Mito de la ciberseguridad

Introducción

Aunque internet ha experimentado avances extraordinarios en las últimas décadas, sigue siendo frágil y vulnerable a ataques de todo tipo. Los usuarios desconocen su complejo funcionamiento y a menudo no pueden distinguir entre un ataque informático perpetrado por un intruso y un fallo en el software de seguridad.

Uno de estos incidentes recientes ocurrió el 18 de noviembre de 2025, cuando Cloudflare sufrió una interrupción global que afectó brevemente a una gran parte de internet[1]. Este no fue un incidente aislado. El anterior había ocurrido solo ocho meses antes, y hubo otros más con anterioridad. De forma similar, Amazon Web Services (AWS) ha sufrido interrupciones frecuentes[2]. Este tipo de interrupciones de internet se ha vuelto casi habitual, y la fiabilidad de estos servicios, diseñados para proteger contra intrusiones cibernéticas, ha sido puesta en entredicho.

El problema

La vulnerabilidad de internet ha sido un problema durante décadas. El año pasado, la Comisión Federal de Comunicaciones (FCC) emitió un Aviso de Propuesta de Reglamentación (NPRM)[3] que identificaba el Protocolo de Puerta de Enlace de Frontera (BGP)[4] como el objetivo para mitigar el riesgo. La Junta de Arquitectura de Internet (IAB), en representación de la comunidad de internet, respondió con un comentario expresando sus preocupaciones[5]. No obstante, la Casa Blanca publicó una hoja de ruta[6] que se centraba en la integridad del BGP como medio para mejorar la seguridad del enrutamiento en internet.

En este sentido, es importante tener en cuenta que el protocolo BGP es necesario para transportar paquetes entre sistemas autónomos (AS)[7] seleccionados por el servidor de nombres de dominio (DNS)[8], basándose en las direcciones IPv4 asignadas a los suscriptores por el Protocolo de Configuración Dinámica de Host (DHCP)[9], que fue creado para solucionar la escasez de direcciones IPv4. Esta pila de protocolos ha dado lugar a una arquitectura de sistema compleja y vulnerable a ataques desde múltiples frentes, cada uno de los cuales requiere una solución específica.

La solución

Un sistema defectuoso da lugar a una serie interminable de soluciones provisionales y parches. Una Internet mucho más robusta puede lograrse mediante una arquitectura simplificada y optimizada que elimine la causa fundamental de la escasez de direcciones IPv4, lo que anularía la necesidad de cualquiera de los cuatro protocolos mencionados anteriormente. Este es el resultado de un sistema determinista denominado EzIP[10].

Evolución de la tecnología y la arquitectura

Cuando se creó Internet, se asignaron grandes bloques de direcciones IPv4 bien definidos a los cinco Registros Regionales de Internet (RIR). Por ejemplo, las curvas de Hilbert[11] que representaban las asignaciones iniciales de AFRINIC (África), APNIC (Asia-Pacífico), ARIN (América del Norte), LACNIC (América Latina y el Caribe) y RIPE (Europa, Oriente Medio y Asia Central) eran fácilmente distinguibles[12].

Aunque cada RIR asignaba las direcciones IP que le correspondían a los proveedores de acceso a Internet (IAP) dentro de su propia región, estos últimos no estaban obligados a respetar la misma restricción. Esto abrió la puerta a la fragmentación de direcciones IP, permitiendo que la ubicación física de un suscriptor no estuviera geográficamente asociada con la región donde se asignó originalmente la dirección IP.

A medida que el conjunto de direcciones IPv4 comenzó a agotarse, DHCP permitió que las operaciones de IAP continuaran reutilizando dinámicamente las direcciones IPv4 públicas disponibles. Posteriormente, se introdujo DNS para aliviar la carga de los suscriptores ante un entorno en constante cambio. Dado que esta combinación de protocolos parecía satisfacer las necesidades urgentes del momento, se convirtió en el componente básico predeterminado de Internet. (Véase la nota a pie de página para conocer las ramificaciones de esta peculiar combinación).

