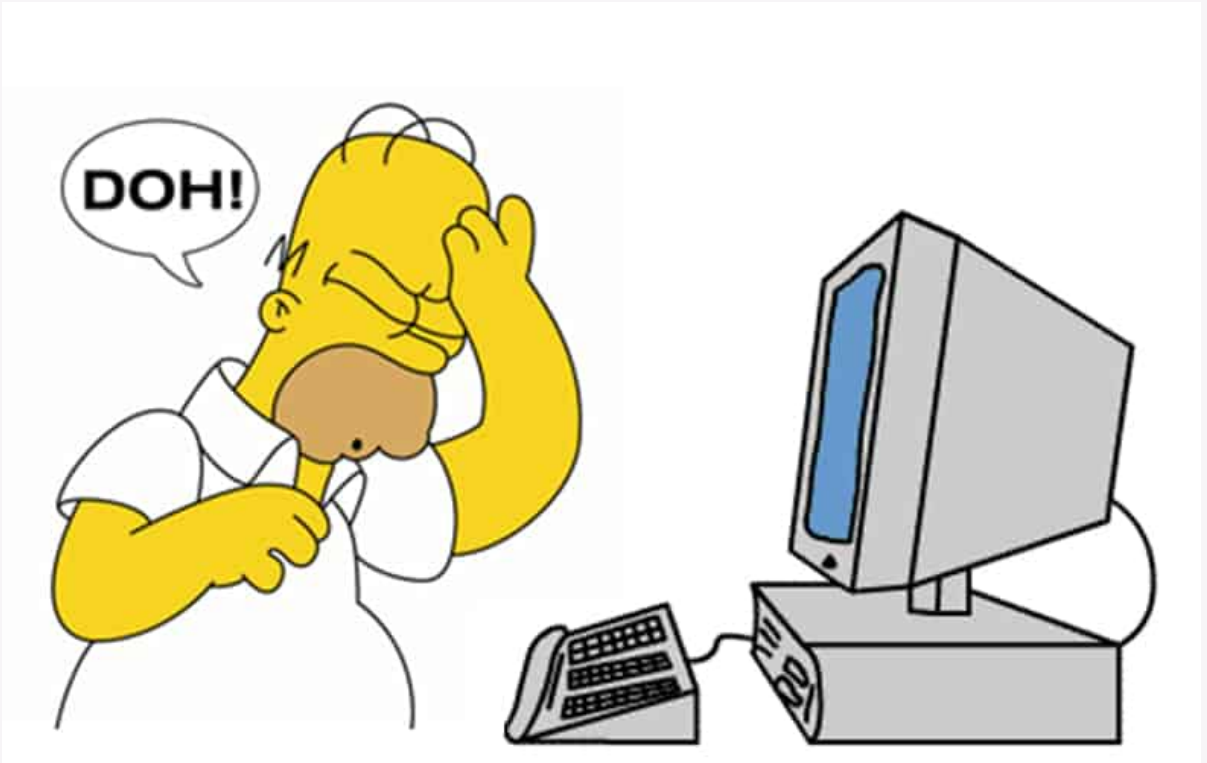


DNS over *

or

How HTTP is ruling the world

Index

- DNS O que é e o que faz
- DNS Problemas e soluções
- DNS e encriptação
- Porque é que isto aconteceu
- Porque é que isto me interessa

