Renove a Internet

1. Antecedentes: Apesar da rápida adoção e ampla implantação da Internet para se tornar a infraestrutura de comunicação mundial de fato, sempre houve uma preocupação incômoda sobre sua vulnerabilidade à violação de segurança. Ou seja, comparado ao PSTN tradicional capaz de localizar o chamador antes mesmo de uma chamada ser atendida, por que a Internet demora tanto tempo, dias, meses ou até mais para começar a especular o autor de um grande ataque cibernético?

A causa desse problema está enraizada no fato de que o design original da Internet baseado em IPv4 não tinha um pool de endereços grande o suficiente para identificar explicitamente e exclusivamente todas as IoTs sendo usadas. Vários esquemas provisórios foram desenvolvidos para lidar dinamicamente com essa desvantagem. Infelizmente, eles também forneceram a camuflagem perfeita para os criminosos, enquanto os usuários comuns eram alvos fáceis ao ar livre. Apesar da nova versão, o IPv6 ter endereços mais do que suficientes para identificar todas as IoTs, de alguma forma o uso dos esquemas provisórios persistiu. Além disso, o IPv6 é mais complicado e caro que o IPv4, tornando as regiões menos afortunadas pressionadas a adotar o IPv6. Uma substituição completa para qualquer grande sistema usado continuamente, como a Internet, está fora de questão. Para contornar esse impasse, um esquema que possa coexistir com as práticas atuais e ao mesmo tempo aperfeiçoá-las em direção a um sistema de longo prazo é o único caminho realista.

2. Solução: Felizmente, descobriu-se que uma parte significativa (um décimo sexto, para ser exato) do pool de endereços IPv4, chamado 240/4 netblock, foi “RESERVADO” para “uso futuro” desde os primeiros dias. Consequentemente, nenhum dos equipamentos de Internet atuais é capaz de usá-lo. Isso oferece uma oportunidade única para uma nova classe de roteadores utilizá-lo para identificar até 256 milhões de IoTs de cada endereço IPv4 existente. Adequadamente administrado, um sistema de comunicação mundial endereçável de ponta a ponta não apenas fornece todos os serviços desejados de maneira uniforme para cada assinante, mas também atenua a causa raiz da vulnerabilidade de segurança cibernética, tudo dentro do escopo da tecnologia IPv4 existente.

3. Implantação em fases: Para combinar com o modo de operação cliente-servidor de Internet atual, a abordagem acima pode ser implantada

imediatamente com um formato degenerado, em que o netblock 240/4 é usado como se fosse o quarto pool de endereços de rede privada, em além de 192.168/16, 172.16/12 e 10/8. Esta fase introdutória requer apenas a habilitação do netblock 240/4, sem modificar mais nada nos designs IPv4 existentes.

4. Implementação: Esta abordagem dificilmente requer qualquer esforço de engenharia. O custo de implantação é o mesmo do equipamento IPv4 atual comparável. E as despesas operacionais serão reduzidas devido às práticas simplificadas que atenuam as interrupções, como ataques cibernéticos:

A. Desenvolvimento de Produto (ProDev): Simplesmente desabilite os códigos de software existentes que estão desabilitando o uso do netblock 240/4.

B. Capital Expenditures (CapEx): Igual aos equipamentos IPv4 atuais para a mesma capacidade de serviço, utilizando o mesmo hardware.

C. Despesas Operacionais (OpEx): Reduzidas por práticas simplificadas que não dependem de esquemas dinâmicos.

D. Segurança Cibernética: Aprimorada pela administração determinística de identificação (endereço) de IoT.

5. Ações propostas:

A. Com as características inerentes de iniciar serviços de Internet a partir de uma rede privada sem esforços de desenvolvimento, este sistema proposto pode ser implantado por qualquer parte interessada (agências governamentais, empresas, empresários, etc.) a partir de um endereço IPv4 válido disponível utilizando equipamentos IPv4 existentes.

B. Como essa abordagem é genérica por natureza, recomenda-se que seja revisada pela ITU-D quanto à sua adequação na implantação universal para renovar a Internet.

Referências:

I. Status de vulnerabilidade de segurança cibernética

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

II. Uma demonstração de viabilidade prontamente replicável desta proposta.

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

III. Comente em um blog do IAB: Propondo este esquema para facilitar a participação do usuário final no desenvolvimento de protocolos/produtos.

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

IV. Minuta do IETF: detalhes técnicos desta proposta

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

V. Propriedade Intelectual: Patente dos EUA Nº: 11.159.425

Terminologia, abreviatura e sigla:

. CG-NAT: Tradução de endereço de rede de nível de operadora

. DHCP: protocolo de configuração de host dinâmico

. DNS: sistema de nomes de domínio

. IAB: Conselho de Arquitetura da Internet

. IETF: Força-Tarefa de Engenharia da Internet

. IoT: Internet das Coisas

. IPv4: Protocolo de Internet versão 4

. IPv6: Protocolo de Internet versão 6

. ITU-D: União Internacional de Telecomunicações – Setor de Desenvolvimento

. PSTN: Rede Telefônica Pública Comutada

. 240/4 Netblock: pool de endereços IPv4 variando de 240.0.0.0 a 255.255.255.255, totalizando aproximadamente 256 milhões (256M) ou um quarto de bilhão (0,25B) de endereços

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