do RPKI asseguram diretamente os pilares de confidencialidade, integridade e disponibilidade, quando considerado os riscos aos quais as informações trafegadas de origem e destino estão suscetíveis durante o processo de roteamento interdomínio. A validação de origem de rotas através dos objetos RPKI permitem que as informações sejam encaminhadas de forma segura no roteamento e permaneçam íntegras até um destino legítimo. Isso significa mitigar os riscos de violação, modificação e da disponibilidade das informações e serviços de rede.

Além do baixo custo para implementação, há uma vasta documentação acerca da solução RPKI. Desse modo, ao se considerar os benefícios que garante a um Sistema Autônomo, como a redução de ataques a infraestrutura de roteamento ou de erros de configuração nos serviços de roteamento, a adoção deste mecanismo tem sido cada vez mais incentivada por principais entidades da Internet, como Registros Regionais de Internet, provedores de serviços, conteúdos e outras organizações. Implementar o RPKI em larga escala contribui para uma Internet cada vez mais segura e com alto nível de confiabilidade e resiliência.

REFERÊNCIAS

ALBARQI, A.; ALZAID, E.; ALGHAMDI, F.; ASIRI, S.; KAR, J. **Public Key Infrastructure:** A Survey**.** Journal of Information Security. Disponível em: <https://doi.org/10.4236/jis.2015.61004>. Acesso em: 03 de fevereiro de 2023.

BALAKRISHNAN, H. **Wide-Area Unicast Internet Routing**. Disponível em: < https://users.ece.cmu.edu/~adrian/731-s07/readings/balakrishnan_bgp.pdf>. Acesso em: 15 de março de 2023.

BUTLER, K.; FARLEY, T. R.; MCDANIEL, P.; REXFORD, J. **A survey of BGP security issues and solutions.** Disponível em: <https://ieeexplore.ieee.org/document/5357585>. Acesso em: 16 de fevereiro de 2023.

CHAO, H. J.; LAM, C.; OKI, E. **Broadband Packet Switching Technologies — A Practical Guide to ATM Switches and IP Routers.** New Jersey: John Wiley & Sons, 2001.

CHUNG, T.; ABEN, E.; BRUIJNZEELS, T.; CHANDRASEKARAN, B.; CHOFFNES, D.; LEVIN, D.; MAGGS, B. M.; MISLOVE, A.; RIJSWIJK-DEIJ, R.; RULA, J; SULLIVAN, N. **RPKI is Coming of Age:** A Longitudinal Study of RPKI Deployment and Invalid Route Origins. Disponível em: < https://dl.acm.org/doi/pdf/10.1145/3355369.3355596>. Acesso em: 14 de abril de 2023.

DOYLE, J.; CARROLL, J**. Routing TCP/IP, Volume II: CCIE Professional Development.** 2.ed. Indianapolis: Cisco Press, 2017.

FUROUZAN, B. **Comunicação de Dados e Redes de Computadores.** 4. ed. Porto Alegre: AMGH, 2008.

HAAG, W.; MONTGOMERY, D.; TAN, A.; BARKER, W. **NIST SP 1800-14A:** Protecting the Integrity of Internet Routing: Border Gateway Protocol (BGP) Route Origin Validation. Disponível em: <https://doi.org/10.6028/NIST.SP.1800-14>. Acesso em: 08 de fevereiro de 2023.

HUSTON, G. **A survey on securing inter-domain routing:** Part 1. 2021. Disponível em: <https://blog.apnic.net/2021/07/08/a-survey-on-securing-inter-domain-routing-part-1/>. Acesso em: 16 de fevereiro de 2023.

KUROSE, J. F.; ROSS, K. W. **Redes de computadores e a Internet: uma abordagem top-down.** 6. ed. São Paulo: Pearson, 2013.

LAD, M.; OLIVEIRA, R.; ZHANG, B.; ZHANG, L.; **Understanding Resiliency of Internet Topology against Prefix Hijack Attacks.** Disponível em: <https://ieeexplore.ieee.org/document/4272988>. Acesso em: 17 de março de 2023.

MASOOD, M.; ABUHELALA, M.; GLESK, I**. A comprehensive study of Routing Protocols Performance with Topological Changes in the Networks**. Disponível em: <https://www.researchgate.net/publication/306323407_A_comprehensive_study_of_Routing_Protocols_Performance_with_Topological_Changes_in_the_Networks>. Acesso em: 05 de março de 2023.

