

“DNS Flag day”

Experiencia y primeros resultados

Hugo Salgado, .CL
Carlos Martínez, LACNIC

LACNIC 31, Punta Cana, República Dominicana



Contenido

- Qué es EDNS
- La campaña DNS Flag Day
- Mediciones de impacto
- Algunos resultados post-flagday

Historia del DNS

- Hitos relevantes:
 - 1987: RFC 1034, 1035 definición del DNS
 - 1999: RFC 2671 primera versión EDNS0
 - 2005: RFC 4033 DNSSEC
 - 2003: RFC 3490 IDN
 - 2013: RFC 6891 segunda versión EDNS0



¿Qué es EDNS?

- RFC 6891: Extension Mechanisms for DNS (EDNS(0))
 - Define un mecanismo compatible con DNS para indicar soporte para nuevas opciones
 - Especificación original incluye soporte para paquetes más grandes (sobre 512 bytes), más códigos de respuesta, etc.

¿Para qué sirve?

Extensiones:

- **NSID** -- RFC 5001: identificación de instancia del servidor
- **DNSSEC** -- bit DO: por favor, responda con registros DNSSEC
- **Client-subnet**, RFC 7871: desde qué red viene esta consulta?
- **Keep-alive**, RFC 7828: timeout variable para DNS sobre TCP.
- **Cookies**, RFC 7873: mecanismo liviano de seguridad.
- Y más en el futuro...

¿Cuál es el problema actual?

- DNS autoritativos que bloquean respuestas porque **no entienden EDNS0**
- Malas implementaciones de DNS que no siguen los estándares.
- Firewalls mal implementados o malas políticas que bloquean tráfico que sigue los estándares.
- DNS resolvers tienen que esperar timeout y reintentar con TCP o sin EDNS
- **Delays en resolución y dificultad para la innovación**

¿Cuál es la solución?

- Eliminar workarounds en forma coordinada
- ¡Que el dolor lo sienta el que lo causa!
- **Riesgo: algunos dominios podrían dejar de funcionar**

Campaña “DNS Flag Day”: el fin de los parches provisorios en EDNS

Fin de los parches

DNS flag day



DNS flag day 2019



- Acuerdo de vendors y resolvers públicos para terminar de hacer parches frente a servidores autoritativos “non-compliant”
- Tomar el compromiso de hacerlos todos a la vez, para evitar la percepción de que “algunos servidores funcionan mal”

¿A quiénes afecta?

- Los parches de código para permitir el funcionamiento de los DNS autoritativos que no cumplen con el standard de EDNS0 van en el software de servidor
 - Proveedores deben gestionar complejidad innecesaria en su código
 - Estos parches se aplican en el código “resolver”
- Si los servidores de un dominio, digamos “example.com” no soportan EDNS0 y los parches son retirados de los resolvers, el efecto es de un dominio que “no puede ser resuelto”

Campaña de educación / visibilización

- Sitio web con información y pruebas
- Análisis en algunos TLDs completos
- Avisos a titulares de dominios afectados
- Presentaciones en eventos:
 - LACNOG 2018, OARC, RIPE, etc.

Herramientas de verificación

https://dnsflagday.net



This change is affecting you only indirectly and you do not need to take any other steps. Thank you for your interest in [DNS!](#)

I'm a domain holder

If you are a domain holder, please use the form below to check if your domain is ready for the planned change. Your test result will include advice on any further steps that may be necessary.

Test your domain

Domain name (without www):

Testing completed:

lacnic.net: All Ok!



- This domain is perfectly ready, you do not need to worry about DNS flag day 2019.
- Your DNS administrator is doing a good job, send them a sincere thank you ;-)

