Identificando servidores DNS Open Resolvers en IPv6

Dario Gomez dario at lacnic dot net
Alejandro Acosta alejandro at lacnic dot net

¿De que se trata esto?

Simple: Como ustedes se imaginan, identificar servidores recursivos en IPv4 es MUY fácil. En IPv6 tuvimos que buscar otra manera

¿Por qué lo hicimos?

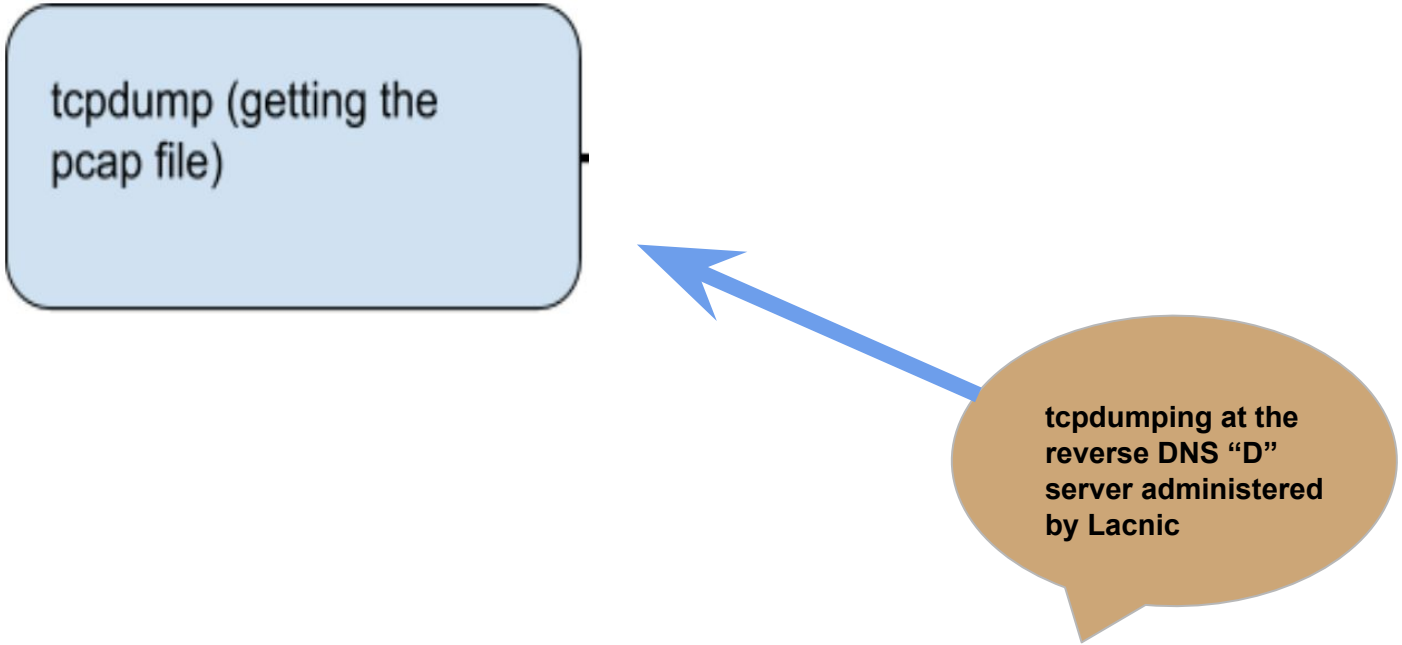
Los servidores recursivos son generalmente negativos:

- Permiten que usuarios externos utilicen sus recursos
- Son susceptibles a ataques de envenenamiento de Cache
- Incrementan los ataques de DDOS & amplificación

