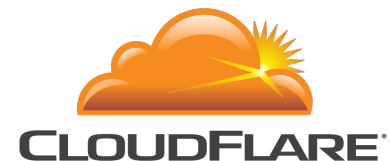


Seguridad y ataques en IPv6

Felipe Tribaldos

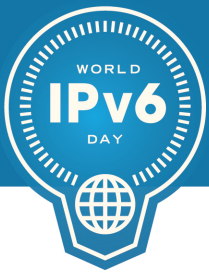
felipe@cloudflare.com

World IPv6 Day 2015



¿Que es CloudFlare ?



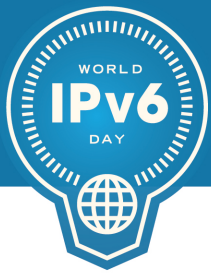


¿Como funciona CloudFlare?

CloudFlare funciona a nivel de la red.

- Un vez habilitado para un sitio web, el trafico es enrutador a través de la red Global de CloudFlare con 32 Centros de Datos a nivel global (5 en la región de LACNIC)
- En cada Centro de Datos, CloudFlare administra DNS, caching, filtrado de seguridad y mitigación contra ataques (IPv4 e IPv6)

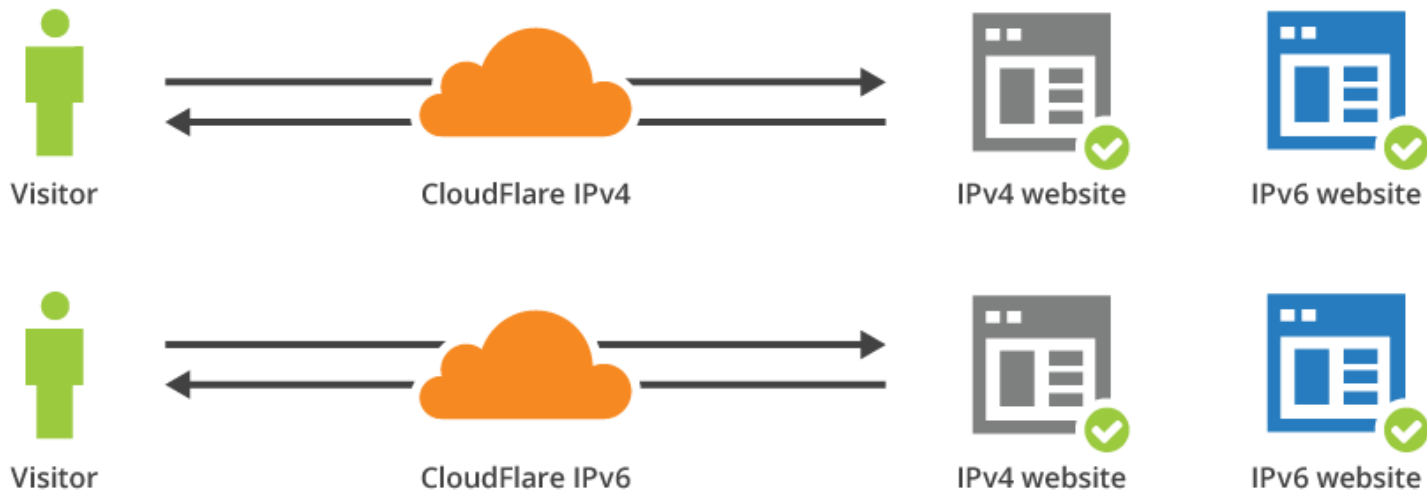


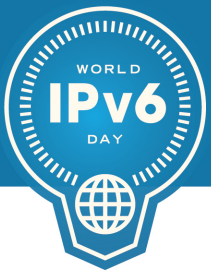


IPv6 Gateway

Introducido en el 2011 CloudFlare ofrece un Gateway de IPv6 automático para habilitar IPv6 para cualquier sitio web.

- No se requiere de hardware, software u otros cambios de infraestructura o hosting.
- Habilitado por defecto en el dashboard de CloudFlare.
- <https://www.cloudflare.com/ipv6>

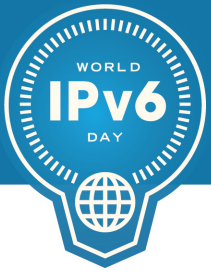




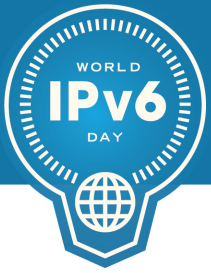
CloudFlare en la región LACNIC



- [Valparaíso, Chile – enero 2014](#)
- [São Paulo, Brazil – julio 2014](#)
- [Medellin, Colombia – July 2014](#)
- [Lima, Peru – diciembre 2014](#)
- [Buenos Aires – abril 2015](#)
- ..

