Mito da cibersegurança

Introdução

Embora a internet tenha apresentado avanços fenomenais nas últimas décadas, continua frágil e vulnerável a ataques de todas as dimensões até aos dias de hoje. Os utilizadores ficam confusos com o seu funcionamento complexo e muitas vezes não conseguem distinguir entre um ataque de um atacante e uma falha no software de proteção.

Um desses acontecimentos recentes ocorreu a 18 de novembro de 2025, quando a Cloudflare sofreu uma interrupção global que afetou brevemente uma grande parte da internet[1]. Este não foi um incidente isolado. O anterior tinha acontecido apenas oito meses antes, e houve outros antes disso. Da mesma forma, a Amazon Web Services (AWS) tem sofrido interrupções frequentes[2]. Este tipo de interrupção da internet tornou-se quase rotineiro, e a fiabilidade destes serviços, concebidos para proteger contra intrusões cibernéticas, tem sido questionada.

O problema

A vulnerabilidade da internet é um problema há décadas. No ano passado, a Comissão Federal de Comunicações (FCC) emitiu um Aviso de Proposta de Regulamentação (NPRM)[3] que identificava o Protocolo de Gateway de Fronteira (BGP)[4] como o alvo para a mitigação do risco. O Conselho de Arquitetura da Internet (IAB), em representação da comunidade da internet, respondeu com um comentário expressando preocupações[5]. Apesar disso, a Casa Branca publicou um roteiro[6] que se focava na integridade do BGP como meio para melhorar a segurança do encaminhamento da internet.

Neste sentido, é importante ter em conta que o BGP é necessário para transportar pacotes entre Sistemas Autónomos (ASes)[7] que são selecionados pelo Servidor de Nomes de Domínio (DNS)[8], com base em endereços IPv4 atribuídos aos subscritores pelo Protocolo de Configuração Dinâmica de Hosts (DHCP)[9], que foi criado para lidar com a escassez de endereços IPv4. Esta pilha de protocolos resultou numa arquitetura de sistema complexa e vulnerável a ataques por diversos ângulos, cada um dos quais requer uma correção específica.

A solução

Um sistema com falhas convida a uma série interminável de correções e remendos. Uma internet muito mais robusta pode resultar de uma arquitetura simplificada e otimizada que elimine a causa raiz da escassez de endereços IPv4, eliminando assim a necessidade de qualquer um dos quatro protocolos anteriormente mencionados. Este é o resultado de um sistema determinístico denominado EzIP[10].

Evoluções da Tecnologia e da Arquitetura

Quando a internet começou, grandes blocos de endereços IPv4 bem definidos foram alocados aos cinco Registos Regionais da Internet (RIRs). Por exemplo, as curvas de Hilbert[11] que representavam as alocações iniciais da AFRINIC (África), APNIC (Ásia-Pacífico), ARIN (América do Norte), LACNIC (América Latina e Caraíbas) e RIPE (Europa, Médio Oriente e Ásia Central) eram facilmente distinguíveis[12].

Embora cada RIR (Registo Regional da Internet) atribuísse os seus endereços alocados aos Internet Access Providers (IAPs) dentro da sua própria região, os próprios IAPs não eram obrigados a observar a mesma restrição. Isto abriu as portas à fragmentação dos endereços IP, permitindo que a localização física de um assinante não estivesse geograficamente associada à região onde o endereço IP atribuído foi originalmente alocado.

À medida que o conjunto de endereços IPv4 começou a esgotar-se, o DHCP garantiu a continuidade das operações da IAP (Internet Access Provider) reutilizando dinamicamente os endereços IPv4 públicos disponíveis. O DNS foi então introduzido para aliviar a carga sobre os subscritores num ambiente em constante mudança. Como esta combinação de protocolos parecia ir ao encontro das necessidades urgentes da época, tornou-se o elemento fundamental da arquitetura da Internet. (Veja a nota de rodapé para as ramificações desta combinação peculiar.)

Com a concordância das instituições pioneiras em libertar blocos de endereços IPv4 excedentes para leilão público, a fim de aliviar a pressão sobre o esgotamento do conjunto de endereços IPv4, tornou-se impraticável esperar que um endereço IPv4 contivesse qualquer informação significativa de localização física, muito menos a possibilidade de geolocalizar um assinante. Um ramo separado da indústria surgiu para satisfazer esta necessidade. No entanto, a resolução e a precisão dos seus relatórios eram frequentemente questionáveis, na melhor das hipóteses[13].