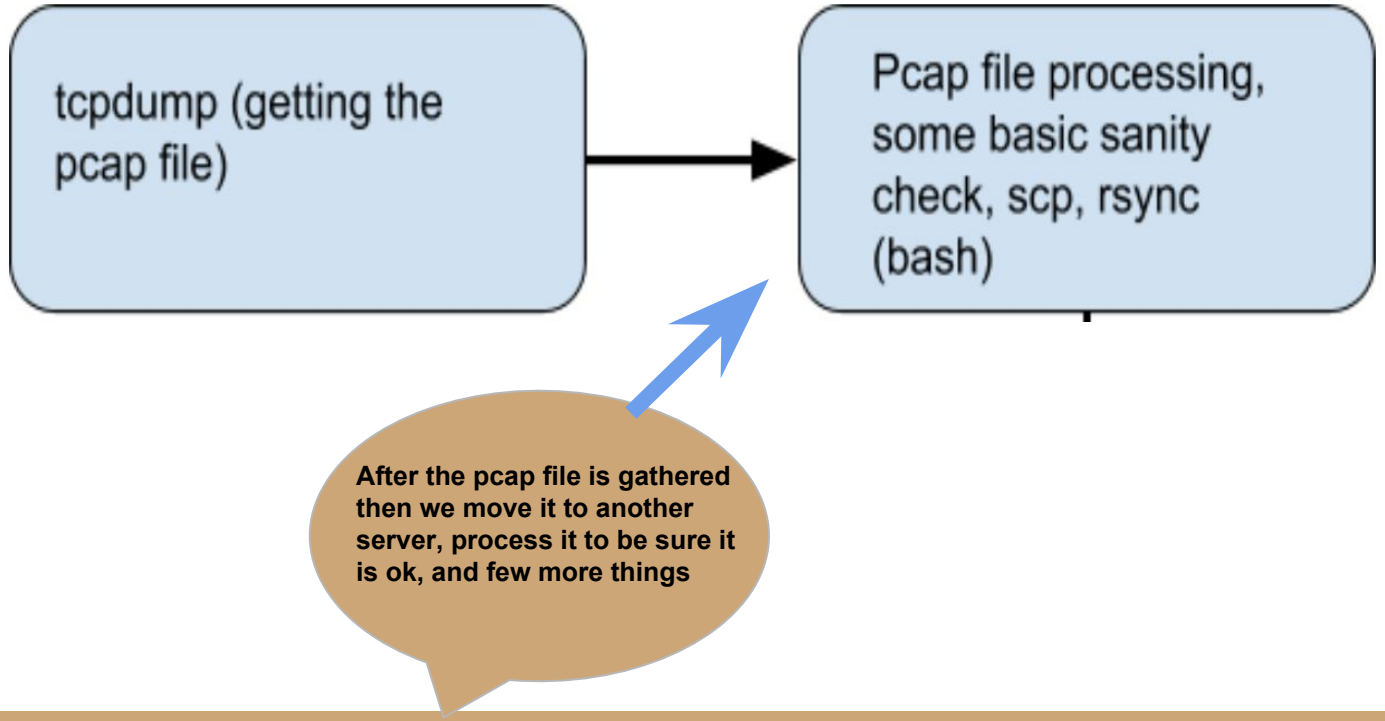
Source: http://dns.measurement-factory.com/surveys/openresolvers.html

Ok.., hemos hablado demasiado!. Qué fue lo que se hizo ! (1/5)