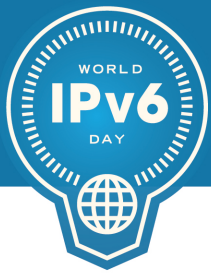


Tráfico IPv6 en la red de CloudFlare



Historia de World IPv6 Day

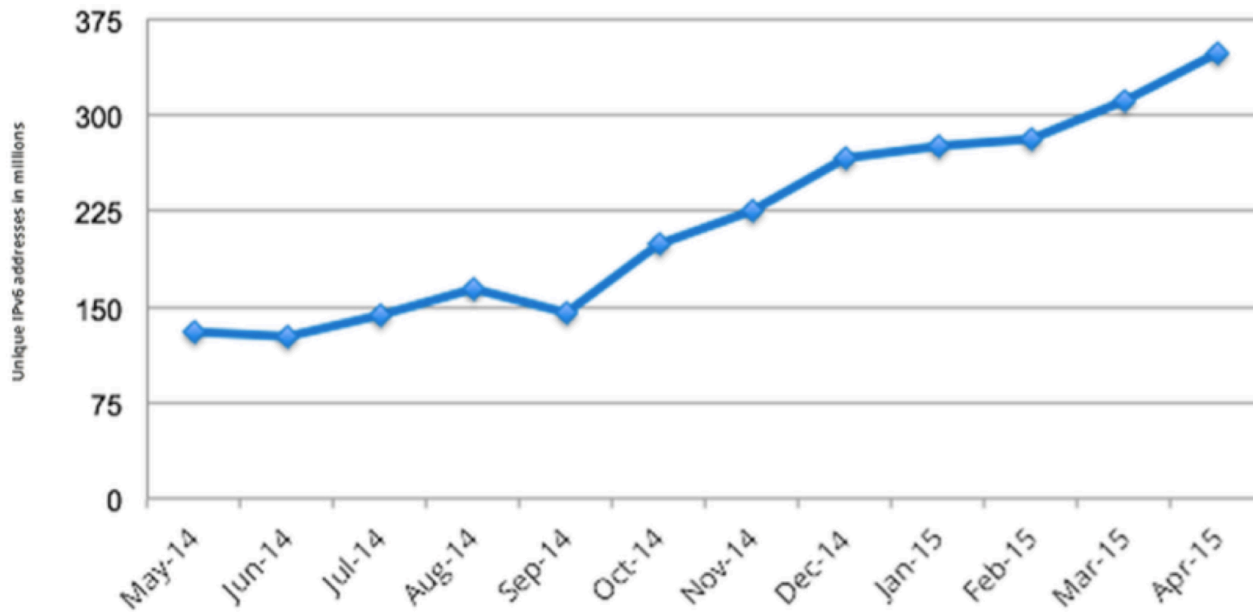
- Primer World IPv6 Day el 6 de junio de 2011. CloudFlare participo.
- CloudFlare Introdujo IPv6 Gateway 27 de sept. de 2011
- World IPv6 Launch en 2012

