Some DNS News (August, 2018)

(And some nightmare)

Author:

Pablo Carboni

Twitter: @pcarboni


Mastodon: @pcarboni@bsd.network

- SysAdmin, DNSAdmin, sometimes NetAdmin, sometimes Unix developer ☺.
- Currently: DevOps at GraphPath.

What happened with DNS services during 2018?

- New DNS services were offered for ***free*** by other companies, in addition to the offered by Google Public DNS (**8.8.8.8/8.8.4.4**).
- There are additional protocols, with *privacy and authenticity in mind that were added:*
  - DNS-Over-TLS - standard RFC (DoT)
  - DNS-Over-HTTPS, draft IETF (DoH)
  - DNSCrypt (Open, no standarization)

New DNS service providers:

↪ *Focused on privacy*

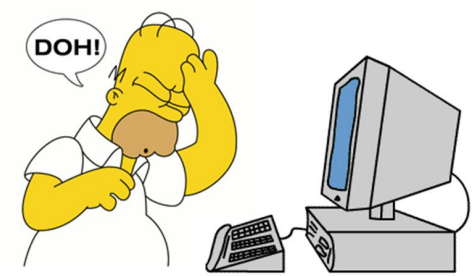
↪ *IPv4 and IPv6*

↪ *This listing is **partial.***
(Additional services are available with other 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)

- DNS queries needs to be trusted (authenticity), and private (no spying), because of user security reasons.
- However, this is not always as we wanted to have...



- *For this purpose, in draft state,* ***DNS over HTTPs (DoH),*** *comes to rescue!*

What's DoH then?

- It's DNS traffic travelling inside an ***encrypted transport like HTTPS***.
- It ***enhances privacy and avoids data tampering***. Avoid attacks like "Man-In-the-Middle" type.

Note: It doesn't have mechanisms for querying to DNS authoritative servers.

Future standard: https://tools.ietf.org/html/draft-ietf-doh-dns-over-https-14 (Aug 16th, 2018)

What's DoT?

- It's DNS traffic travelling over a ciphered channel with TLS cryptographic protocol.
- It enhances privacy and avoid data tampering, trying to avoid attacks like "Man-In-the-Middle" type.
- **RFC 7858 / RFC 8310**

Some DoT implementations, both testing and production quality (August 2018)

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

More info:

➪ https://www.dnsprivacy.org *(Main Hub with news, info about implementations, 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






Some DoH implementations, both testing and production quality (August'2018)

- **Browsers:** Firefox, Bromite (Chromium), cURL, OkHttp
- **Services (companies):** CloudFare, CleanBrowsing, Google
- **Proxies:** DNSCrypt-Proxy, client-server (Frank Denis), Facebook DoH client, jDnsProxy, Start Brilliant (client-server)

  Note: There is no way to send queries to DNS authoritative servers.

More info:

https://github.com/curl/curl/wiki/DNS-over-HTTPS *(Up-to-date implementations listing)*

https://www.dnsprivacy.org *(Main hub with news, implementations, etc)*

https://en.wikipedia.org/wiki/DNS_over_HTTPS *(Description from Wikipedia)*

But … our world isn't a perfect world …

Let's imagine a world (2018 year) **without** DNS **security** running over the **internet** …

Are really enough those mechanisms descripted previously?

"The answer will not surprise you"

NO ! (MORE PROTECTION IS BETTER)

When the bad guys appear ...