Tras el acuerdo de las instituciones pioneras en la adopción de IPv4 para liberar bloques de direcciones IPv4 excedentes y subastarlos públicamente con el fin de aliviar la presión sobre el agotamiento del conjunto de direcciones IPv4, dejó de ser práctico esperar que una dirección IPv4 contuviera información significativa sobre la ubicación física, y mucho menos la posibilidad de geolocalizar a un suscriptor. Surgió entonces una rama independiente de la industria para satisfacer esta necesidad. Sin embargo, la resolución y la precisión de sus informes a menudo resultaban cuestionables, en el mejor de los casos[13].

A lo largo del tiempo, los proveedores de acceso a Internet (IAP) que poseían uno o más bloques de direcciones IPv4 desarrollaron sus respectivos esquemas de entrega de paquetes IP. Los bloques de direcciones que compartían la misma política de transporte se agruparon para formar un sistema autónomo (AS). Dado que el alcance de cada AS varía y suele ser limitado, se recurrió al protocolo BGP para reenviar los paquetes IP a través de las fronteras de los AS. A medida que aumentaba el número de AS, también lo hacía la complejidad del BGP, responsable del enrutamiento de los paquetes que recorrían distancias considerables, a menudo solo dentro de la red local, sin mencionar aquellos destinados a direcciones globales que debían cruzar múltiples fronteras de AS.

Si bien cada uno de estos protocolos es inherentemente distribuido, sus operaciones requieren una coordinación significativa que depende de esfuerzos centralizados, lo que conduce al predominio de unas pocas empresas con grandes recursos, como los operadores de redes de distribución de contenido (CDN)[14], entre los que se incluyen Cloudflare, AWS, etc. Estas empresas se convierten en la infraestructura central para el transporte de datos en Internet.

Contradicciones

Existen numerosas prácticas en Internet que hacen que sus principios y funcionamiento resulten confusos:

Internet promueve la igualdad de oportunidades. Sin embargo, la Ciudad del Vaticano recibe 21,4 direcciones IPv4 por habitante, mientras que más de una docena de entidades no reciben ninguna, y otras naciones obtienen asignaciones intermedias[15]. (Nota: La asignación de 58,4 direcciones a Seychelles es una excepción, resultado de que las empresas aprovechan el entorno político local para obtener oportunidades a nivel global).

Internet prometía una conectividad de extremo a extremo. Sin embargo, su modelo de funcionamiento predominante actual, las redes de distribución de contenido (CDN), obstaculiza este objetivo, incluso dentro de una comunidad local.

Internet surgió como una alternativa al monopolio de las compañías telefónicas y a la regulación gubernamental de la red telefónica pública conmutada (PSTN). Sin embargo, ahora Internet está dominada por conglomerados multinacionales que prácticamente monopolizan diversos sectores empresariales, hasta el punto de ignorar sus responsabilidades y eludir las regulaciones. ¿Acaso esta centralización no contradice precisamente la visión de una Internet descentralizada?

Además, la comunidad de internet critica el potencial de que aproximadamente 200 jurisdicciones globales fragmenten internet, convirtiéndola en una "internet fragmentada" con implicaciones geopolíticas[16], mientras que los sistemas autónomos (AS) ya han transformado internet en una red con estructura de capas, similar a una cebolla, con al menos 77.000 capas[7]. Es más, dado que la mayoría de los sistemas autónomos solo dan servicio a partes específicas del mundo, cada capa de esta estructura se asemeja más a una red de pesca parcial con agujeros.

Lo más desconcertante es que Internet defiende con vehemencia su principio de ausencia de fronteras, mientras que su principal mecanismo de enrutamiento ha evolucionado hasta convertirse en BGP, ¡donde la "B" representa precisamente las fronteras que rodean a cada sistema autónomo (AS)!

En general, debido a la naturaleza dinámica y distribuida de estos protocolos, que implican una gran complejidad, Internet se vuelve susceptible a una amplia gama de violaciones de seguridad maliciosas, desde acoso diario hasta ataques de ransomware.