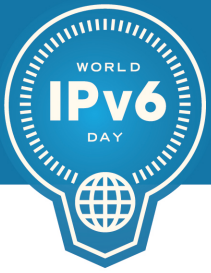


Crecimiento de 166%

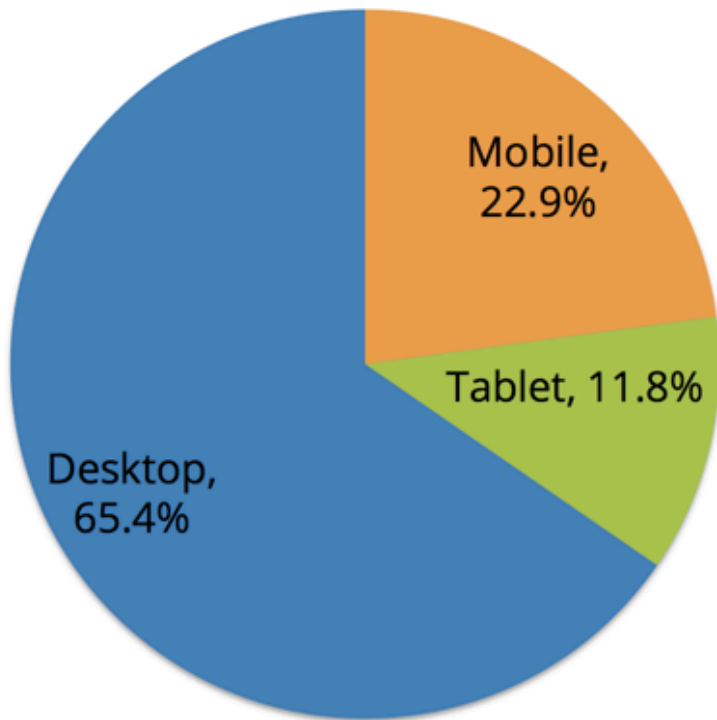
Numero de direcciones IPv6 (/64's) en Millones

166% Growth in unique IPv6 IPs in the last year

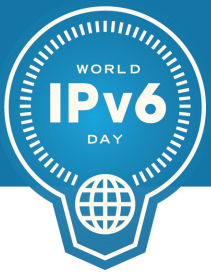




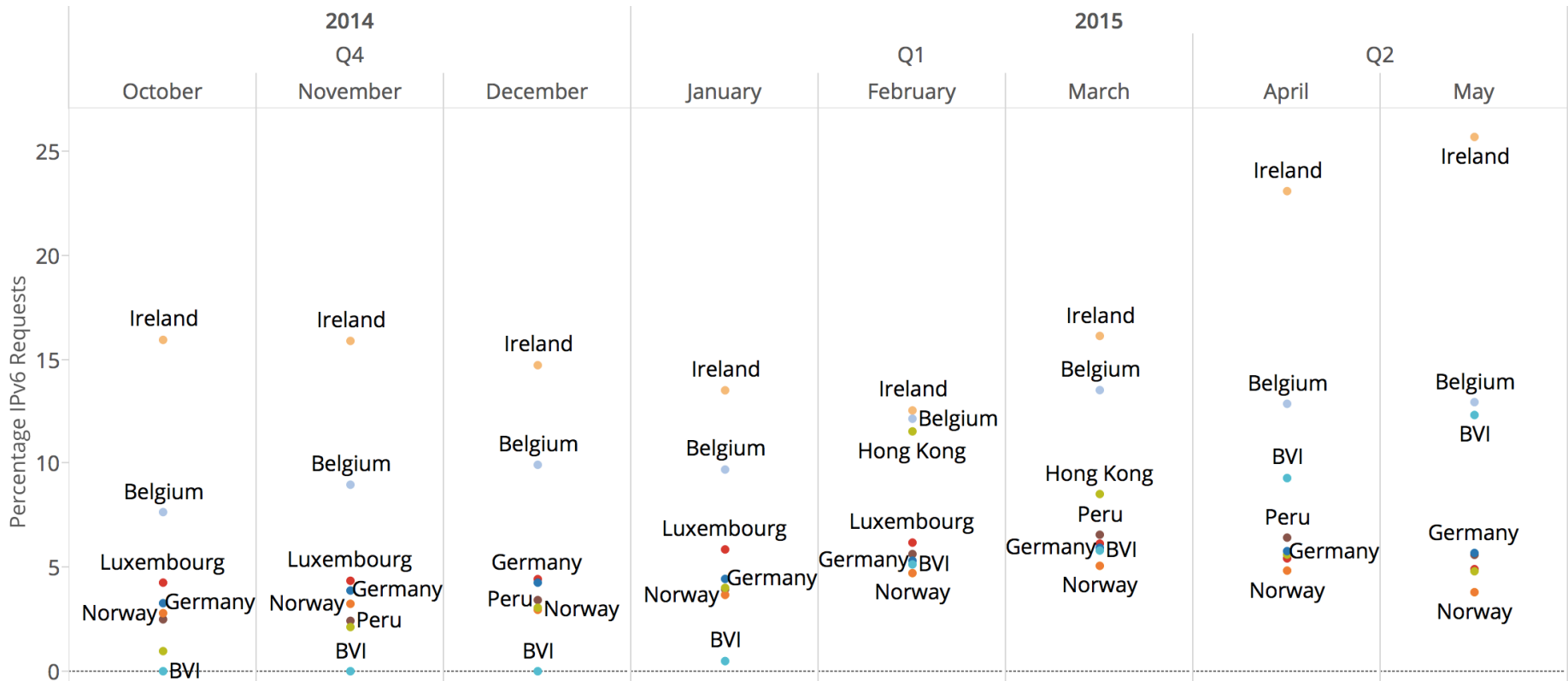
Porcentaje de trafico IPv6 por tipo de dispositivo