technical report <https://ednscomp.isc.org/ednscomp/992f639d36>

Mediciones del impacto

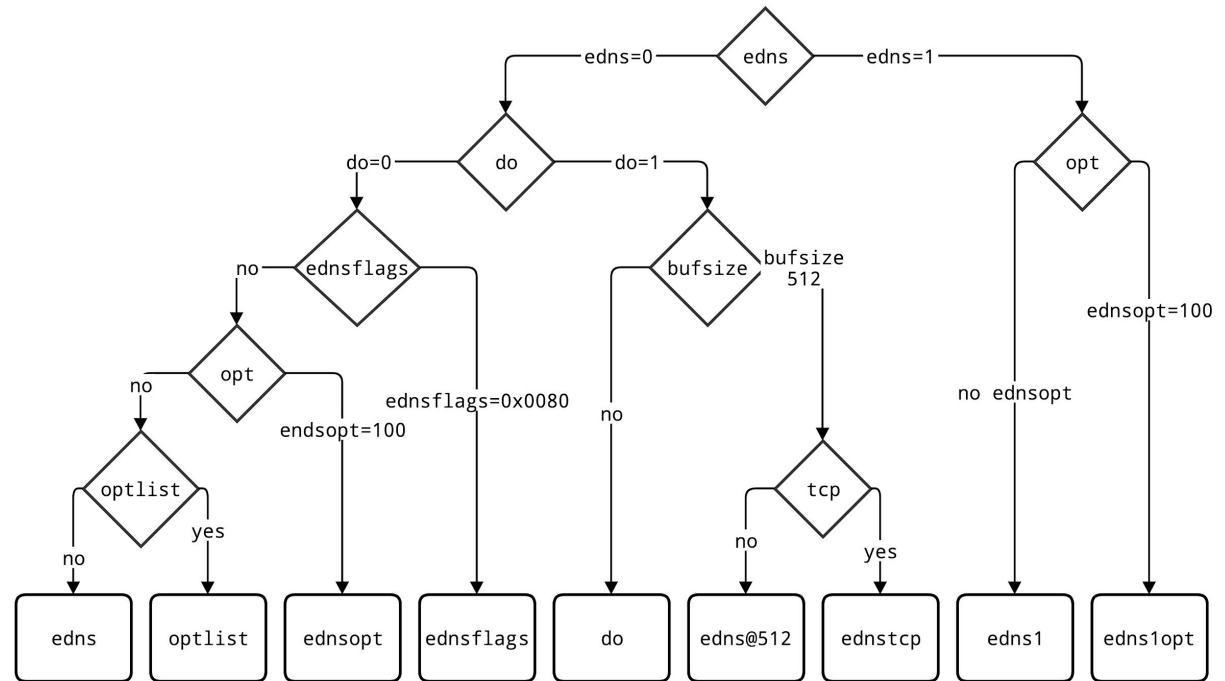
¿Cómo se hace la medición?

- Herramienta “DNS Compliance Testing” escrita por ISC
<https://gitlab.isc.org/isc-projects/DNS-Compliance-Testing>
- Dada una lista de dominios y sus servidores de nombre, verifica por conformidad con los estándares de DNS
 - Nosotros ejecutamos el subset de pruebas de EDNS
- Herramienta “EDNS Compliance scanner for DNS zones” de CZ.NIC para preprocesar la zona de cada TLD y reducir el número de pruebas
 - Si un servidor tiene mil dominios, no es necesario probar mil veces.

Jerarquía de pruebas

Diferentes valores
diferentes compon

Existen dependenc



¿Cuántos dominios estarían afectados?

(Gráfico con 3 meses pre-DNSflagday y 2 post, para varios TLDs)

(Resumen: ~1% de dominios)

¿Cómo puedo saber si afecta a mi dominio?

- Hay un sitio web con información y prueba en línea.
 - <https://dnsflagday.net>
- Colección por parte de ISC
 - <https://ednscomp.isc.org>
 - Cubre servidores raíz y TLDs
- Estoy encargado de un TLD, ¿cómo repito este análisis?
 - EDNS Compliance Scanner de CZ.NIC
 - <https://gitlab.labs.nic.cz/knot/edns-zone-scanner/>