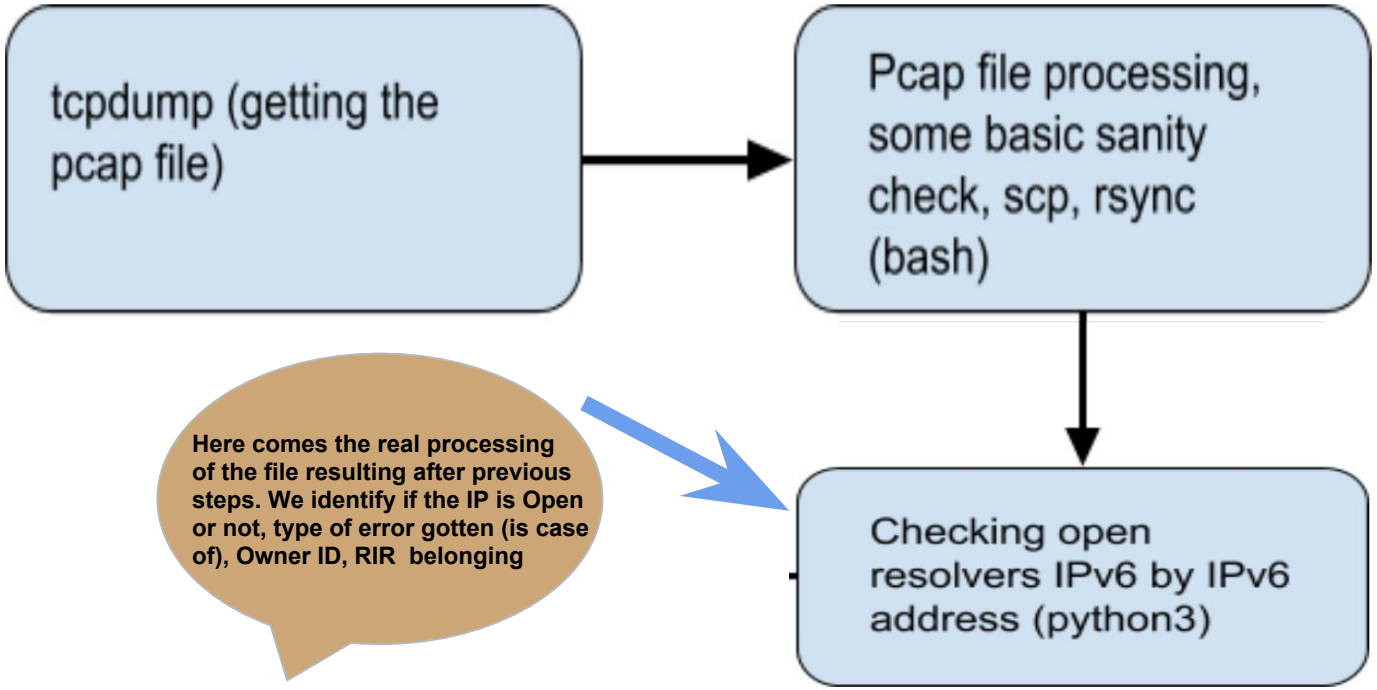
Ok.., hemos hablado demasiado!. Qué fue lo que se hizo ! (2/5)



Ok.., hemos hablado demasiado!. Qué fue lo que se hizo ! (3/5)

