Mythe de la cybersécurité

Introduction

Bien qu'Internet ait connu des avancées phénoménales au cours des dernières décennies, il reste fragile et vulnérable aux attaques, qu'elles soient de grande ou de petite ampleur. Les utilisateurs sont déconcertés par son fonctionnement complexe et sont souvent incapables de distinguer une intrusion malveillante d'une simple défaillance du logiciel de protection.

Un incident de ce type s'est produit récemment, le 18 novembre 2025, lorsque Cloudflare a subi une panne mondiale qui a brièvement paralysé une grande partie d'Internet[1]. Il ne s'agissait pas d'un incident isolé. Le précédent avait eu lieu seulement huit mois auparavant, et d'autres l'avaient précédé. De même, Amazon Web Services (AWS) a connu de fréquentes interruptions[2]. Ce type de panne Internet est devenu presque monnaie courante, et la fiabilité de ces services, censés protéger contre les intrusions informatiques, est désormais remise en question.

Le problème

La vulnérabilité d'Internet est un problème qui persiste depuis des décennies. L'année dernière, la Commission fédérale des communications (FCC) a publié un avis de proposition de réglementation[3] identifiant le protocole BGP (Border Gateway Protocol)[4] comme cible prioritaire pour atténuer ce risque. L'Internet Architecture Board (IAB), représentant la communauté Internet, a réagi en formulant des observations exprimant ses préoccupations[5]. Malgré cela, la Maison Blanche a publié une feuille de route[6] axée sur l'intégrité du protocole BGP comme moyen de renforcer la sécurité du routage Internet.

À cet égard, il est important de garder à l'esprit que le protocole BGP est nécessaire pour acheminer les paquets entre les systèmes autonomes (AS)[7] sélectionnés par le serveur de noms de domaine (DNS)[8], en fonction des adresses IPv4 attribuées aux abonnés par le protocole DHCP (Dynamic Host Configuration Protocol)[9], conçu pour pallier la pénurie d'adresses IPv4. Cette pile de protocoles a engendré une architecture système complexe, vulnérable aux attaques sous de nombreux angles, chacune nécessitant l'application d'un correctif spécifique.

La solution

Un système défectueux engendre une série interminable de correctifs et de solutions de contournement. Un Internet beaucoup plus robuste peut être obtenu grâce à une architecture simplifiée et rationalisée qui élimine la cause profonde de la pénurie d'adresses IPv4, rendant ainsi inutiles les quatre protocoles mentionnés précédemment. Tel est le résultat d'un système déterministe baptisé EzIP[10].

Évolutions technologiques et architecturales

Aux débuts d'Internet, de grands blocs d'adresses IPv4 bien définis ont été attribués aux cinq registres Internet régionaux (RIR). Par exemple, les courbes de Hilbert[11] illustrant les attributions initiales d'AFRINIC (Afrique), d'APNIC (Asie-Pacifique), d'ARIN (Amérique du Nord), de LACNIC (Amérique latine et Caraïbes) et de RIPE (Europe, Moyen-Orient et Asie centrale) étaient facilement discernables[12].

Bien que chaque registre Internet régional (RIR) ait attribué ses adresses IP aux fournisseurs d'accès Internet (FAI) de sa propre région, ces derniers n'étaient pas tenus de respecter cette même restriction. Cela a ouvert la voie à une fragmentation des adresses IP, permettant ainsi que la localisation physique d'un abonné ne corresponde pas à la région où l'adresse IP lui a été initialement attribuée.

À mesure que le pool d'adresses IPv4 s'épuisait, le protocole DHCP a permis de maintenir les opérations d'accès à Internet en réutilisant dynamiquement les adresses IPv4 publiques disponibles. Le DNS a ensuite été introduit pour simplifier la gestion des connexions pour les abonnés dans cet environnement en constante évolution. Ce duo de protocoles ayant répondu aux besoins urgents de l'époque, il est devenu la base de l'architecture d'Internet. (Voir la note de bas de page pour les conséquences de cette combinaison particulière.)