Distintos niveles de falla

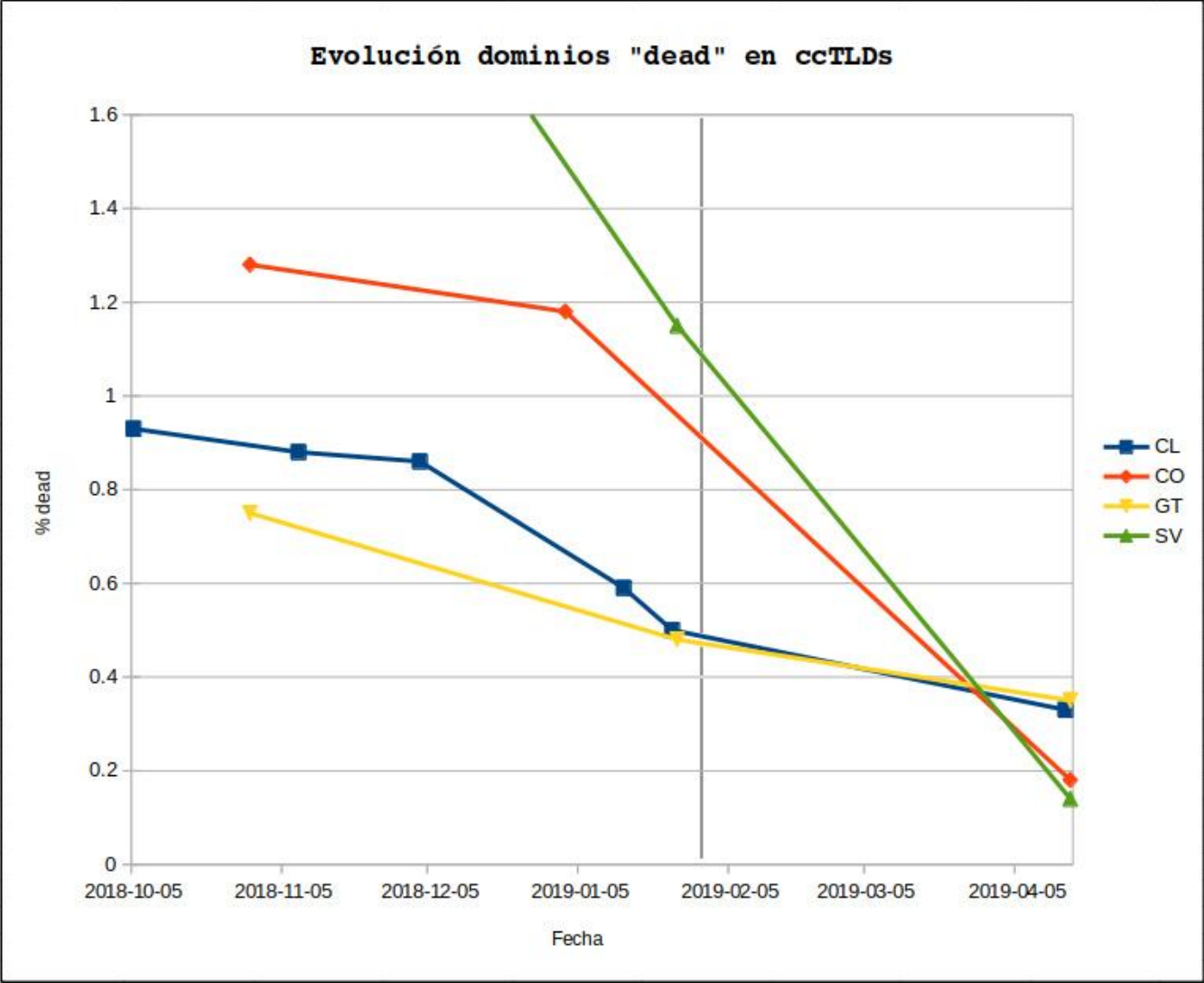
- **EDNS Compliance scanner** propone 4 estados para un dominio:
 - OK: El dominio no está afectado
 - Compatible: El dominio tiene algunos problemas pero no se verá afectado el DNS Flag Day
 - High Latency: El dominio sufrirá de timeouts al tratar de resolverlo
 - Dead: El dominio no funcionará
- Además define 2 modos: Permissive (como en éstos momentos) y Strict (después de Flag day)

Mi dominio está afectado, ¿cómo corrijo los errores?

- Actualizar tu software de DNS a una versión moderna
- Utilizar software que adhiera a los estándares
- Corregir reglas de firewall, especialmente inspección profunda de paquetes DNS
- Re-testear