DNS

DNS – Domain Name System – Sistema de Nomes de Domínios

Responsável pela tradução de nomes na Internet

dns.pt - 185.39.208.69

- 2a04:6d80:0:1::5

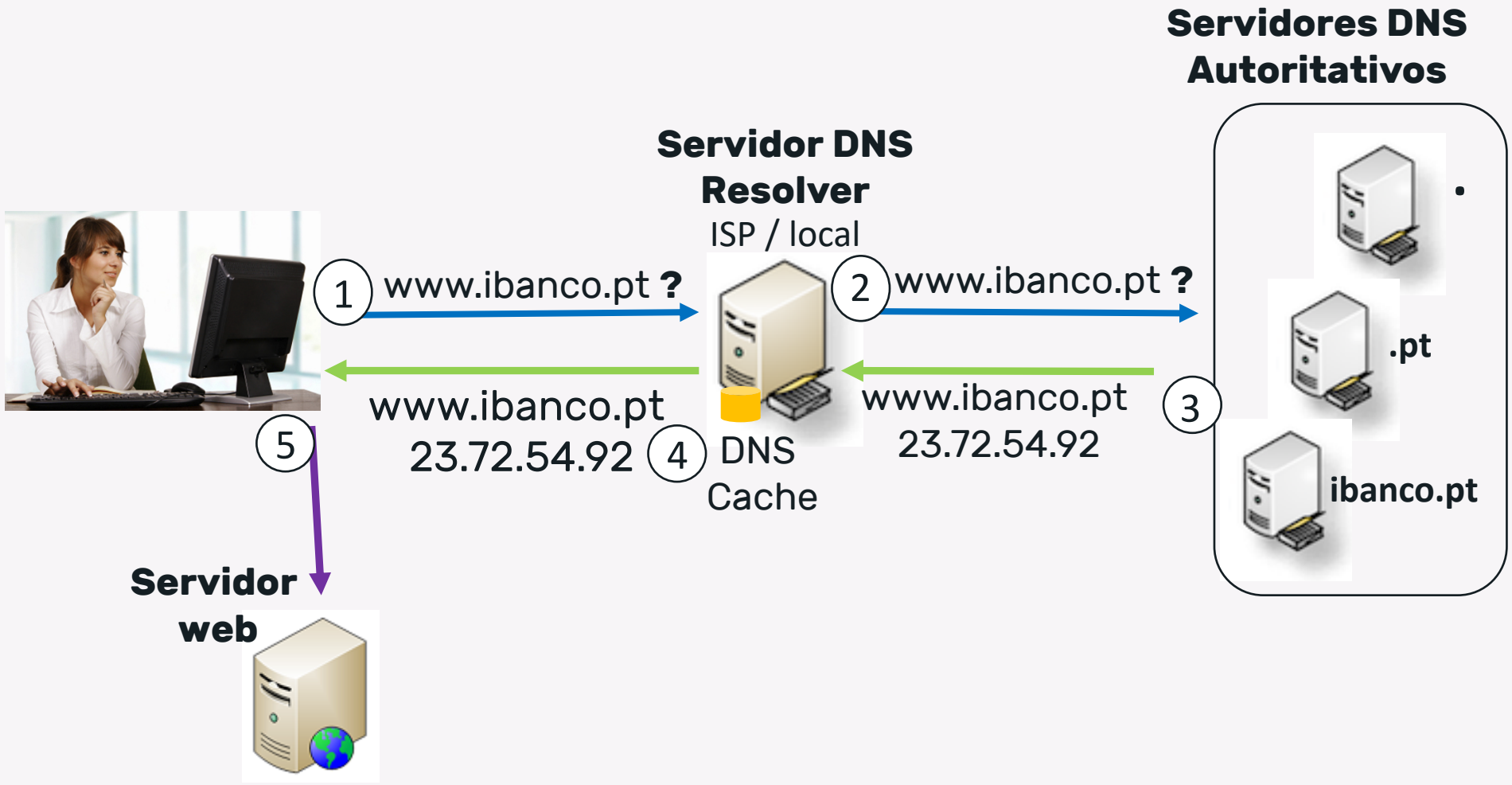
www.google.pt - 216.58.201.163

rtp.pt. - 94.46.160.136

- 94.46.160.176

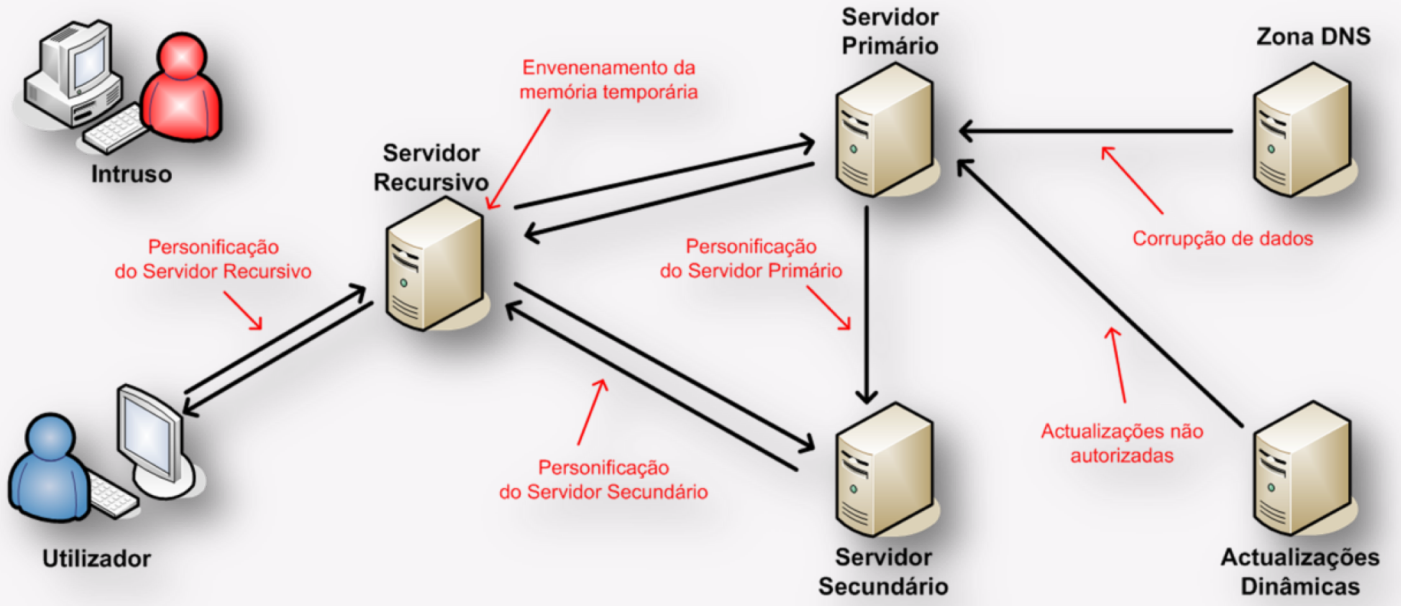
- 94.46.160.126

Resolução DNS



Resolução DNS

- Fragilidades de segurança no DNS

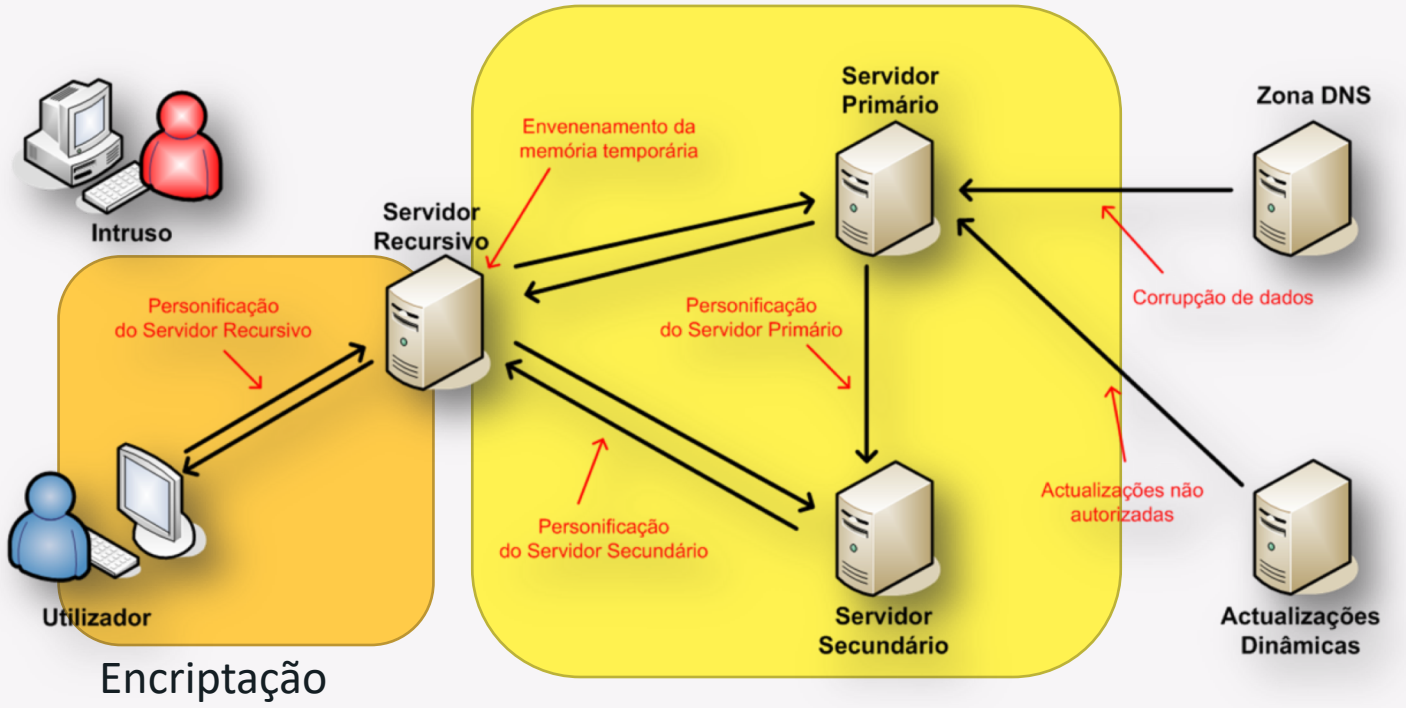


Protocolo criado para ser simples e prático mas:

