Privacidad y seguridad en tiempos de DNS

(Hechos, no palabras...)

Acerca del autor

Pablo Carboni (42), Buenos Aires, Argentina.

→ Sysadmin / DNSAdmin / NetAdmin

... A veces Unix developer 😊 ...

Twitter: @pcarboni

Mastodon: @pcarboni@bsd.network

Uno de los pilares de internet: “El DNS”

Breve introducción

- ***Fundamental*** para que funcione internet. ***Distribuido***.
  De los más ***antiguos***.
- ***Soporte inicial:*** mapea nombres a IP, envío de e-mail, sin uso de archivos locales - ***(“hosts.txt”)***. - *Ref: Paul Mockapetris, RFC 882/883, Nov 1983.*
- ***Simple*** implementación.
- ***Inconvenientes en seguridad y privacidad.***

¿Por qué problemas de privacidad y seguridad?

Necesidad de privacidad y seguridad:

➔ **Queries/answers** en plain text (compresión opcional)

⇒ ***Fácilmente visualizable***.

➔ **No verifica la respuesta**, solo la **'acepta'**.

⇒ ***Fácilmente modificable***.

➔ En 1983, **privacidad** y **seguridad** era algo impensado.
Hoy (2019), es ***casi imprescindible***

Internet dejó de ser un mundo ideal hace tiempo ...

¿Se imaginan en 2019, un mundo **sin privacidad ni seguridad** de **DNS** en **internet** ?

- **Ataques simples:**
  - **Intercepción:** “**Man in the middle**” attack (MiTM)
  - **Modificación** (data tampering).

- Ocasiona **problemas** de diferente índole a nivel mundial.

Consecuencias de lo anterior ...

Privacidad/seguridad:

- ➔ Intercepción/modificación: **registrars**, **ISPs**, **organismos autorizados legalmente** (policía, servicios secretos, etc), llegando incluso a **gobiernos**.
- ➔ En la práctica: frecuentes **bloqueos**, **censura**, incluso **persecuciones**.

Algunos hechos comprobados (¿evitables?)

➔ **Redirección del “.com”** (2003, Verisign, TLD server, ‘sitefinder’).

Consultas a dominios .com inexistentes, respondidas con la dirección IP del propio website.

Detalle: esto mismo me sucedió también con un proveedor de Argentina años más tarde, pero en el Resolver.

➔ **Bloqueo y censura de países:** China, Rusia, Iran, y otros.

➔ “Secuestro” y falsificación de rutas BGP, junto a servidor de DNS falso:

- **Robo de dinero** (Criptomonedas, myetherwallet.com, 2018).

Evitando inconvenientes

Diferentes mecanismos surgieron:

★ **DNSSEC** (Domain Name System Security Extensions, 1997) [**RFC 2065 y actualizaciones**]

Integridad en la respuesta - **verifica origen.** Usa claves públicas. ⇒ ***No encripta*** *el contenido*

★ **DoT** (DNS over Transport Layer Security" - 2016) [**RFC 7858 y actualizaciones**].

Canal **cifrado** e **integridad** del mismo. Usa **TLS >=1.2**, y puerto **853/tcp** (*Bloqueable*)

★ **DoH** (DNS over HTTPS - 2018) [**RFC 8484**]

Canal **cifrado** e **integridad** del mismo. Usa HTTPS (TLS 1.3) y puerto 443/tcp.

⇒ Solo cliente DNS (Stub) ⇐⇒ Resolver. (**Dificulta MiTM y bloqueo)**

Nota: Hay otros mecanismos como DNSCrypt, DNSCurve, pero no son estándares.

DNSSEC al rescate ... (¿Para que nos sirve?)

Detalles:

- Son extensiones del protocolo de DNS
- Comprueban que las respuestas del servicio sean auténticas, usando claves publicas.
- Las zonas/registros, están firmadas.
- Usa EDNS0 (extensiones a DNS) y o bien TCP

Algunos opinan que por su naturaleza es complementario a DoH/DoT.

Otras, además indican que DNSSEC no es suficiente.

