Réorganiser l'Internet

1. Contexte: Malgré l'adoption rapide de l'Internet et son déploiement en tant que de facto infrastructure de communication mondiale, il y a toujours eu une préoccupation quant à sa vulnérabilité aux failles de sécurité. Autrement dit, par rapport au RTPC traditionnel qui est capable de localiser un appelant avant même que l'appel ne soit répondu, pourquoi est-ce que l'Internet prend autant de temps – des jours, des mois ou même plus – pour commencer à spéculer sur l'auteur d'une cyberattaque majeure ?

La cause de ce problème est lié au fait que la conception Internet originale basée sur IPv4 ne disposait pas d'un pool d'adresses suffisamment grand pour identifier explicitement et de manière unique tous les IoT utilisés. Divers dispositifs transitoires ont été élaborés pour faire face à ce probleme. Malheureusement, ils ont également fourni le camouflage parfait pour les auteurs, tandis que les utilisateurs ordinaires étaient vulnérables. Bien que la nouvelle version IPv6 ait plus qu'assez d'adresses pour identifier tous les IoT, l'utilisation des schémas provisoires a persisté. De plus, IPv6 est plus compliqué et coûteux qu'IPv4, ce qui fait que les régions moins fortunées ont du mal à adopter IPv6. Un remplacement complet de n'importe quel grand système utilisé en continu comme l'Internet est hors de question. Pour contourner cette impasse, la seule voie réaliste est un schéma qui peut coexister avec les pratiques actuelles tout en les faisant évoluer vers un système à long terme.

2. Solution: Heureusement, on a découvert qu'une partie importante (un seizième, pour être exact) du pool d'adresses IPv4, appelé netblock 240/4, a été "RÉSERVÉE" pour une "utilisation future" depuis sa création. Par conséquent, aucun des équipements Internet actuels n'est capable de l'utiliser. Cela offre une opportunité unique à une nouvelle classe de routeurs de l'utiliser pour identifier jusqu'à 256 millions d'IoT à partir de chaque adresse IPv4 existante. Correctement administré, un système de communication mondial entièrement adressable de bout en bout pourrait fournir non seulement tous les services souhaités de manière uniforme à chaque abonné, mais aussi atténuer la cause première de vulnérabilité de la cybersécurité, le tout dans le cadre de la technologie IPv4 existante.

3. Déploiement progressif: pour se fondre dans le mode de fonctionnement actuel du serveur-client Internet, l'approche ci-dessus peut être déployée immédiatement avec un « degenerated format », dans lequel le

netblock 240/4 est utilisé comme s'il s'agissait du quatrième pool d'adresses de réseau privé, dans en plus de 192.168/16, 172.16/12 et 10/8. Cette phase d'introduction ne nécessite que l'activation du netblock 240/4, sans rien modifier d'autre dans les conceptions IPv4 existantes.

4. Mise en œuvre: cette approche ne nécessite pratiquement aucun effort d'ingénierie. Le coût de déploiement est le même que celui de l'équipement IPv4 actuel comparable. De plus, les dépenses d'exploitation seront réduites grâce aux pratiques rationalisées qui atténuent les perturbations telles que les cyberattaques :

A. Développement de produits (ProDev) : Désactivez simplement les codes logiciels existants qui ont désactivé l'utilisation du netblock 240/4.

B. Dépenses d'investissement (CapEx) : Identique à l'équipement IPv4 actuel pour la même capacité de service, en utilisant le même matériel.

C. Dépenses d'exploitation (OpEx) : réduites par des pratiques simplifiées ne s'appuyant pas sur des schémas dynamiques.

D. Cybersécurité : Améliorée par l'administration déterministe de l'identification (adresse) de l'IdO.

5. Actions proposées:

A. Avec les caractéristiques inhérentes au démarrage de services Internet à partir d'un réseau privé sans efforts de développement, ce système peut être déployé par toute partie intéressée (agences gouvernementales, entreprises, entrepreneurs, etc.) à partir d'une adresse IPv4 valide disponible en utilisant l'équipement IPv4 existant.

B. Étant donné que cette approche est générique, il est recommandé qu'elle soit examinée par l'UIT-D pour déterminer si elle convient au déploiement universel afin de réorganiser l'Internet.

Les références:

I. État de vulnérabilité de la cybersécurité

https://blog.apnic.net/2021/02/03/the-internet-of-trash/

II. Une démonstration de faisabilité facilement reproductible de cette proposition.

https://www.avinta.com/phoenix-1/home/RegionalAreaNetworkArchitecture.pdf

III. Commentaire sur un blog de l'IAB : proposer ce schéma pour faciliter la participation de l'utilisateur final aux développements de protocoles/produits.

https://blog.apnic.net/2020/08/31/rfc-8890-the-internet-is-for-end-users/

IV. IETF Draft : Détails techniques de cette proposition

https://datatracker.ietf.org/doc/html/draft-chen-ati-adaptive-ipv4-address-space

V. Propriété intellectuelle : Brevet américain n° : 11,159,425

Terminologie, abréviation et acronyme:

. CG-NAT: traduction d'adresses réseau de qualité opérateur

. DHCP: protocole de configuration dynamique de l'hôte

. DNS: système de nom de domaine

. IAB: Conseil d'architecture Internet

. IETF: Groupe de travail sur l'ingénierie Internet

. IoTs: Internet des objets

. IPv4: Protocole Internet version 4

. IPv6: Protocole Internet version 6

. UIT-D: Union internationale des télécommunications – Secteur du développement

. PSTN: Réseau Téléphonique Public Commuté

. 240/4 Netblock: pool d'adresses IPv4 allant de 240.0.0.0 à 255.255.255.255, soit environ 256 millions (256 millions) ou un quart de milliard (0,25 milliard) d'adresses

https://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml