DDoS Attacks y Botnets

Rodrigo Peña

Senior Software Engineer II @ ZeroFox

My stats

- Desde los 14 años en la escena.
- **20+** Sitios del estado vulnerados.
- **100+** Targets vulnerados (RCE, SQLi, LPE, Cred. Stuffing).
- Fundador de GamerLive (AS263797) (2010-2019 🪦).
  - Empresa de IaaS para juegos multiplayer.
  - Víctima de muchos ataques DDoS y script kiddies.
-
  -
- Bug Bounty: Fintual (US $150), Buda.com (**US $1000** 🤑).

Availability – ¿por qué importa?

- **Disponibilidad (Availability)** es uno de los tres pilares de la seguridad de la información (CIA triad).
- Garantiza que los **usuarios autorizados** puedan acceder a la información y sistemas **cuando la necesitan**.
- Un ataque DDoS es, en esencia, un ataque directo a este principio:
    - El dato sigue siendo íntegro y confidencial, pero es **inaccesible** para quienes lo necesitan.

Outline

- **i)** Diferencias entre DoS, DDoS y DrDoS
- **ii)** Deep dive en DrDoS
  - Amplificación (PPS vs Gbps/Tbps), IP spoofing y flujo DNS de reflexión
- **iii)** Impacto en la víctima, daño colateral asociado
- **iv)** Mecanismos de defensa
- **v)** Aspecto social/psicológico de los ataques DDoS

DoS / DDoS / DrDoS

- **Denial of Service Attack (DoS)**
  - Comúnmente fallas a nivel de protocolo/aplicación (L4/L7).
  - **Objetivo:** afectar a la disponibilidad del servicio.
  - **Ejemplos:** Slowloris (HTTP), ReDoS, Born to be a Pig (Counter-strike 1.6).

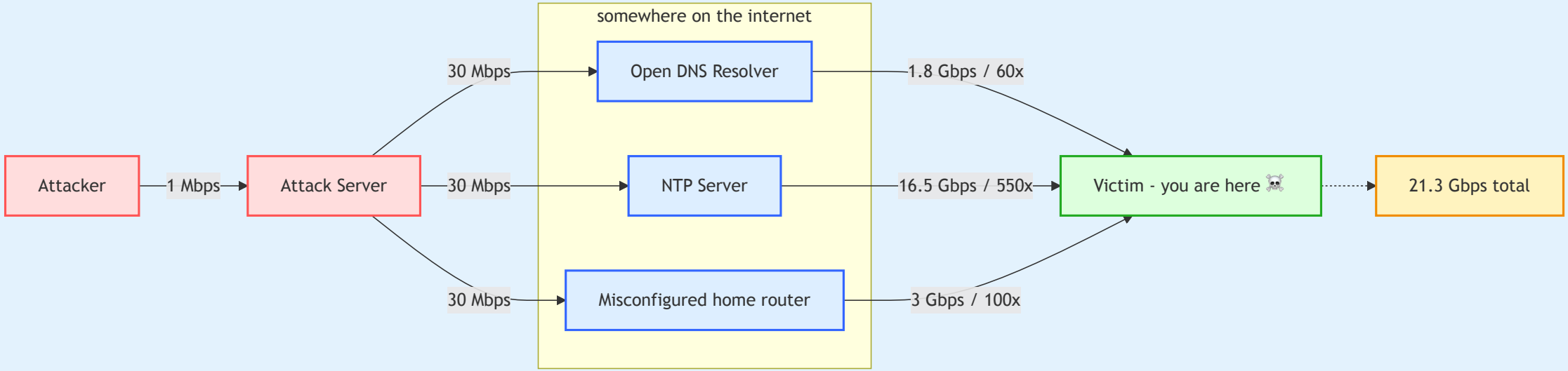
DoS / DDoS / DrDoS

- **Distributed Denial of Service Attack (DDoS)**
  - Comúnmente actua en capas más bajas del modelo OSI (L3/L4/L5).
  - Buscan lograr una ventaja a través de una mayor capacidad de ataque.
    - Muchos destinos envían un payload a la víctima de manera coordinada.
  - **Ejemplos:** Botnets, MagisTV/Bigpanzi (weaponized APK), Suficiente gente enojada y coordinada (LOIC).

DoS / DDoS / DrDoS

- **Distributed Reflection Denial of Service Attack (DDoS)**
  - Abusa de servidores mal configurados para enviar tráfico no solicitado a una víctima.
  - Suele utilizar protocolos diseñados para/durante la internet del pasado.
  - Difícil de localizar / mayor anonimato.
  - **Protocolos:** NTP (550x), DNS (60x), SSDP (100x), SNMP (6x), CHARGEN (400x), ECHO (37x), entre otros.