- **Sem considerações de segurança (fraco)**
- **Implementações com vulnerabilidades**

Resolução DNS

- Fragilidades de segurança no DNS



Métodos transporte DNS

- Implementações de DNS
  - DNS over UDP – 1º método de transporte, rápido e eficaz, continuando a ser dominante
  - DNS over TCP – método de transporte que adicionou fiabilidade
  - DNS over QUIC – método experimental, sem grande base de suporte que adicionou confidencialidade
  - DNS over TLS – método de transporte usando SSL
  - DNS over HTTPS – método de transporte usando SSL e HTTP

Métodos transporte DNS

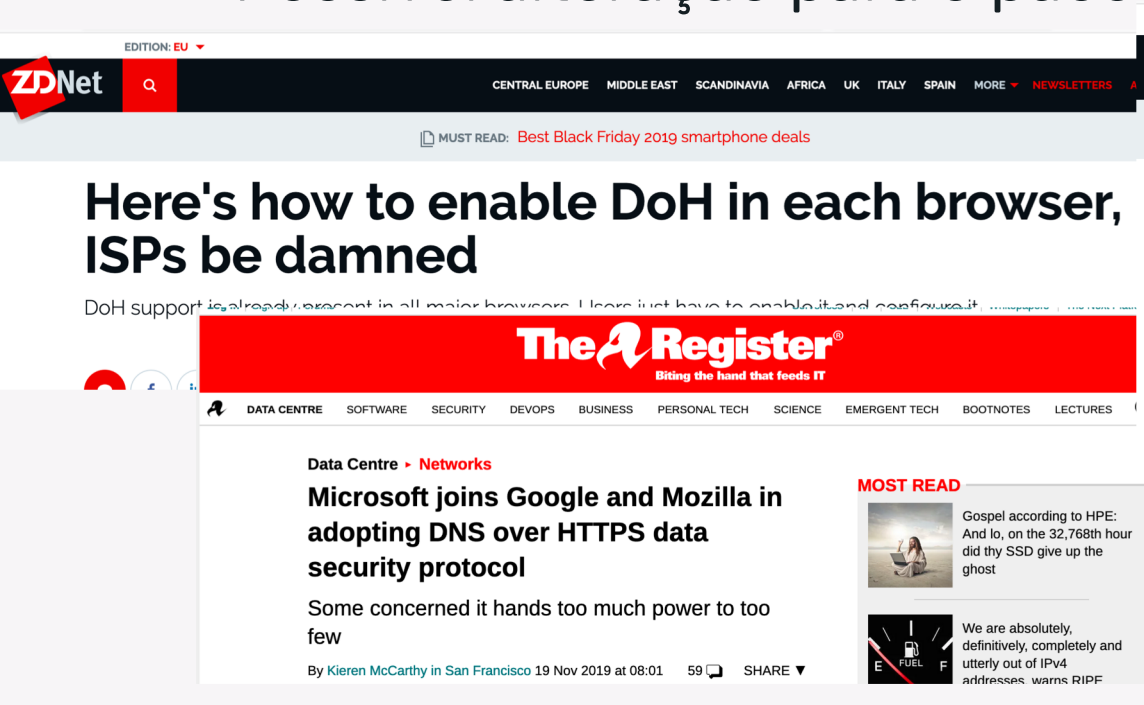
- Implementações de DNS
  - DNS over UDP – 1º método de transporte, rápido e eficaz, continuando a ser dominante
  - DNS over TCP – método de transporte que adicionou fiabilidade
  - DNS over QUIC – método experimental, sem grande base de suporte que adicionou confidencialidade
  - **DNS over TLS – método de transporte usando SSL**
  - **DNS over HTTPS – método de transporte usando SSL e HTTP**