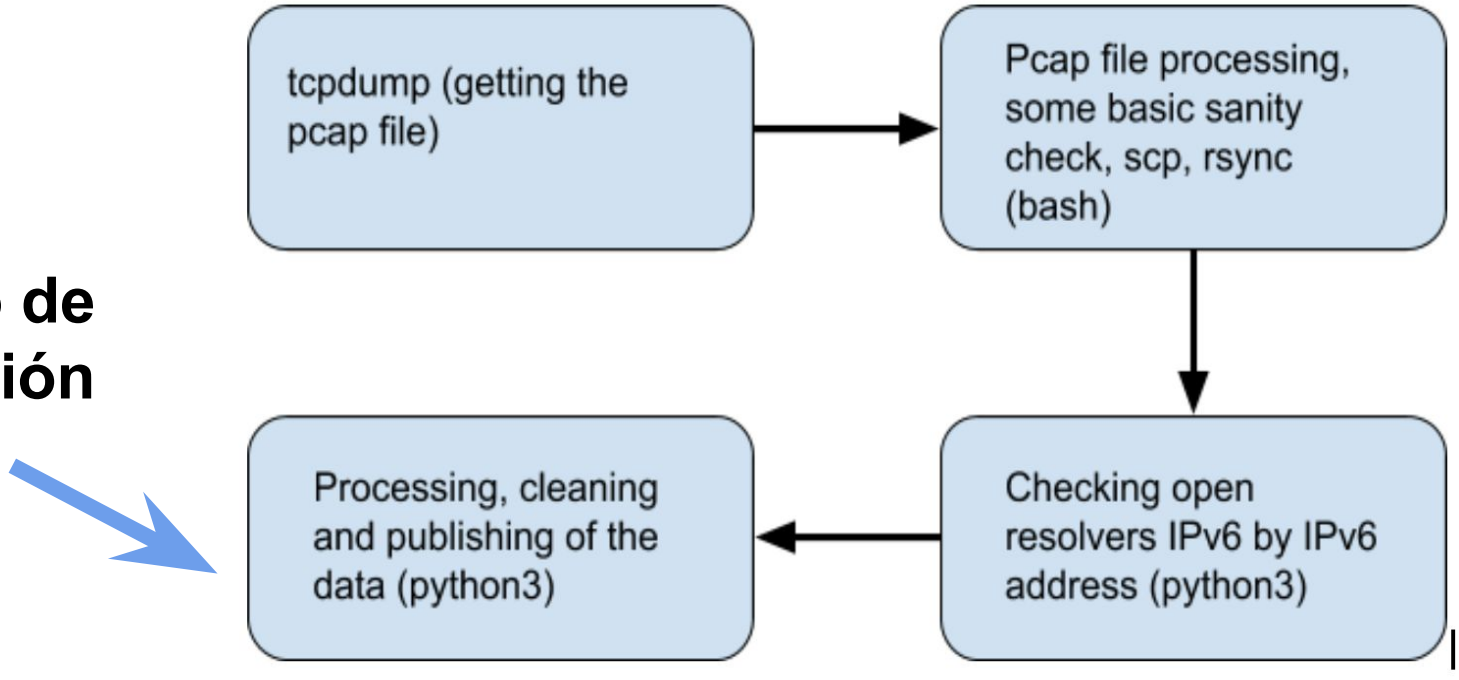


Ok.., hemos hablado demasiado!. Qué fue lo que se hizo ! (4/5)



Ok.., hemos hablado demasiado!. Qué fue lo que se hizo ! (5/5)

Fase en proceso de entonación



Que resultados esperamos (y publicaremos)

.- # de Servidores DNS identificados
.- % de Servidores DNS identificados x RIR
.- % de Servidores abiertos DNS identificados
.- % de Servidores abiertos DNS identificados x RIR
.- Algunos miscelaneos

Resultados parciales

5112 DNS Servers

164 Open Resolvers

4975 Non-Open Resolvers

239 Resolvers in Lacnic region

1489 Resolvers in Arin region

3177 Resolvers in Ripe region

244 Resolvers in APNIC region

17 Resolvers in AFRINIC region

224 Non-Open Resolvers in Lacnic region

15 Open Resolvers in Lacnic region

1423 Non-Open Resolvers in Arin region

78 Open Resolvers in Arin region

17 Non-Open Resolvers in Afrinic region

4 Open Resolvers in Afrinic region

3149 Non-Open Resolvers in Ripe region

36 Open Resolvers in Ripe region

210 Non-Open Resolvers in Apnic region

42 Open Resolvers in APNIC region

Resultados parciales

En la región de Lacnic ya hemos detectado algunos Open Resolvers !

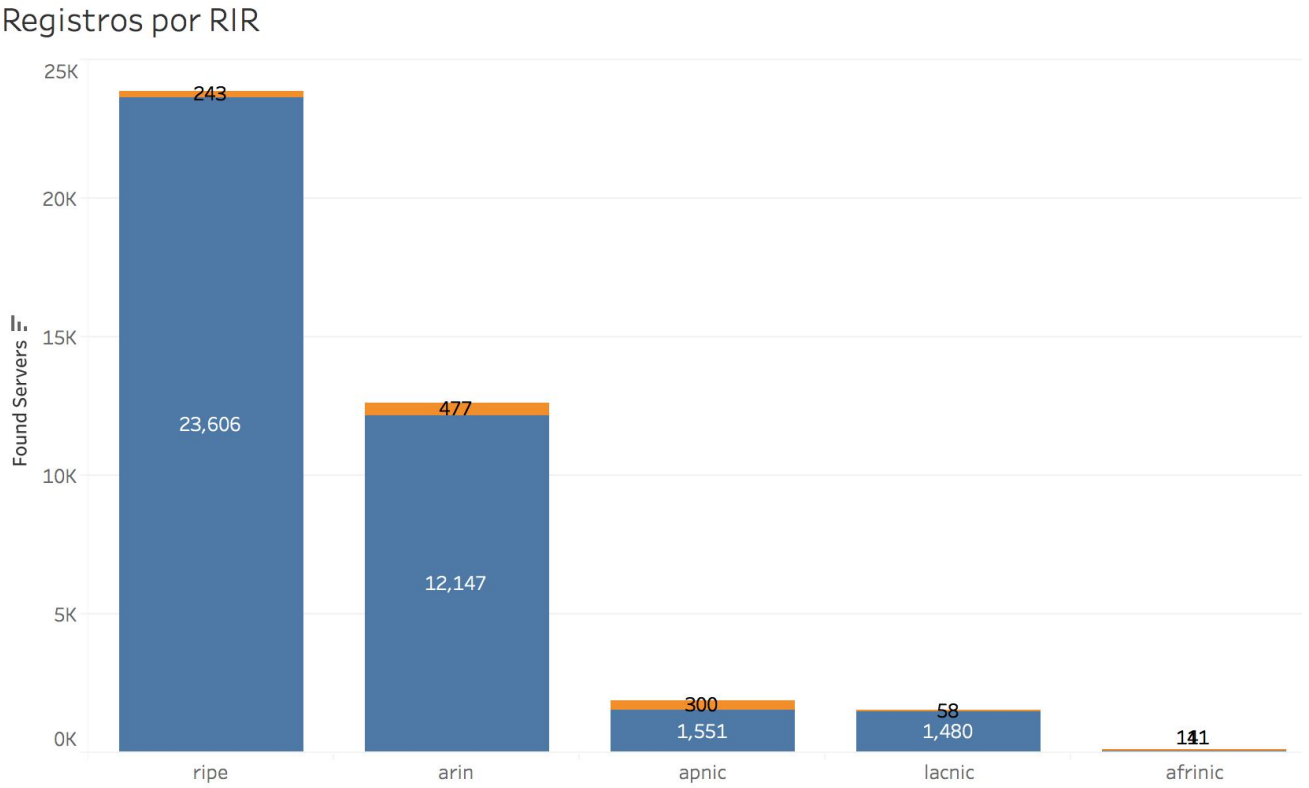
2803:XXXX:0:XXXX::242 | noerror | VE-YYYY-LACNIC