Ao longo do tempo, os fornecedores de acesso à internet (IAPs) que possuíam um ou mais blocos de endereços IPv4 desenvolveram os seus respetivos esquemas de entrega de pacotes IP. Os blocos de endereços que partilhavam a mesma política de transporte foram agrupados para formar um Sistema Autónomo (AS). Como o alcance de cada AS varia e é geralmente limitado, foi utilizado o protocolo BGP para encaminhar os pacotes IP através das fronteiras dos ASs. Com o aumento do número de ASs, a complexidade do BGP também cresceu, especialmente para pacotes que percorriam distâncias consideráveis, muitas vezes apenas localmente, sem mencionar aqueles destinados a endereços globais que necessitavam de atravessar múltiplas fronteiras de ASs.

Embora cada um destes protocolos seja inerentemente distribuído, as suas operações requerem uma coordenação significativa que depende de esforços centralizados, o que leva ao domínio de um pequeno número de empresas com recursos abundantes, como os operadores de Redes de Distribuição de Conteúdo (CDN)[14], incluindo a Cloudflare, a AWS, etc. Estas empresas tornam-se a infraestrutura central para o transporte de dados na internet.

Contradições

Existem diversas práticas na internet que tornam os seus princípios e funcionamento confusos:

A internet promove a igualdade de oportunidades. No entanto, a Cidade do Vaticano recebe 21,4 endereços IPv4 por habitante, enquanto mais de uma dúzia de entidades não recebem nenhum, e outras nações recebem quantidades variadas entre estes extremos[15]. (Nota: A atribuição de 58,4 endereços às Seychelles é uma anomalia, resultado das empresas que aproveitam o ambiente político local para obter oportunidades globais.)

A conectividade de ponta a ponta foi uma promessa da internet. No entanto, o seu modelo de operação predominante atual, as redes de distribuição de conteúdos (CDN), impede que este objetivo seja alcançado, mesmo dentro de uma comunidade local.

A internet surgiu como uma alternativa ao monopólio das empresas de telecomunicações e à regulação governamental sobre a Rede Pública de Telefonia Comutada (PSTN). No entanto, a internet é hoje dominada por conglomerados multinacionais, que praticamente monopolizam os seus respetivos setores de negócio, ao ponto de ignorarem responsabilidades e de contornarem regulamentos. Esta centralização não contradiz precisamente a visão de uma internet distribuída?

Além disso, o potencial de aproximadamente 200 jurisdições globais fragmentarem a internet, transformando-a numa "Splinternet" geopolítica[16], está a ser criticado pela comunidade da internet, enquanto os Sistemas Autónomos (ASes) já transformaram a internet numa rede complexa com pelo menos 77 mil camadas[7]. Ademais, como a maioria dos ASes serve seletivamente apenas partes do mundo, cada camada desta complexa estrutura assemelha-se mais a uma rede de pesca parcial com buracos!

O facto mais intrigante é que a internet defende veementemente o seu princípio de ausência de fronteiras, enquanto o seu principal mecanismo de encaminhamento evoluiu para o BGP, onde o "B" representa precisamente as fronteiras em torno de cada sistema autónomo (AS)!

Em suma, devido à natureza altamente complexa, dinâmica e distribuída destes protocolos, a internet torna-se suscetível a uma vasta gama de violações de segurança maliciosas, desde o assédio diário até aos ataques de ransomware.

Talvez seja prudente referir neste momento que, de alguma forma, o IPv6, sem aproveitar o seu vasto espaço de endereçamento, adoptou as práticas do IPv4, desenvolvidas para fazer face a necessidades temporárias. Ora, a importância do IPv6 parece estar a diminuir discretamente[17], e já não se fala na data de desativação do IPv4. Uma vez que o IPv6 não apresenta vantagens assinaláveis em relação ao IPv4, a maioria das discussões atuais sobre a internet já não faz distinção entre os dois protocolos.