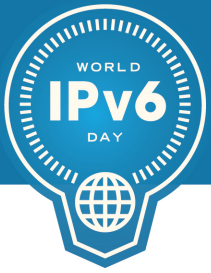


- Muestra un porcentaje importante de trafico móvil.
- Demuestra adopción por operadores Móviles

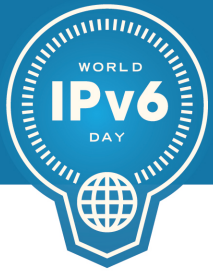


Porcentaje de Trafico IPv6 por País



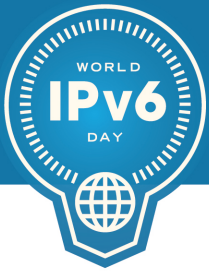


Ataques sobre IPv6 (in the wild)



Ataques sobre IPv6

- En mayor medida los ataques sobre IPv6 son muy parecidos a ataques sobre IPv4
- Por lo general de enfoque reducido debido a menor numero de usuarios finales de IPv6 en la internet.
- Con algunas excepciones de ciertos ataques concentrados en IPv6



Ataques sobre IPv6

- DNS Cache-busting Query attacks
- No solamente de IPv6, pero interesante que se observa sobre IPv6
- Botnets, crean consultas desde resolvers normales, que utilizan subdominios aleatorios que no pueden ser servidos de cache.

Algunos Queries Recibidos

[ebepexklyfaxmloh.www.popvote.hk](#)

[ktylstudkr.www.popvote.hk](#)

[ohunarajmbkrej.www.popvote.hk](#)

[wwtdheilzcv.www.popvote.hk](#)

[zktvvotoyrewaku.www.popvote.hk](#)

.....

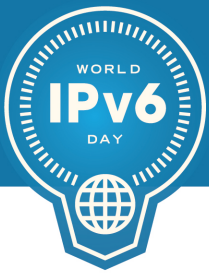
[khyhavsnijslyb.www.popvote.hk](#)

[gchjpexychflvfv.api-token.popvote.hk](#)

[ruqnpvp.api-token.popvote.hk](#)

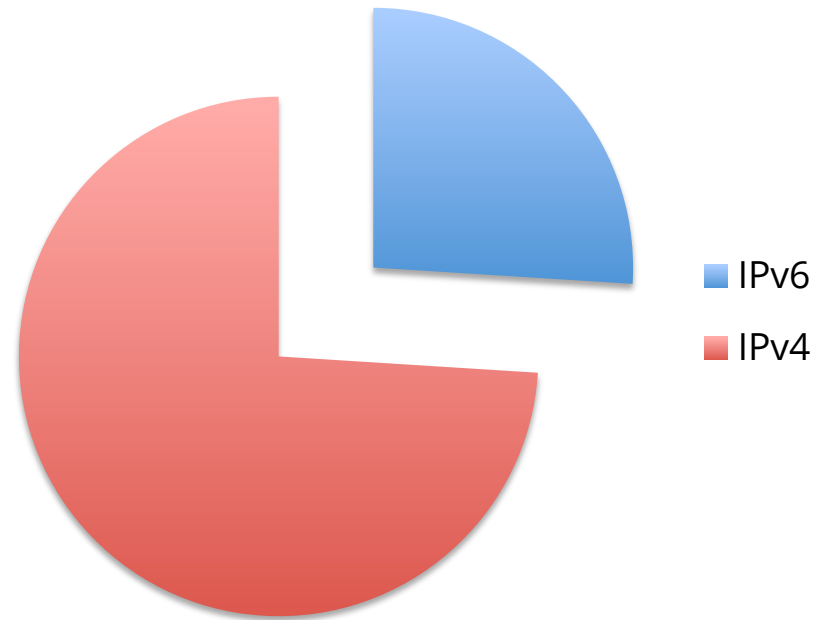
[fapzefvgowzonss.api-token.popvote.hk](#)

[mcvhothfketpgre.api-token.popvote.hk](#)

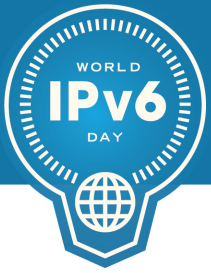


Ataques sobre IPv6

- Observamos una relación igual entre tráfico normal de DNS y tráfico de ataques a la que observamos en el tráfico total (IPv4 vs. IPv6).
- En los ISP's, lo primero que se le habilita IPv6 es la infraestructura propia (ej. Servidores DNS)
- Cuando la infraestructura es Dual-Stack, el abuso sigue de igual medida !