MURPHY, S. **RFC 4274:** BGP Security Vulnerabilites Analysis. Disponível em: < https://www.rfc-editor.org/rfc/rfc4274>. Acesso em: 11 de março de 2023.

NIC.br; CGI.br. **Fascículos sobre a Infraestrutura da Internet: Endereços IP e ASN - Alocação para Provedores Internet (Versão 2).** Disponível em: <https://www.nic.br/publicacao/fasciculos-sobre-a-infraestrutura-da-internet-enderecos-ip-e-asns-alocacao-para-provedores-internet/>. Acesso em: 26 de fevereiro de 2023.

NCC, RIPE. **YouTube Hijacking:** A RIPE NCC RIS case study. Disponível em: <https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study>. Acesso em: 14 de março de 2023.

OSUNADE, O. **A Packet Routing Model for Computer Networks.** International Journal of Computer Network and Information Security. Disponível em: <https://www.mecs-press.org/ijcnis/ijcnis-v4-n4/IJCNIS-V4-N4-2.pdf>. Acesso em: 15 de abril de 2023.

PHOOKER, A. **Interdomain routing security:** Motivation and challenges of RPKI. Disponível em: <https://www.researchgate.net/publication/264970579_Interdomain_routing_security_Motivation_and_challenges_of_RPKI>. Acesso em: 10 de março de 2023.

REGISTRO.BR. **RPKI - Numeração**. Disponível em: <https://registro.br/tecnologia/numeracao/rpki/>. Acesso em: 10 de março de 2023.

REKHTER, Y.; LI, T.; HARES, S. **RFC 1771:** A Border Gateway Protocol 4 (BGP-4). Disponível em: <https://www.ietf.org/rfc/rfc4271.txt>. Acesso em: 19 de março de 2023.

SCHILLER, J. et al. **CSRIC III WORKING GROUP 4 Network Security Best Practices FINAL Report–BGP Security Best Practice.** Disponivel em: <https://storage.googleapis.com/pub-tools-public-publication-data/pdf/41862.pdf>. Acesso em: 30 de março 2023.

SIDDIQUI, A. **For 12 Hours, Was Part of Apple Engineering's Network Hijacked by Russia's Rostelecom?.** Disponível em: <https://www.manrs.org/2022/07/for-12-hours-was-part-of-apple-engineerings-network-hijacked-by-russias-rostelecom/>. Acesso em: 27 de março de 2023.

SOCIETY, INTERNET. **What is BGP prefix hijacking? (Part 1).** Disponível em: < https://www.manrs.org/2020/09/what-is-bgp-prefix-hijacking-part-1/>. Acesso em: 06 de março de 2023.

TANENBAUM, A. **Redes de Computadores.** 6. ed. Porto Alegre: Bookman, 2021.

GLOSSÁRIO

AS: Corresponde a um conjunto de roteadores que seguem uma mesma política de roteamento e que são gerenciados por uma única entidade ou organização.

AS Path: Atributo do BGP que registra os caminhos entre Sistema Autônomos.

Backbone: Parte da infraestrutura de um provedor de serviços de rede que conecta vários pontos de presença e data centers em uma região geográfica ou mesmo em diferentes regiões geográficas.

BGP: Protocolo padrão para roteamento interdomínio.

C.A: Autoridade de certificação de uma infraestrutura de chaves públicas.

EBGP: Sessões BGP entre roteadores de Sistemas Autônomos distintos.

EGP: Protocolos de roteamento executados entre roteadores interdomínio de um Sistema Autônomo.

IBGP: Sessão BGP entre roteadores do mesmo Sistema Autônomo.

IGP: Protocolos de roteamento executados em roteadores internos de um Sistema Autônomo.

IP: Protocolo que permite a comunicação entre dispositivos conectados em rede através do endereçamento lógico.

ISP: Provedor de serviços de Internet.

ROA: Objetos criptográficos que permitem que proprietários de Recursos de Número da Internet especifiquem quais Sistemas Autônomos estão autorizados a anunciar rotas para seus prefixos de IP.

RPKI: Infraestrutura de chave pública que visa garantir a autenticidade e a integridade das informações de roteamento na Internet.

RSYNC: Utilitário que permite a sincronização e transferência de arquivos e diretórios.

TCP: Protocolo de rede com alto nível de confiabilidade utilizado para estabelecer e manter conexões entre processos em uma rede.