DoS / DDoS / DrDoS



El diagrama muestra cómo un atacante envía paquetes spoofeados a varios servidores reflectores. Estos servidores, pensando que el origen es la víctima, responden enviando tráfico amplificado hacia la víctima real, saturando su red.

Deep dive into DrDoS

Conceptos importantes

- Packet Amplification - ⬆️ Packets per Second (PPS)
- Bandwidth Amplification - ⬆️ Traffic Volume (Gbps/Tbps)
- IP Spoofing

Deep dive into DrDoS

PPS vs Gbps/Tbps



Software Router

- Ruteo ocurre a nivel de kernel
- Procesa paquetes de manera individual a través de CPU
- Mejor observabilidad



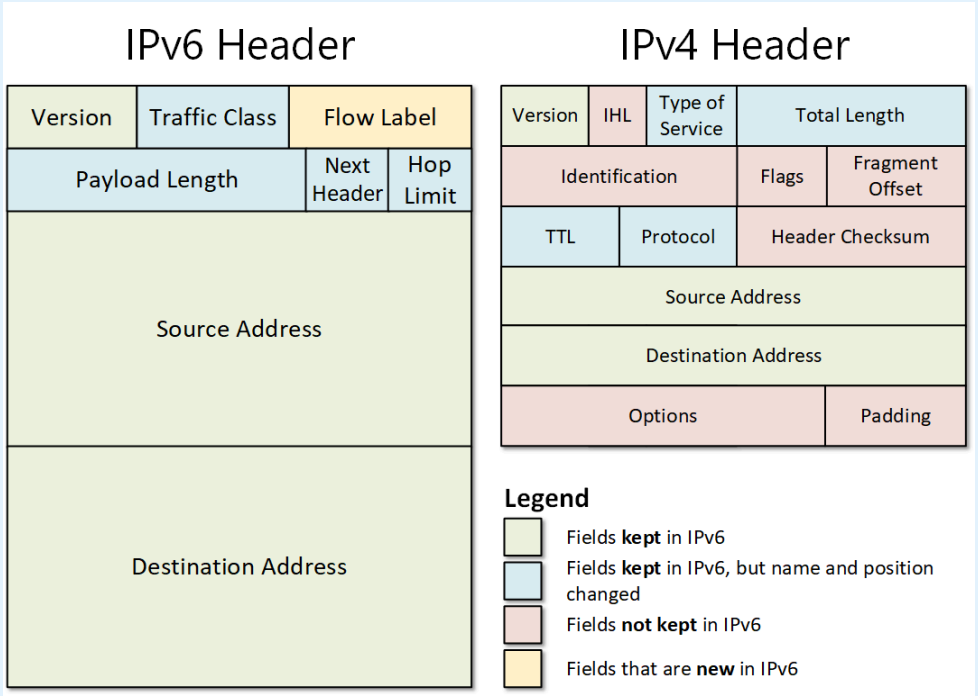
Hardware Router

- Procesa paquetes a través de chip dedicado (ASIC/FPGA)
  - **Tráfico no pasa por CPU**
- Line-rate forwarding
- Menor observabilidad

Nota aparte: pregúntale a ChatGPT cómo el modelo de procesamiento de paquetes en base a vectores está revolucionando la industria de los routers de software.