Referencias:

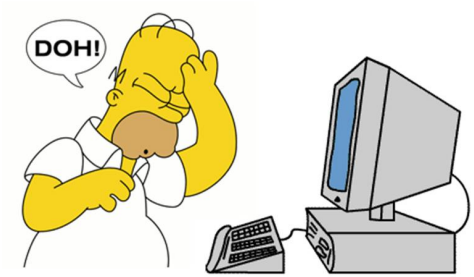
https://blog.apnic.net/2018/08/17/sunrise-dns-over-tls-sunset-dnssec/
(Willem Toorop, NLnet Labs, 17/Ago/2018)

https://blog.apnic.net/2018/08/20/dnssec-and-dns-over-tls/
(Geoff Huston, APNIC, 20/Ago/2018)

Controversias en DoH - 1/2 - Voces a favor

Voces a favor (argumento)**:**

Ayudar a usuarios poder efectuar **queries** de **DNS**, **sin** **intercepción/rastreo** por parte de ISPs, gobiernos opresivos (dictaduras), etc.



Controversias en DoH - 2/2 - Voces en contra

Voces en contra (Fuertes controversias):

¿Motivos? Modificar mecanismos nativos del DNS, concentración de datos, y a veces de forma casi compulsiva. ***Veamos algunos hechos****:*

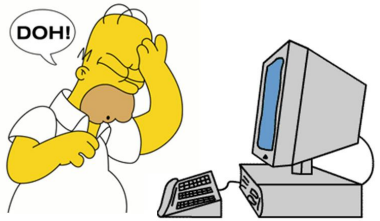
⇒ ***Concentración***: pocos proveedores conocidos (ej, **CloudFlare**). Los **queries DoH** son enviados en forma **centralizada.**

"Se pierde, el **espíritu** del **DNS** - **distribuido**, y **privacidad**, por **disponer un tercero logs**".

⇒ ***Septiembre'2019***: Mozilla foundation *habilitó* por DEFAULT en **Firefox** el cliente de **DoH** en **USA**, configurado para **CloudFlare**.

⇒ ***OpenBSD*: Por lo anterior, deshabilitó** ese **default** en su **instalación.**

⇒ **GDPR:** gracias a esto, no sucede en **Europa**.



Algunos proveedores conocidos de DoH

Una lista exhaustiva está disponible en https://dnscrypt.info/public-servers/

Para mencionar algunos de los más conocidos:

- **Cloudflare**: (dns.cloudflare.com)
- **CleanBrowsing** (doh.cleanbrowsing.org)
- **Google**: (dns.google)
- **Quad9** (dns.quad9.net)

Implementaciones DoT (Nov'2019)

- **Browsers:** Firefox, Chrome, cURL.
- **Servidores/Clientes (DNS):** Unbound, Bind, Knot
- **OS:** systemd-resolvd (Linux), Android 9 (Pie)
- **Servidores (compañías):** CloudFlare, Quad9, CleanBrowsing
- **Proxies:** DNSCrypt-Proxy (Frank Denis). **LB:** dnsdist (PowerDNS)

Para más referencias:

➪ https://www.dnsprivacy.org *(Hub principal de noticias, implementaciones, etc)*


Implementaciones DoH (Nov'2019)

- **Browsers:** Firefox, Chrome(Test via flags), cURL, OkHttp.
- **Compañías (servicios DoH):** CloudFlare, CleanBrowsing, Google, Comcast(nuevo)
- **Proxies:** DNSCrypt-Proxy, cliente-servidor (Frank Denis), Facebook DoH client, jDnsProxy, Start Brilliant (cliente-servidor)
- **Servidores**: BIND 9.16/17 (Planeado, Octubre'2020)

Detalle: Por diseño, recordar que es consulta de STUB a DNS recursivo. (pero no autoritativo)