Lorsque les premières institutions à adopter le protocole IPv4 ont accepté de mettre aux enchères les blocs d'adresses IPv4 excédentaires afin d'atténuer la pression liée à l'épuisement du pool d'adresses IPv4, il est devenu irréaliste de s'attendre à ce qu'une adresse IPv4 contienne des informations de localisation physique significatives, et encore moins de pouvoir géolocaliser un abonné. Une nouvelle branche de l'industrie est née pour répondre à ce besoin. Cependant, la fiabilité et la précision de ses rapports étaient souvent discutables, au mieux[13].

Au fil du temps, les fournisseurs d'accès à Internet (FAI) possédant un ou plusieurs blocs d'adresses IPv4 ont développé leurs propres schémas de routage des paquets IP. Les blocs d'adresses partageant la même politique de transport ont été regroupés pour former un système autonome (AS). Comme la portée de chaque AS est variable et souvent limitée, le protocole BGP a été utilisé pour acheminer les paquets IP au-delà des frontières des AS. Avec l'augmentation du nombre d'AS, la complexité du protocole BGP a également augmenté, notamment pour les paquets parcourant des distances importantes, même localement, sans parler de ceux destinés à des adresses globales et devant traverser plusieurs frontières d'AS.

Bien que chacun de ces protocoles soit intrinsèquement distribué, leur fonctionnement nécessite une coordination importante qui repose sur des efforts centralisés, ce qui conduit à la domination d'un petit nombre d'entreprises disposant de ressources importantes, telles que les opérateurs de réseaux de diffusion de contenu (CDN)[14], parmi lesquels Cloudflare, AWS, etc. Ces entreprises constituent l'infrastructure centrale du transport des données sur Internet.

Contradictions

Il existe un certain nombre de pratiques sur Internet qui rendent ses principes et son fonctionnement difficiles à comprendre :

Internet contribue à égaliser les chances. Cependant, la Cité du Vatican bénéficie d'une allocation de 21,4 adresses IPv4 par habitant, tandis que plus d'une douzaine d'entités n'en reçoivent aucune, et que d'autres nations se situent entre ces deux extrêmes[15]. (Note : L'allocation de 58,4 adresses aux Seychelles est une anomalie, résultant du fait que des entreprises profitent de l'environnement politique local pour saisir des opportunités à l'échelle mondiale.)

Internet avait promis une connectivité de bout en bout. Cependant, son modèle de fonctionnement actuel, basé sur les réseaux de diffusion de contenu (CDN), fait obstacle à cet objectif, même au sein d'une communauté locale.

Internet s'est initialement opposé au monopole des opérateurs de télécommunications et à la réglementation gouvernementale du réseau téléphonique public commuté (RTPC). Pourtant, Internet est aujourd'hui dominé par des conglomérats multinationaux qui monopolisent de fait certains secteurs d'activité, au point d'ignorer leurs responsabilités et de contourner les réglementations. Cette centralisation ne va-t-elle pas précisément à l'encontre de la vision d'un Internet décentralisé ?

Par ailleurs, la possibilité que quelque 200 juridictions mondiales fragmentent Internet pour en faire un « Splinternet » géopolitique[16] est critiquée par la communauté Internet, tandis que les systèmes autonomes (AS) ont déjà transformé Internet en un réseau en couches (type « réseau oignon ») comportant au moins 77 000 couches[7]. De plus, étant donné que la plupart des systèmes autonomes ne desservent que certaines parties du monde, chaque couche de ce réseau ressemble davantage à un filet de pêche troué !

Le fait le plus déconcertant est que l'Internet défend avec vigueur son principe d'absence de frontières, alors que son principal mécanisme de routage a évolué pour devenir le protocole BGP, où le « B » représente précisément les frontières autour de chaque système autonome !

Dans l'ensemble, en raison de la nature dynamique et distribuée de ces protocoles, qui impliquent de nombreux acteurs, Internet devient vulnérable à un large éventail de failles de sécurité malveillantes, allant du harcèlement quotidien aux rançongiciels.

Il est peut-être judicieux de mentionner à ce stade que l'IPv6, sans exploiter pleinement son vaste espace d'adressage, a adopté certaines pratiques de l'IPv4, développées pour répondre à des besoins transitoires. Aujourd'hui, l'importance de l'IPv6 semble s'estomper discrètement[17], et la date de fin de l'IPv4 n'est plus évoquée. Comme l'IPv6 ne présente pas d'avantages notables par rapport à l'IPv4, la plupart des discussions actuelles sur Internet ne font plus de distinction entre les deux protocoles.