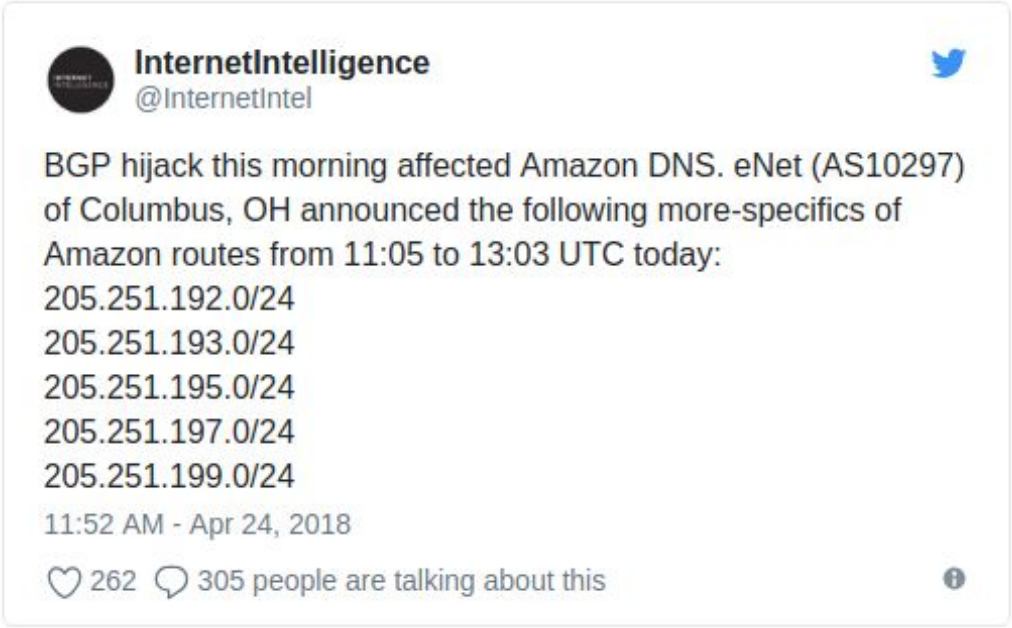
What happens when someone access to a financial service, ... **but it isn't what you supposed to be? (phishing)**

What happens when your browser, suddenly says that your SSL (TLS) certificate isn't ***VALID*** anymore? (unsigned)

(HTTPS validates signed certificates **... but nothing to do with hostname to ip mapping**) - A trusted IP address.

That's it ... ***Scams come to life!***

Hackers in action (1 of 2)



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

April 24th, 2018:

In a illegal way, **fake BGP routes (prefixes) were published** for DNS service, "Route 53" (AWS), affecting the service in a partial way, 1300 IPs roughly (**BGP hijacking**)

The attack - few hours -, had as final destination **MyEtherWallet.com site,** with DNS servers redirecting traffic to servers located in Russia.

Detail: Damage was about 150.000 USD. (215 ETHereum)

It should be noted that the DNS zone lacked DNSSEC support...

DNSSEC to our rescue ... (What's its purpose?)

DNSSEC/DNS Security Extensions, are extensions to DNS protocol, that are meant to verify in a unique way thats answers from the DNS service are authentic, because there are signed zone/records (by using PKI).

It alse uses as mechanism, EDNS0 (DNS extensions to the original protocol).

There are some thoughts that says (because since its nature), is complementary to **DoH/DoT.**

Others, says that DNSSEC is not enough.

References:

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

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

Hackers in action (2 of 2)

DNS Rebinding attacks over IOT (Jun 19th, 2018, PoC). *"TL;DR"*

This kind of attacks affects a home network, generally speaking a WiFi network, by affecting mainly devices like TVs, Roku, Speakers, Routers WiFi, Thermostats(!), etc.

It consists in mapping DNS crafted records, in an ephemere fashion (low TTL for quickly changing destination IP), by using JS + POST on the objective.

References:

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

Exploit report (thermostat):

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

https://dnsflagday.net/

IMPORTANT: February 1st, 2019, the following vendors:

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

Will remove workarounds from their software, for broken EDNS0 implementations, making that timeouts will valid ***only*** for network issues - and not for broken implementations.

Presentation at DNS-OARC 28, by 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

Finally...

Happy 35th birthday DNS!

- First Test, June/1983
- RFC 882, First RFC with DNS description, November/1983

Acknowledgements:

(Alphabetic order):

- 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 / http://www.sinodun.com

Thank you!