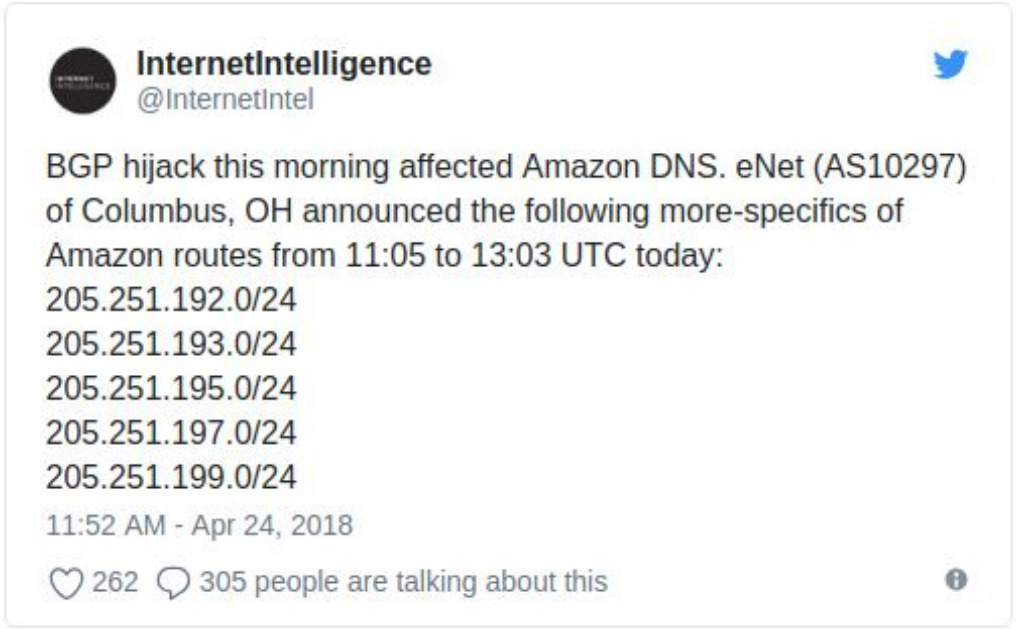
Más referencias:

https://github.com/curl/curl/wiki/DNS-over-HTTPS *(Listado actualizado de implementaciones)*

https://www.dnsprivacy.org *(Hub principal de noticias, implementaciones, etc)*

https://en.wikipedia.org/wiki/DNS_over_HTTPS *(Descripción de Wikipedia)*

Hackers en acción: Robo de dinero (y ~~DNSSEC??~~).



Fuente:
https://doublepulsar.com/hijack-of-amazons-internet-domain-service-used-to-reroute-web-traffic-for-two-hours-unnoticed-3a6fodda6a6f

24/Abril/2018:

De manera ilegal, **se publicó por BGP rutas falsas** del servicio de DNS, "Route 53" (AWS), afectando en forma parcial al servicio, unas 1300 IPs - (BGP hijacking)

El ataque -de pocas horas-, tuvo como objetivo final a **MyEtherWallet.com**, con DNSes redirigiendo tráfico a servidores Rusia.

Detalle: El daño fue de 150.000 USD. (215 ETHereum)

Cabe destacar que hubo falta de DNSSEC en la zona...

Hackers en acción (Poniendo tu vida en riesgo)

Ataques de DNS Rebinding sobre IOT (19/Jun/2018, PoC). *"TL;DR"*

Con este tipo de ataques, se afecta a una red hogareña, comúnmente WiFi, afectando principalmente elementos como TVs, Roku, Speakers, Routers WiFi, Termostatos(!), etc.

Consiste en mapear registros de DNS maliciosos en forma efímera (TTL bajo para cambio rápido de IP de destino), utilizando JS + POST sobre el objetivo.

Referencias:

https://medium.com/@brannondorsey/attacking-private-networks-from-the-internet-with-dns-rebinding-ea7098a2d325

Reporte de exploit (termostato):

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11315%29

Más información sobre DNSSEC/DoT/DoH:

(En orden alfabético):

- Asian Pacific Network Information Centre (RIR) / www.apnic.net
- CZ.NIC (NIC de República Checa) / www.nic.cz
- DNS-OARC / www.dns-oarc.net
- DNSCrypt-Proxy / Frank Denis
- DNS Privacy Project / www.dnsprivacy.org
- Internet Software Consortium / www.isc.org
- NLNet Labs / www.nlnetlabs.nl
- PowerDNS / www.powerdns.com
- Sinodun Internet Technologies / www.sinodun.com

¡Muchas gracias!