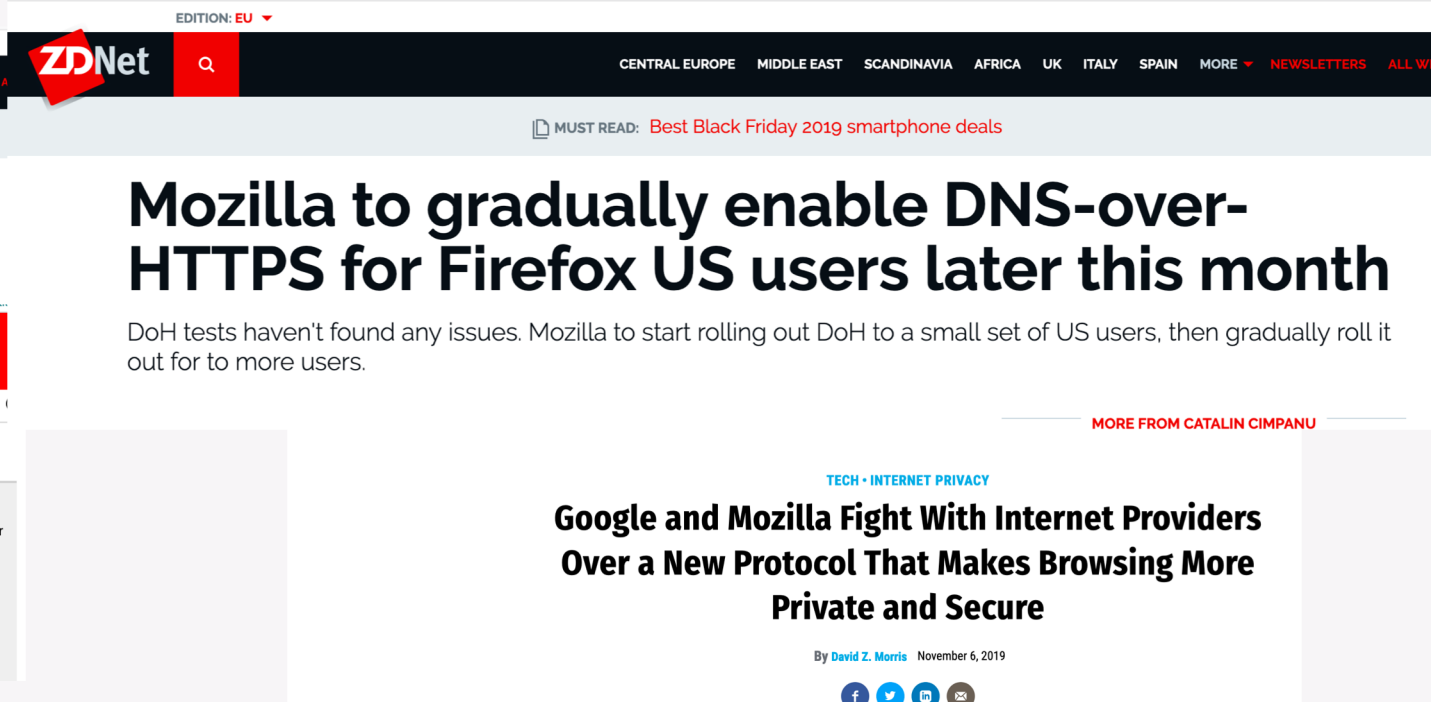
DNS over TLS (DoT)

- Proposto no IETF há cerca de 5 anos
- Necessitou do boost da standartização do TLS1.3
- Simplesmente colocou o DNS over SSL
- Porta 853
- Funciona com TLS oportunistico
- Introduzido no Android Pie
- Todos os grandes cloud resolvers o oferecem

DNS over HTTPS (DoH)

- Coloca o pacote de DNS sobre HTTPS
- Promovido pelos produtores de Browsers
- Rápida adoção no IETF
- Ao invés do DoT não foi standartizado mecanismo de descoberta
  - Chrome – DoH oportunistico
  - Firefox – TRR
- Possível alteração para o pacote de DNS se tornar JSON





Porquê?