Referências

1. Cloudflare Histórico de interrupções (2019-2025)
   https://controld.com/blothe/biggest-cloudflare-outages/

2. Um histórico de interrupções na cloud e nos centros de dados da AWS
   https://www.datacenterknowledge.com/outages/a-history-of-aws-cloud-and-data-center-outages

3. Relatório sobre o progresso na mitigação de riscos do Protocolo Border Gateway; Encaminhamento seguro da Internet
   https://www.federalregister.gov/documents/2024/06/17/2024-13048/reporting-on-border-gateway-protocol-risk-mitigation-progress-secure-internet-routing

4. Protocolo de gateway de fronteira
   https://en.wikipedia.org/wiki/Border_Gateway_Protocol

5. Comentários da Internet Society, do Internet Architecture Board e da Internet Corporation for Assigned Names and Numbers sobre o assunto "Relatório sobre o progresso na mitigação de riscos do Border Gateway Protocol"
   https://datatracker.ietf.org/doc/statement-iab-comments-of-the-internet-society-internet-architecture-board-and-internet-corporation-for-assigned-names-and-numbers-in-the-matter-of-reporting-on-border-gateway-protocol-risk-mitigation-progress/

6. Roteiro para melhorar a segurança do encaminhamento da internet
   https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/09/Roadmap-to-Enhancing-Internet-Routing-Security.pdf

7. Sistema autónomo (Internet)
   https://en.wikipedia.org/wiki/Autonomous_system_(Internet)

8. Sistema de Nomes de Domínio
   https://en.wikipedia.org/wiki/Domain_Name_System

9. Protocolo de Configuração Dinâmica de Host
   https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

10. Uma Internet Determinística
    https://avinta.com/gallery/DeterministicInternet-SPKR.pdf

11. Curva de Hilbert
    https://en.wikipedia.org/wiki/Hilbert_curve

12. Visualização do espaço de endereços IPv4 utilizando curvas de Hilbert
    https://thebayesianobserver.wordpress.com/2011/10/23/121/

13. Geolocalização na Internet
https://en.wikipedia.org/wiki/Internet_geolocation

14. Rede de entrega de conteúdos
https://en.wikipedia.org/wiki/Content_delivery_network

15. Lista de países por atribuição de endereços IPv4
https://en.wikipedia.org/wiki/List_of_countries_by_IPv4_address_allocation

16. Splinternet
https://en.wikipedia.org/wiki/Splinternet

17. Geoff Huston: O passado, o presente e o futuro da Internet
(TM: 1:08:18, "IPv6 – Cada vez mais irrelevante")
https://cloudflare.tv/this-week-in-net/geoff-huston-the-internet-s-past-present-and-future/dg78lmvO

Nota de rodapé

O DHCP e o DNS formam a dupla de tecnologias de internet mais desconcertante que nos acompanha há anos. O DHCP promete privacidade individual ao atribuir endereços IP aos utilizadores de forma dinâmica, conforme a necessidade, mas esta promessa é imediata e completamente anulada pelo DNS, que apresenta, mediante pedido, o endereço IP mais recente atribuído a um determinado utilizador, com base apenas na sua identidade! Isto faz com que os utilizadores comuns se comportem como avestruzes, com a falsa crença de estarem protegidos, ao mesmo tempo que garante o emprego de muitos engenheiros informáticos. Este é um exemplo perfeito do provérbio chinês "Lança contra escudo" (矛盾).

Não obstante, foram sendo construídas camadas adicionais de protocolos baseados neste esquema, desde o AS e o BGP até ao estabelecimento de redes de distribuição de conteúdos (CDN) que possibilitaram o domínio de conglomerados multinacionais, chegando a grandes serviços como o Cloudflare e o AWS, que prometiam fornecer um transporte fiável de pacotes com segurança melhorada. No entanto, a robustez destes serviços tem sido frequentemente questionada. E, quando a internet sofreu violações de segurança, ninguém parecia disposto a assumir responsabilidades e a procurar alternativas para reduzir a vulnerabilidade. Talvez fosse difícil atribuir culpas, uma vez que toda a internet é tão distribuída?

Por outro lado, a configuração atual da internet é um meio ideal para um criminoso, que pode simplesmente assumir qualquer endereço IP fictício como se fosse um assinante comum da internet para iniciar o ataque e depois abandoná-lo, deixando praticamente nenhum registo permanente com identidade válida para rastreio forense.