Quizás sea prudente mencionar en este punto que, de alguna manera, IPv6, sin aprovechar su enorme espacio de direcciones, adoptó las prácticas de IPv4, desarrolladas para satisfacer necesidades transitorias. Ahora, la importancia de IPv6 parece estar desvaneciéndose discretamente[17], y ya no se menciona la fecha límite para la transición de IPv4. Dado que IPv6 no presenta ventajas notables sobre IPv4, la mayoría de las discusiones actuales sobre Internet ya no distinguen entre ambos protocolos.

Referencias

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

2. Historial de interrupciones de la nube y los centros de datos de AWS
   https://www.datacenterknowledge.com/outages/a-history-of-aws-cloud-and-data-center-outages

3. Informe sobre los avances en la mitigación de riesgos del Protocolo de puerta de enlace fronteriza; Enrutamiento seguro de 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 puerta de enlace de borde
   https://en.wikipedia.org/wiki/Border_Gateway_Protocol

5. Comentarios de la Internet Society, el Internet Architecture Board y la Internet Corporation for Assigned Names and Numbers sobre el asunto de "Informe sobre el progreso en la mitigación de riesgos del Protocolo de puerta de enlace de frontera (BGP)"
   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. Hoja de ruta para mejorar la seguridad del enrutamiento de 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 nombres de dominio
   https://en.wikipedia.org/wiki/Domain_Name_System

9. Protocolo de configuración dinámica de host
   https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

10. Una Internet determinista
    https://avinta.com/gallery/DeterministicInternet-SPKR.pdf

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

12. Visualización del espacio de direcciones IPv4 mediante curvas de Hilbert
    https://thebayesianobserver.wordpress.com/2011/10/23/121/

13. Geolocalización de Internet
    https://en.wikipedia.org/wiki/Internet_geolocation

14. Red de entrega de contenido
    https://en.wikipedia.org/wiki/Content_delivery_network

15. Lista de países según la asignación de direcciones IPv4
    https://en.wikipedia.org/wiki/List_of_countries_by_IPv4_address_allocation

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

17. Geoff Huston: El pasado, el presente y el futuro de Internet
    (TM: 1:08:18, "IPv6: Cada vez más irrelevante")
    https://cloudflare.tv/this-week-in-net/geoff-huston-the-internet-s-past-present-and-future/dg78lmvO

Nota

DHCP y DNS son la pareja de tecnologías de internet más desconcertante que nos ha acompañado durante todos estos años. DHCP promete privacidad individual al asignar direcciones IP a los usuarios de forma dinámica según sea necesario, solo para que DNS lo anule de inmediato y por completo, revelando, a petición, la última dirección IP asignada a una entidad, ¡basándose únicamente en la identidad de dicha entidad! Esto convierte a los usuarios comunes en avestruces que viven con la falsa creencia de estar protegidos, mientras que mantiene a muchos ingenieros informáticos con trabajo. Este es un ejemplo perfecto del proverbio chino "Lanza contra escudo" (矛盾).

Sin embargo, a partir de este esquema se fueron desarrollando capas adicionales de protocolos, desde AS y BGP hasta la creación de redes de distribución de contenido (CDN) que permitieron el dominio de grandes conglomerados multinacionales, llegando incluso a servicios importantes como Cloudflare y AWS, que prometían un transporte de paquetes fiable con mayor seguridad. No obstante, la solidez de estos servicios ha sido objeto de frecuentes críticas. Y cuando se produjeron fallos en internet, nadie parecía dispuesto a asumir la responsabilidad ni a buscar alternativas para reducir la vulnerabilidad. Quizás resultaba difícil asignar culpas, precisamente por la naturaleza descentralizada de internet.

Por otro lado, la configuración actual de Internet es un entorno ideal para un atacante, quien puede simplemente asumir cualquier dirección IP ficticia arbitraria como si fuera un suscriptor de Internet ordinario y válido para iniciar el ataque, y luego abandonarla, sin dejar prácticamente ningún rastro permanente con una identidad válida que permita su rastreo forense.