Reporte DNS @ IETF

LACNIC 32
Octubre 2019, Ciudad de Panamá

hugo@nic.cl

nic chile
SOMOS EL PUNTO CL

Working groups

- DNSOP
  - Operaciones en DNS
- DPRIVE
  - Privacidad en DNS
- ADD (BoF), REGEXT (EPP)

DNSOP (1/5)

- Obsoleting DLV
  - Técnica de trust anchors fuera de la raíz con DNSSEC
  - No hay implementaciones
- CNAME @ apex
  - El problema clásico de CNAME en apex con los múltiples CDN.
  - Opciones: ANAME en DNSOP, HTTPSSVC en HTTPbis

DNSOP (2/5)

- Serve stale
  - Permitir que resolvers utilicen RRs expirados si los autoritativos están inalcanzables
  - Update de 1035
  - Problema con posible abuso por hijos para evitar delegaciones interrumpidas (C&C)
- ALT TLD
  - Un TLD para resolver nombres que “no son DNS”
  - Ej: onion (Tor), bitcoins.
  - Permite que el resolver tenga hardcodeado el NXDOMAIN y no ocurran “leaks”.

DNSOP (3/5)

- Extended error
  - Agregar mensajes de error más granulares como extensión EDNS
  - Ejemplo: forged answer, DNSSEC bogus, signature expired, censored, etc.
- Resolver information
  - Publicar JSON con información del resolver: DNSSEC, qmin, DoT, etc.
  - Vía DNS (reverso con RESINFO) o HTTPS (well-known URI)

DNSOP (4/5)

- Running a Root Server Local to a Resolver
  - Obtener y mantener copia fresca:
    - axfr desde ICANN-DNS y algunos root servers
    - https desde internic.net
    - Servicio localroot.isi.edu
  - Siempre local al resolver (loopback)
- Multi-provider DNSSEC
  - Modelos de multiple signer
    - Common KSK, unique ZSK per provider
    - Unique KSK and ZSK per provider

DNSOP (5/5)

- Running a Root Server Local to a Resolver
  - Obtener y mantener copia fresca:
    - axfr desde ICANN-DNS y algunos root servers
    - https desde internic.net
    - Servicio localroot.isi.edu
  - Siempre local al resolver (loopback)
- Multi-provider DNSSEC
  - Modelos de multiple signer
    - Common KSK, unique ZSK per provider
    - Unique KSK and ZSK per provider

DPRIVE

- Publicó DoT, Do”DTLS”, EDNS0 padding, etc.
- BCP para operadores de resolutores con privacidad
  - On the wire
  - Data on rest
  - “DROP statement”
- Bis del “Privacy considerations” (7626)

ADD

- Applications Doing DNS.
- No es WG aún (BoF)
- El problema es el “resolver-less” DNS (DoH)
  - Split horizon
  - Filtrado
  - Quiebre de paradigma (OS, ISP,...)

¡Gracias!

- Más información
  - reporte LACTLD: https://listas.nic.cl/pipermail/dns-esp/2019-June/000461.html
  - IETF WGs: https://tools.ietf.org/wg/
  - IETF-LAC (LACNOG): https://mail.lacnic.net/mailman/listinfo/ietf-lac

- Hugo Salgado – hugo@nic.cl - @huguei