Deep dive into DrDoS

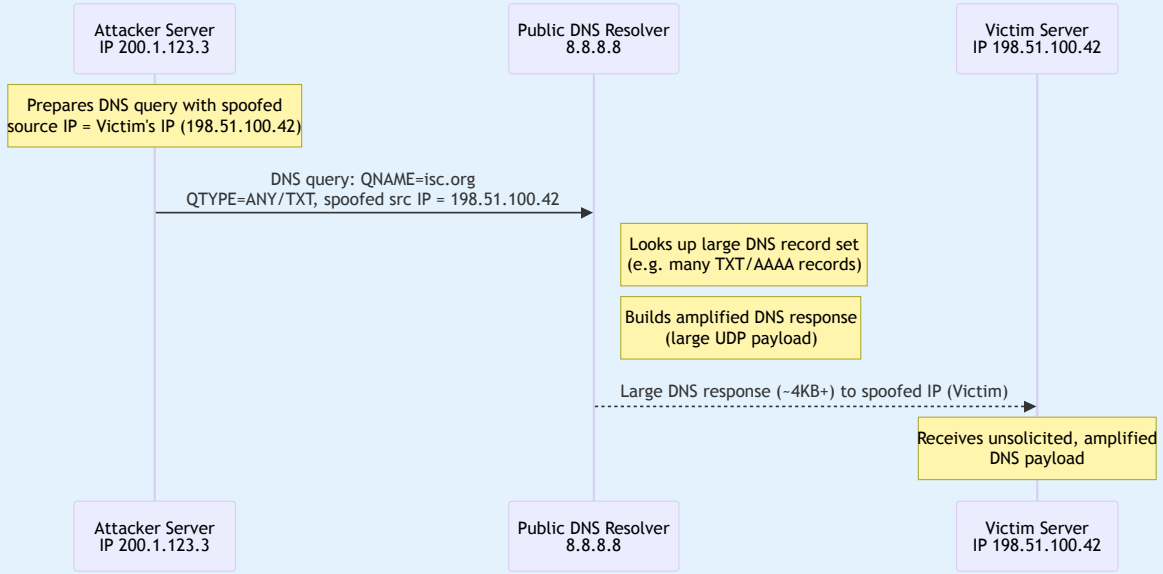
IP Spoofing



- Puedes crear el struct como quieras, pero:
  - Deberás eliminar algunas capas de abstracción para poder enviar el paquete:
    - AF_INET + POSIX sendto()
  - El router podría descartar el envío según el payload.

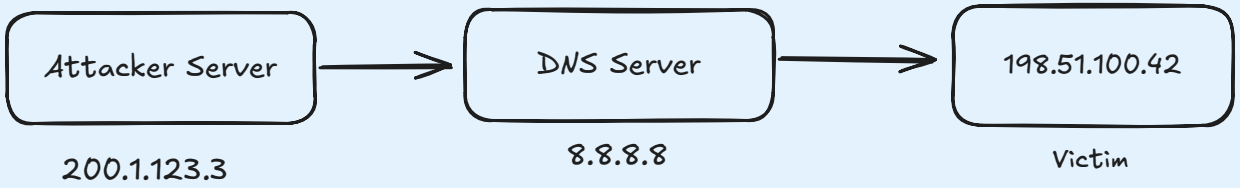
Deep dive into DrDoS

DNS spoofed reflection (DNS → víctima)



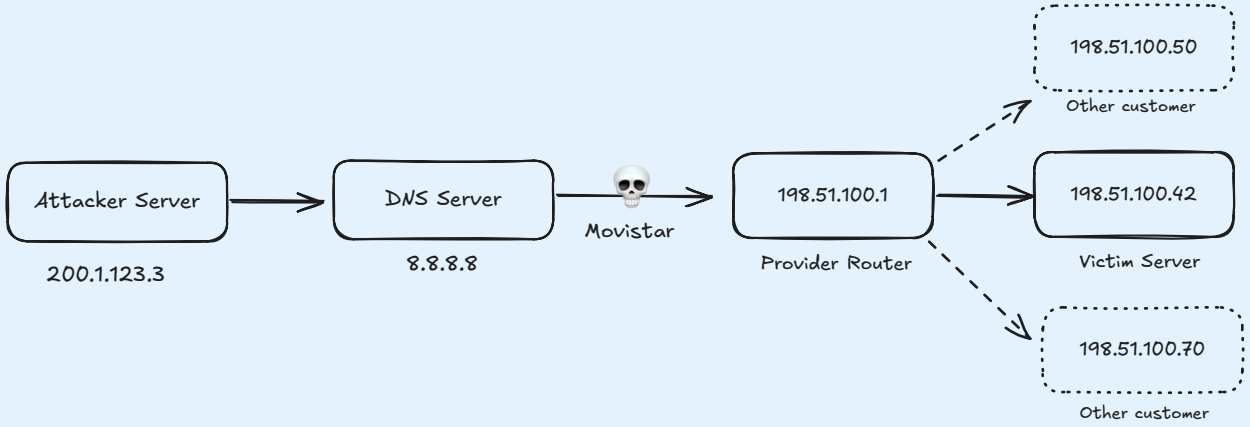
Deep dive into DrDoS

Impacto en la víctima directa



Deep dive into DrDoS

Daño colateral a otros clientes



¿Puede el ataque DDoS no solo botar a la víctima, pero también al proveedor del proveedor?

Deep dive into DrDoS

La red de **Andorra Telecom experimenta desde la mañana del lunes un nuevo ataque de denegación de servicio (DDoS**, por sus siglas en inglés), como ha notificado la compañía proveedora de Internet a través de Twitter.