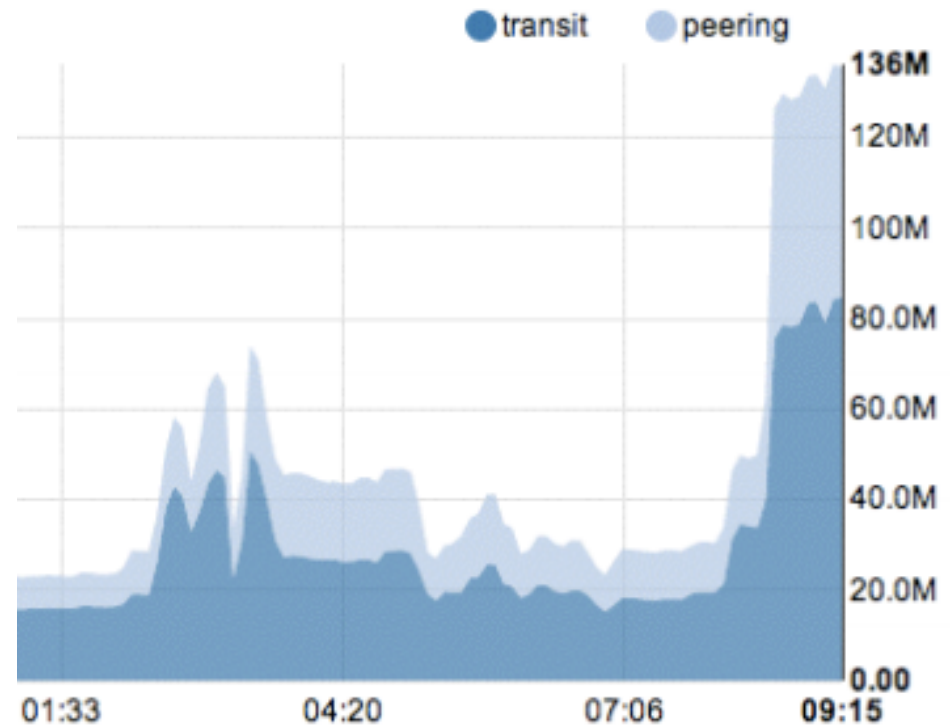


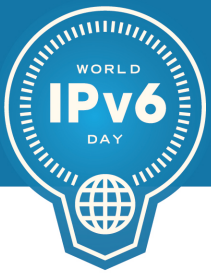
```
$ host ns1.tribaldos.com
ns1.tribaldos.com has address 162.159.0.28
ns1.tribaldos.com has IPv6 address 2400:cb00:2049:1::a29f:1c
```