2803:XXXX:4100:XXXX::5 | noerror | CO-YYYY-LACNIC

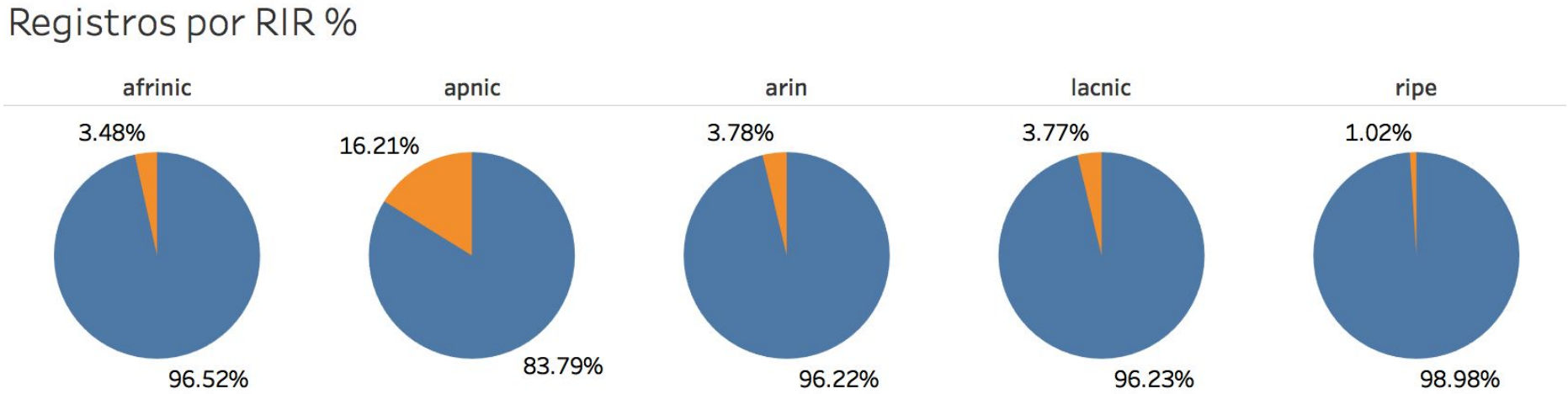
2803:XXXX:4200:XXXX::6 | noerror | CO-YYYY-LACNIC

2001:XXXX:3000:20:XXXX:7c1f:XXXX:f3c1 | noerror | MX-YYYY-LACNIC

Resultados parciales



Resultados parciales



Miscelaneos

Number of resolvers per /64:

Miscelaneos

Number of resolvers per /64:

2001:XXXX:XXXX:2/64 62

2a02:XXXX:0:XXXX/64 38

2a02:XXXX:0:XXXX/64 38

2001:XXXX:52:XXXX/64 34

2a02:XXXX:0:XXXX/64 32

Próximos pasos

1.- Todo automatizado (ongoing)

Próximos pasos

1.- Todo automatizado (ongoing)
2.- Alerta temprana a los afectados
3.- Publicar resultados del estudio

¡ Utopía del proyecto !

QUE CORRIJAN LA CONFIGURACIÓN DE LOS SERVIDORES AFECTADOS :-)

Preguntas / Comentarios