Algunas Noticias de DNS (Agosto '2018)

(Y algunas pesadillas)

Autor:

Pablo Carboni

Twitter: @pcarboni


Mastodon: @pcarboni@bsd.network

- SysAdmin, DNSAdmin, a veces NetAdmin, algunas veces Unix developer ☺.
- Actualmente: DevOps en GraphPath.

¿Que sucedió con los DNSes durante 2018?

- Nuevos servicios de DNS ofrecidos ***gratis*** por otras compañías, además de los ofrecidos por Google Public DNS (**8.8.8.8/8.8.4.4**).
- Protocolos adicionales para *privacidad y autenticidad*:
  - **DNS-Over-TLS** - estándar **RFC (DoT)**
  - **DNS-Over-HTTPS, draft IETF (DoH)**
  - **DNSCrypt (Abierto, sin estandarizar)**

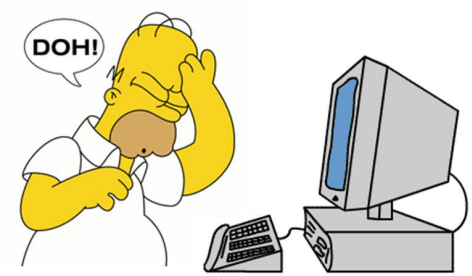
Nuevos proveedores de servicios de DNS:

↪ Con foco en privacidad
↪ IPv4 e IPv6
↪ El listado es **parcial.** (Servicios adicionales disponibles en otras IPs)

- **"Quad9"** (IBM- PCH - Global CyberAlliance)
  - DoT
  - **9.9.9.9 / 149.112.112.122** [IPv4]
  - **2620:fe::fe, 2620:fe::9** [IPv6]
- **"1.1.1.1"** (CloudFare - APNIC)
  - DoT, DoH
  - **1.1.1.1 / 1.0.0.1** [IPv4]
  - **2606:4700:4700::1111** [IPv6]
  - **2606:4700:4700::1001** [IPv6]
- **"CleanBrowsing"** (CleanBrowsing)
  - DoT, DoH, DNSCrypt
  - **185.228.168.168 / 185.228.169.168** [IPv4]
  - **2a0d:2a00:1::, 2a0d:2a00:2::** [IPv6]

DoH! (DNS over HTTPS)

- Las consultas a los DNS, necesitan ser confiables (autenticidad), y privadas (no ser espiadas), por cuestiones de seguridad del usuario.
- Sin embargo, esto no siempre es así....



- *Para este propósito, en estado draft,* **DNS over HTTPs (DoH)**, *viene al rescate!*

¿Qué es entonces DoH?

- Son queries de *DNS sobre un medio cifrado como HTTPS*.
- *Aumenta privacidad y evita modificación* de datos. Evita ataques del tipo “Man-In-the-Middle”.

Detalle: No tiene forma de consultar a servidores de DNS Autoritativos.

FUTURO ESTÁNDAR: HTTPS://TOOLS.IETF.ORG/HTML/DRAFT-IETF-DOH-DNS-OVER-HTTPS-14 (16/Ago/2018)

¿Qué es DoT?

- Son queries de DNS sobre un canal cifrado con TLS.
- Aumenta privacidad y evita la modificación de los datos, procurando evitar ataques del tipo “Man-In-the-Middle”.

- RFC 7858 y RFC 8310

Algunas implementaciones DoT, en testing y producción (Ago’2018)

- **Browsers:** Firefox, Chrome, cURL.
- **Servidores/Clientes (DNS):** Unbound, Bind, Knot
- **OS:** systemd-resolvd 239 (Linux), Android 9 (Pie)
- **Servidores (compañías):** CloudFare, Quad9, CleanBrowsing
- **Proxies:** DNSCrypt-Proxy (Frank Denis). **LB:** dnsdist (PowerDNS)

Para más referencias:

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

https://hacks.mozilla.org/2018/05/a-cartoon-intro-to-dns-over-https/

https://bitsup.blogspot.com/2018/05/the-benefits-of-https-for-dns.html

Algunas implementaciones DoH, en testing y producción (Ago'2018)

- **Browsers:** Firefox, Bromite (Chromium), cURL, OkHttp
- **Servidores (compañías):** CloudFare, CleanBrowsing, Google
- **Proxies:** DNSCrypt-Proxy, cliente-servidor (Frank Denis), Facebook DoH client, jDnsProxy, Start Brilliant (cliente-servidor)

  Detalle: No tiene forma de consulta a servidores de DNS Autoritativos.

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)*

curl://

CLOUDFLARE

CleanBrowsing

DNSCrypt-Proxy 2

Pero ... no siempre es mundo perfecto ...