- Privacidade

Porquê?

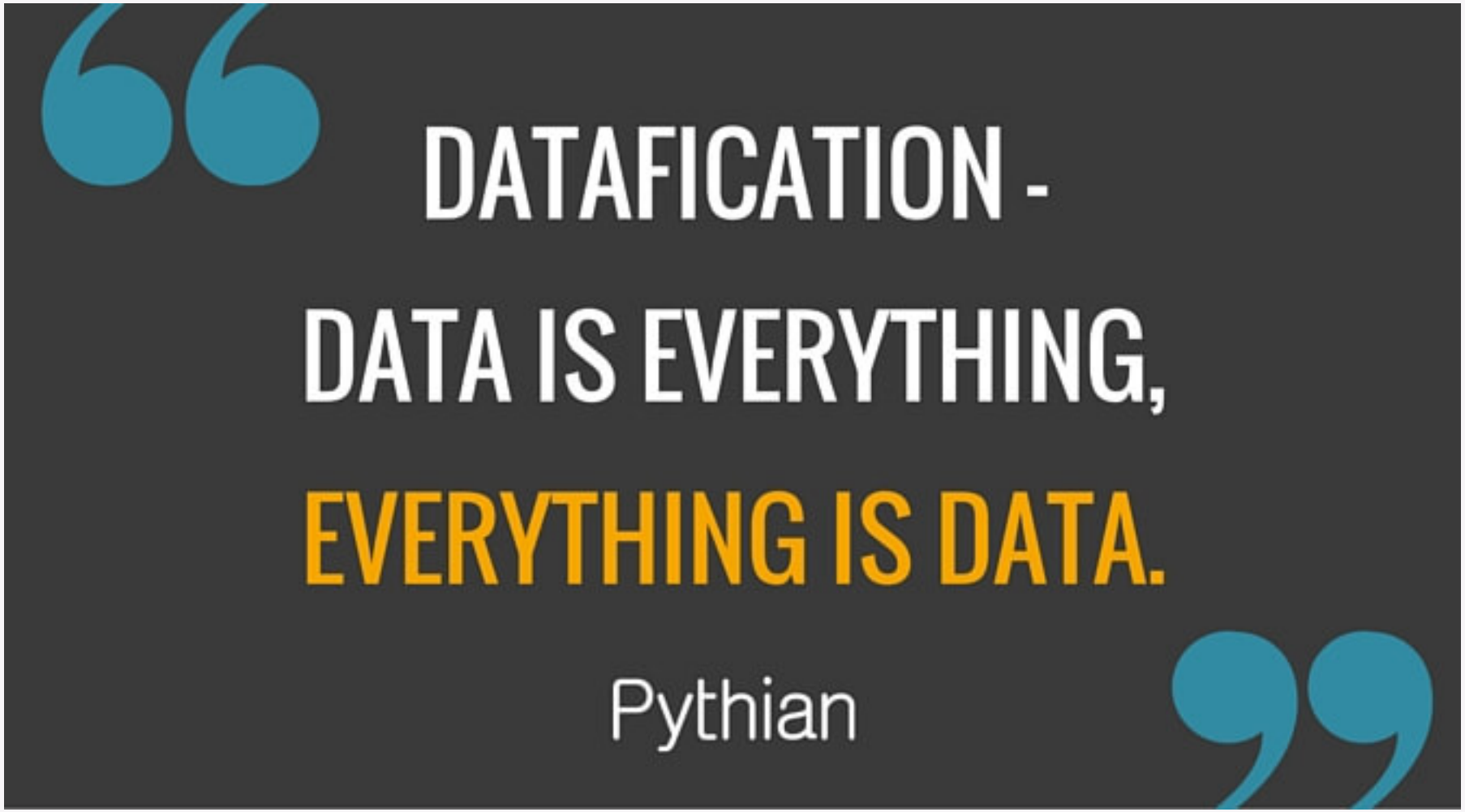
- Rapidez

Porquê?

