ESpanix

DDoS – La (no) colaboración
GORE-23

9 abril 2018

DDoS

- Ataques masivos a destinos muy concretos
- Objetivos “subvencionados” por todo tipo de motivos
  - Competencia
  - Derechos
  - Política
  - Activismo
- Uso de botnets desde dispositivos de usuarios finales (PCs, móviles, routers, TVs…)
- Controlados desde los centros de C&C

Dinámica de los ataques

- En los días previos, se hacen unas “Pruebas de Concepto”
  - Volúmenes de tráfico medios, durante varios minutos.
- El día o días del ataque, se activa el DDoS
  - El tráfico se dispara inmediatamente hasta el nivel prefijado.
  - En caso de necesidad (¿contrato?) se eleva a otro salto.
    - P.ej. De 20 Gbps a 40 Gbps
  - El apagado es también instantáneo.
- El objetivo: Colapsar el destino
  - El daño collateral: Colapsar la red del operador que lo conecta.
  - Y los que le conectan a él.
  - Y los IXPs.
  - Y lo que pille por medio…

Qué no funciona

- Filtrar la dirección destino
  - Se colapsará el equipo que aplica el filtro
- Tirar la sesión BGP/bloquear el prefijo en el puerto colapsado
  - El tráfico irá por otro camino, que colapsará
- Lamento colectivo en las listas

Qué debería funcionar (pero no)

- Activar blackholes distribuidos (p.ej. 65535:666)
  - Muy poca adopción por parte de los operadores
  - Muchos ni siquiera son “blackhole friendly” (admitir prefijos /32 para hacer el bloqueo)
- Detectar preventivamente botnets/troyanos y bloquearlos
  - Solo los que lo hacen (pocos)

Qué funciona

- Aumento del ancho de banda
  - A ver quién la tiene más grande…
  - Pasa a ser un “prodo” (el de la pequeña)
- Bloqueo de la IP destino por parte de los ISPs atacantes
  - Ojo, una lista de acceso puede tirar el router
  - Pero, ¿luego cómo se recupera?

Cómo colaboramos en Espanix

- Vender más ancho de banda ☺
- Bloqueo en los switches (blackhole MAC)
- Resolución de blackhole (de IP a MAC)
- Community de blackhole (en route-server)
  - Todo esto requiere, como mínimo, que el operador acepte el anuncio (típicamente /32)
- Eliminado de las IPs de las LANs de intercambio del BGP
  - Pero quedan en riesgo de hijacking…

Y un cambio de política…

- ¿Qué se hace si hay un colapso?
- Hasta ahora, el perjudicado por el ataque era el atacante (ISP)
  - Todo su tráfico, con cualquier destino, se ve afectado.
- Ahora, el perjudicado será el atacado
  - El tráfico de los ISPs no se ve afectado.
- ¿Qué es lo más adecuado?

Gracias por su atención

http://www.espanix.net