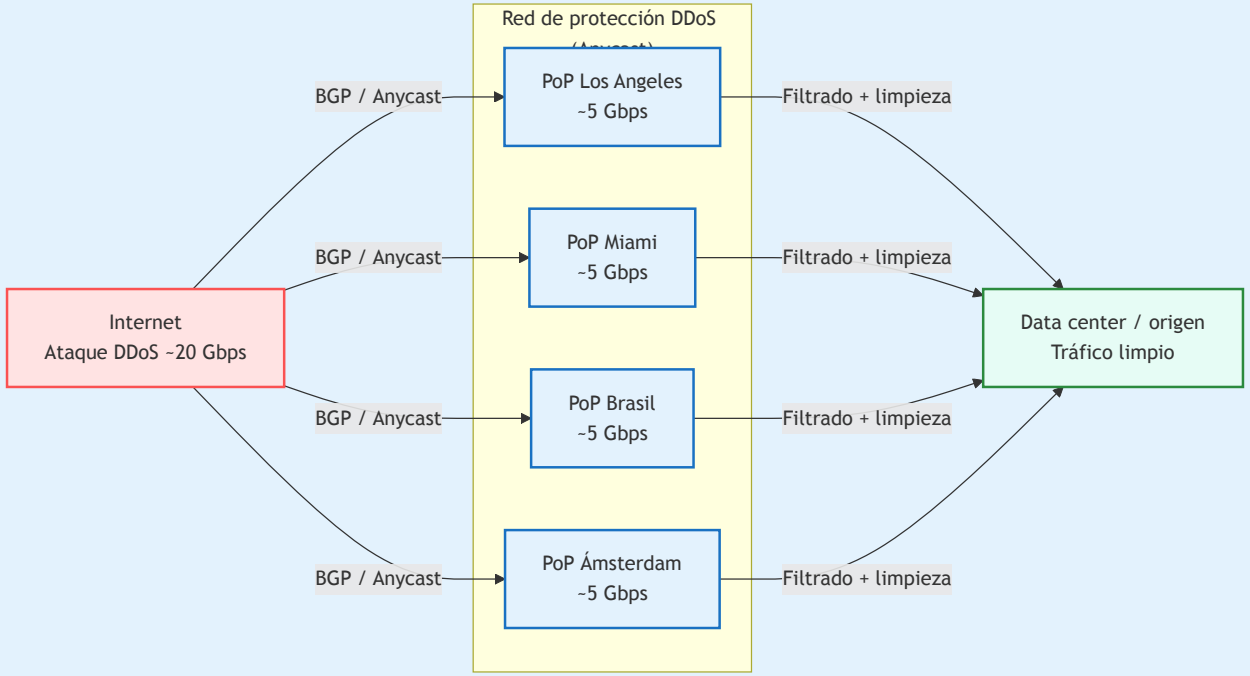
A causa del ataque, algunos usuarios están experimentando **dificultades para acceder a Internet**, lo que incluye también a varios de los 'youtubers' con residencia en Andorra, como Auron Play y El Rubius, entre otros.



Defensa – ¿Qué opciones existen?

- **RTBH (Remote Triggered Blackhole)**
  - Permite avisarle al proveedor que no envíe tráfico dirigido a una cierta IP
    - El atacante gana, pues el servicio pierde totalmente su conectividad.
- **Remote DDoS Protection**
  - Proveedores especializados / scrubbing centers que reciben tu tráfico, lo limpian y te reenrutan solo el tráfico legítimo a través de protocolo IP GRE.
- **Tu propio backbone anycast**
  - Múltiples PoPs / ubicaciones, misma IP anunciada vía BGP para distribuir y absorber ataques volumétricos.
- **Otras capas de defensa**
  - L7 😳

Defensa – Remote DDoS Protection (vista lógica)



Un ataque de ~20 Gbps se "esparce" entre varios Points of Presence (Los Angeles, Miami, Brasil, Ámsterdam), donde se filtra el tráfico malicioso y solo se reinyecta al origen el tráfico legítimo.

Aspecto social/psicológico detras de ataques DDoS

- El poder ejecutar ataques DDoS da status/autoridad en la darknet*
  - *: sólo cuando logra su cometido.
- Son utilizados como medio de venganza, censura, engaño
- El atacante busca recibir un acuso de recibo/feedback sobre el evento
  - Reclamos
  - Noticias
  - Comunicados oficiales

Aspecto social/psicológico detras de ataques DDoS



Cierre – Fin de la Presentación 1

Prompts Interesantes:

- MANRS y BCP38
- Cual fue la motivación del ataque del 2013 a Spamhaus
- Cuentame sobre Paras Jha, y la invención de Mirai
- Que son los bulletproof hostings y por qué son importantes para los ataques DDoS