- Bloqueios no DNS

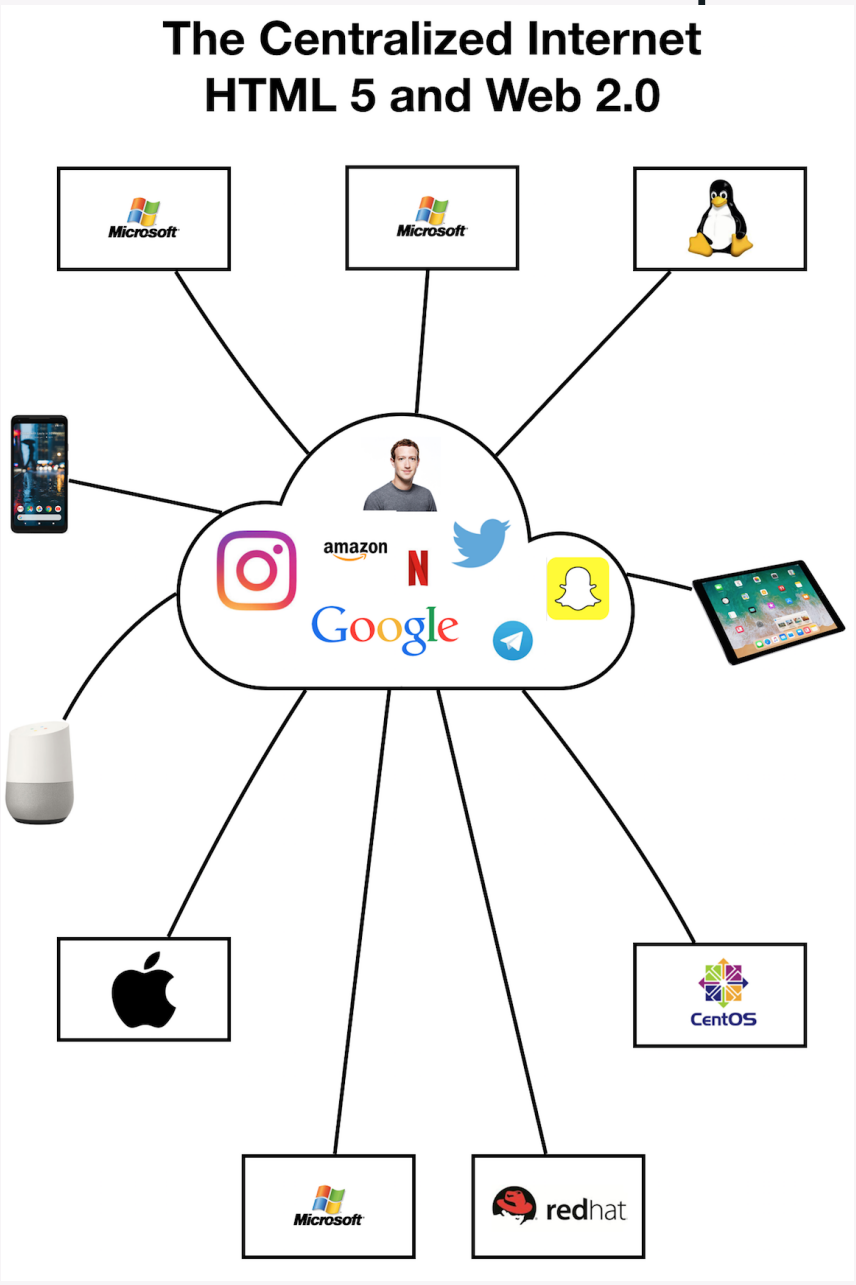
Porquê?

- Mas também... Dados



Porquê?

- Leva à centralização da Internet



Porquê?

- Malware via DoH

ZDNet

CENTRAL EUROPE MIDDLE EAST SCANDINAVIA AFRICA UK ITALY SPAIN MORE NEWSLETTERS

MUST READ: Best Black Friday 2019 smartphone deals

First-ever malware strain spotted abusing new DoH (DNS over HTTPS) protocol

Godlua, a Linux DDoS bot, is the first-ever malware strain seen using DoH to hide its DNS traffic.