Primeros resultados










Escaneo zonas LATAM



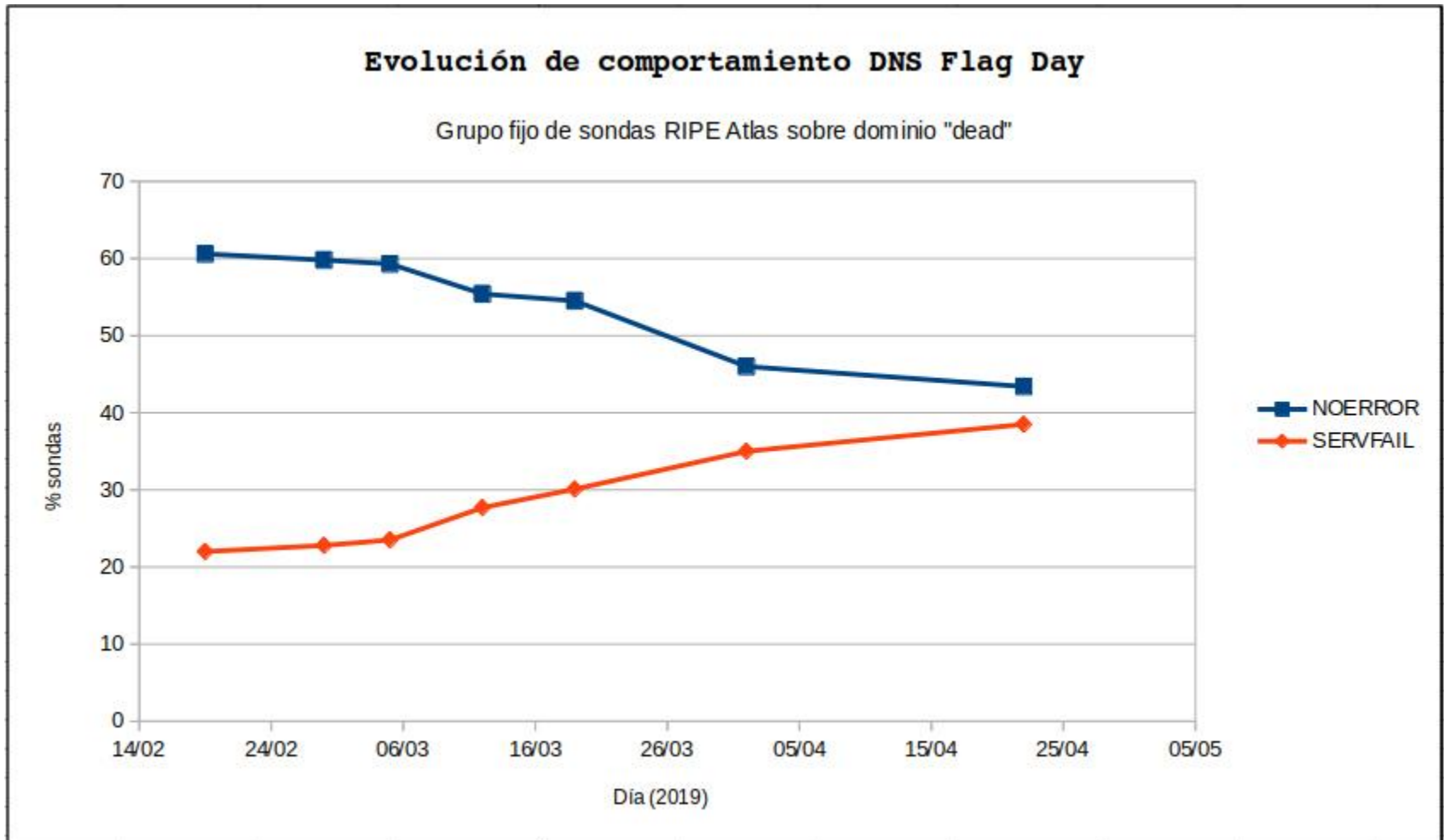
Versiones de software “DNS-flag-day”

	Versión	Fecha
Bind prod.	9.14.0	22 marzo
Bind dev.	9.13.4	22 noviembre 2018
Knot	All versions	<2017
PowerDNS	4.2.0	1 febrero
Unbound	1.9.0	5 febrero

Despliegue en algunos open resolvers

Cloudflare	
Comodo	
Dyn	
Google	
Level3	
Norton	
Opendns	
Quad9	
Ultradns	

Evolución del despliegue en resolvers



Errores comunes

- Firewalls!
 - instrucciones para F5, Juniper, BlueCat, etc:
 - <https://dnsflagday.net/#dns-admins>
- Versiones de software antiguos

Preguntas

dnsflagday.net/es/

Hugo Salgado, hsalgado@nic.cl
Carlos Martínez, carlos@lacnic.net