Références

1. Cloudflare Historique des pannes (2019-2025)
   https://controld.com/blothe/biggest-cloudflare-outages/

2. Historique des pannes du cloud et des centres de données d'AWS
   https://www.datacenterknowledge.com/outages/a-history-of-aws-cloud-and-data-center-outages

3. Rapport sur les progrès réalisés en matière d'atténuation des risques liés au protocole BGP (Border Gateway Protocol) ; routage Internet sécurisé
   https://www.federalregister.gov/documents/2024/06/17/2024-13048/reporting-on-border-gateway-protocol-risk-mitigation-progress-secure-internet-routing

4. Protocole de passerelle de frontière
   https://en.wikipedia.org/wiki/Border_Gateway_Protocol

5. Observations de l'Internet Society, de l'Internet Architecture Board et de l'Internet Corporation for Assigned Names and Numbers concernant le rapport sur les progrès réalisés en matière d'atténuation des risques liés au protocole BGP (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. Feuille de route pour le renforcement de la sécurité du routage Internet
   https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/09/Roadmap-to-Enhancing-Internet-Routing-Security.pdf

7. Système autonome (Internet)
   https://en.wikipedia.org/wiki/Autonomous_system_(Internet)

8. Système de noms de domaine
   https://en.wikipedia.org/wiki/Domain_Name_System

9. Protocole de configuration dynamique des hôtes
   https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

10. Un Internet déterministe
    https://avinta.com/gallery/DeterministicInternet-SPKR.pdf

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

12. Visualisation de l'espace IPv4 à l'aide des courbes de Hilbert
    https://thebayesianobserver.wordpress.com/2011/10/23/121/

13. Géolocalisation Internet
https://en.wikipedia.org/wiki/Internet_geolocation

14. Réseau de diffusion de contenu
https://en.wikipedia.org/wiki/Content_delivery_network

15. Liste des pays par attribution d'adresses IPv4
https://en.wikipedia.org/wiki/List_of_countries_by_IPv4_address_allocation

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

17. Geoff Huston : Le passé, le présent et l'avenir d'Internet
(TM: 1:08:18, « IPv6 – De plus en plus inutile »)
https://cloudflare.tv/this-week-in-net/geoff-huston-the-internet-s-past-present-and-future/dg78lmvO

Note de bas de page

Le DHCP et le DNS constituent le couple de technologies Internet le plus déroutant qui soit, et ce depuis des années. En effet, le DHCP promet la confidentialité des données en attribuant dynamiquement des adresses IP aux abonnés selon leurs besoins, une promesse immédiatement et totalement annulée par le DNS qui, sur simple demande, fournit la dernière adresse IP attribuée à une entité, en se basant uniquement sur son identité ! Cela donne aux utilisateurs l'illusion d'être protégés, tout en assurant l'emploi de nombreux ingénieurs informaticiens. C'est un parfait exemple du proverbe chinois « La lance contre le bouclier » (矛盾).

Néanmoins, des couches de protocoles supplémentaires basées sur ce schéma se sont progressivement développées, d'AS à BGP, jusqu'à la mise en place de réseaux de diffusion de contenu (CDN) qui ont permis la domination des conglomérats multinationaux, et ce, jusqu'aux principaux services tels que Cloudflare et AWS, qui promettaient un transport de paquets fiable et une sécurité renforcée. Cependant, la robustesse de ces services a souvent été remise en question. Et, lors des incidents de sécurité sur Internet, personne ne semblait disposé à assumer la responsabilité ni à rechercher des solutions alternatives pour réduire la vulnérabilité. Peut-être était-il difficile d'attribuer les responsabilités, étant donné la nature décentralisée d'Internet ?

D'un autre côté, la configuration actuelle d'Internet constitue un outil idéal pour un malfaiteur qui peut simplement utiliser n'importe quelle adresse IP fictive comme s'il s'agissait d'un abonné Internet ordinaire et légitime pour lancer son attaque, puis l'abandonner par la suite, ne laissant pratiquement aucune trace permanente permettant de l'identifier et de le retrouver.