Ataques sobre IPv6 Observados

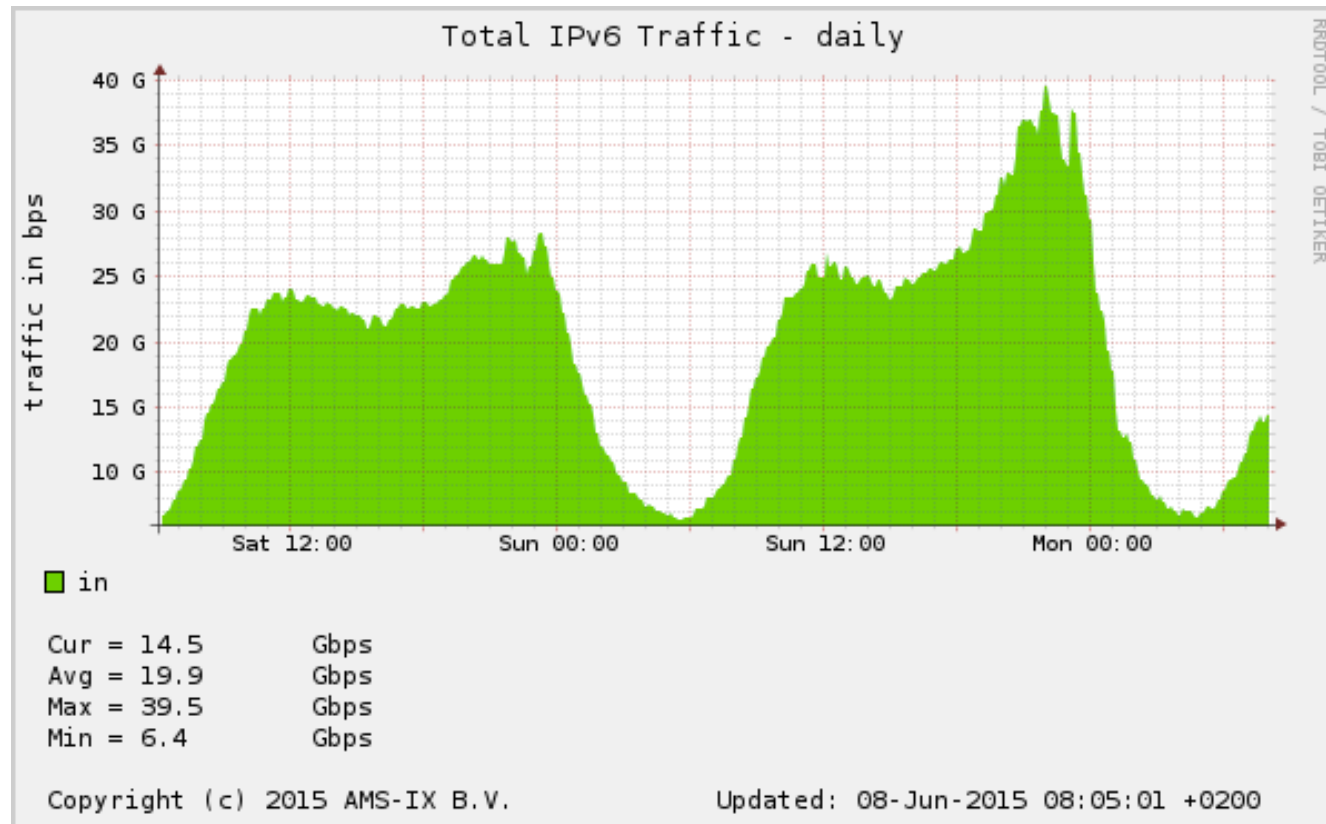
- Estos ataques pueden ser muy efectivos.
- Ataques creciendo a mas de 100M PPS (paquetes por segundo)
- Considerando la relación total entre trafico IPv6 y IPv6
 - Es mas de ~20M PPS de trafico IPv6 !

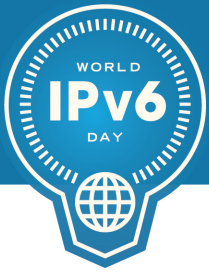




Ataques sobre IPv6 Observados

- Igual al trafico promedio total IPv6 PPS Total en el el AMS-IX (en Amsterdam) !





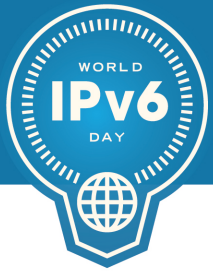
Ataques en IPv6 Observados

- IPv6 SYN Floods (y otros ataques de flooding based)
- La Botnet envía comandos/ataques dirigidos hacia un hostname (ej. example.com)

```
$ host example.com
```

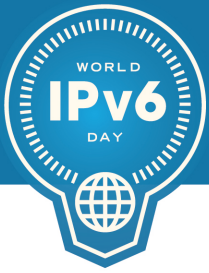
```
example.com has address 93.184.216.119
```

```
example.com has IPv6 address 2606:2800:220:6d:26bf:  
1447:1097:aa7
```



Ataques en IPv6

- El Botnet master posiblemente no envía tráfico intencionalmente hacia hosts IPv6
- Per los bots dentro de la botnet ven las respuestas AAAA y envían tráfico a esas direcciones.
- Selección preferencial de IPv6



Gracias !

Mas Información:

<https://blog.cloudflare.com>

<https://www.cloudflare.com/ipv6>

<https://tribaldos.com>

[@ftribaldos](https://twitter.com/ftribaldos)



CLOUDFLARE®