Imaginen un mundo (año 2018) **sin seguridad** de **DNS** en **internet** ...

¿Alcanzan los mecanismos descriptos?

"La respuesta no los sorprenderá"

¡ NO ! *(cuantas más medidas se tomen, mejor)*

Cuando los chicos malos aparecen ...

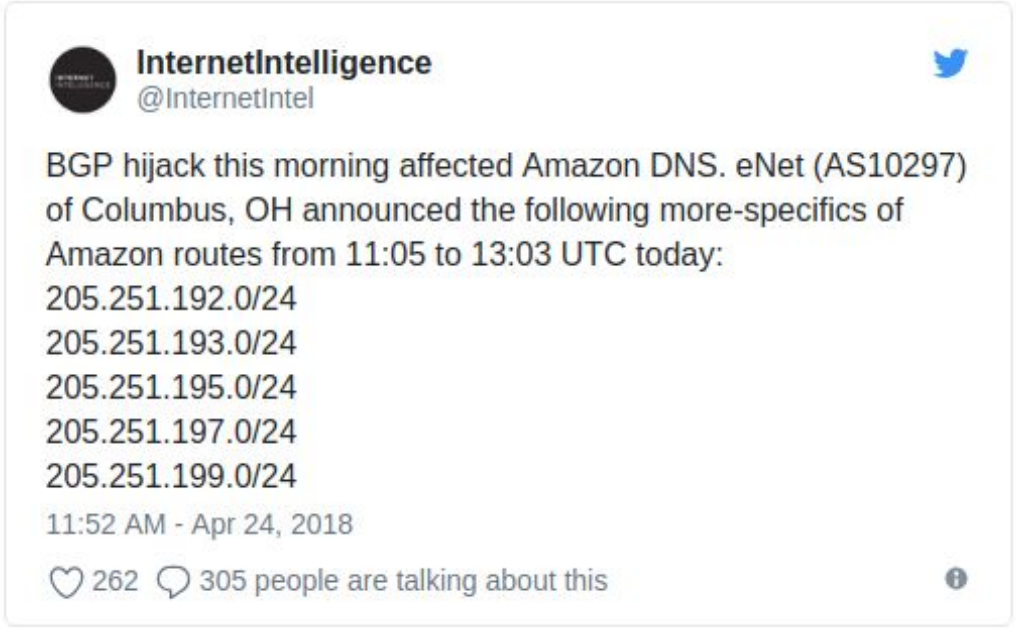
¿ Qué pasa cuando alguien accede a un servicio financiero, ... **pero no todo es lo que dice ser? (phishing)**

¿ Qué pasa cuando tu browser, repentinamente dice que el certificado SSL (TLS), dejó de ser ***VALIDO*** (sin firmar)?

(HTTPS valida certificados firmados **... pero no el mapeo de hostname a IP**)

Exactamente eso ... ***¡Se cometen estafas!***

Hackers en acción (1 de 2)



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...

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

DNSSEC/DNS Security Extensions, son extensiones del protocolo de DNS, que sirven para comprobar de forma inequívoca que las respuestas del servicio sean auténticas, al estar firmadas las zonas/registros (usando PKI) .

Utiliza además como mecanismo, EDNS0 (extensiones al protocolo original de DNS).

Existen algunas opiniones al respecto, indicando 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)

Hackers en acción (2 de 2)

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

Con este tipo de ataques, se afecta a una red hogareña, comunmente 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

https://dnsflagday.net/

IMPORTANTE: El 1ero de febrero de 2019, los vendors:

BIND (ISC), Knot Resolver (CZ.NIC), PowerDNS, and Unbound (NLnet Labs)

Dejarán de proveer workarounds sobre software que no implemente apropiadamente EDNS0, haciendo que los timeouts sean válidos ***únicamente*** por problema de red - y no por malas implementaciones.

Presentación en DNS-OARC 28, por Ondrej Sury (Internet Systems Consortium), Peter van Dijk (PowerDNS), Petr Špaček (CZ.NIC), Ralph Dolmans (NLnet Labs)

Slides:https://indico.dns-oarc.net/event/28/contributions/515/attachments/490/799/Removing_EDNS_Workarounds.pdf
Video: https://youtu.be/9YYH8JFH_bY?t=5198

Finalmente....

¡Felices 35 años DNS!

- Primer Test, Junio/1983
- RFC 882, el primer RFC de DNS, Noviembre/1983

Reconocimientos por la información publicada:

(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
- Internet Software Consortium / www.isc.org
- NLNet Labs / www.nlnetlabs.nl
- PowerDNS / www.powerdns.com
- Sinodun Internet Technologies / www.sinodun.com

¡Muchas gracias!