By Catalin Cimpanu for Zero Day | July 3, 2019 -- 13:17 GMT (14:17 BST) | Topic: Security

MORE FROM CATALIN CIMPANU

Hardware
HPE tells users to patch SSDs to

ANTI-CORRUPTION DIGEST

Home Anti-Corruption Governance and Ethics Anti-Money Laundering Cyber Risk Security Ri

First-ever malware strain spotted abusing new DoH (DNS over HTTPS) protocol

by Paul Mackessey | Jul 4, 2019 | Security Risks | 0 comments

Tags: anti-corruption | corruption | Security Risk

— Anti-Corruption News Story Curated by Anti-Corruption Digest International Risk & Compliance News

Tra
Sele
Tecnol
Sear

First malware to abuse DNS over HTTPS poses challenge for defenders

John Leyden 04 July 2019 at 13:41 UTC

Malware DDoS

DDoS bots' tactics could break existing controls

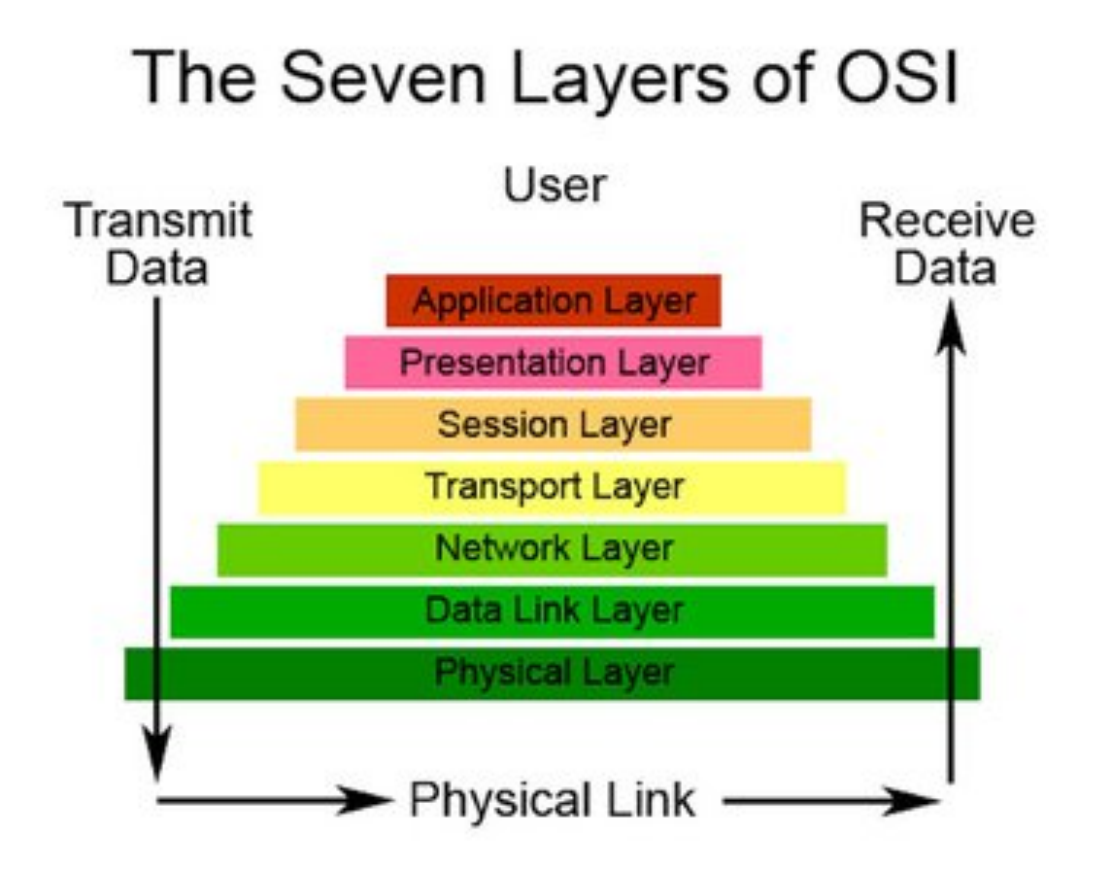
The First Malware Abuses DNS over HTTPS (DoH)

By Jessica Foreman

Posted on September 3, 2019

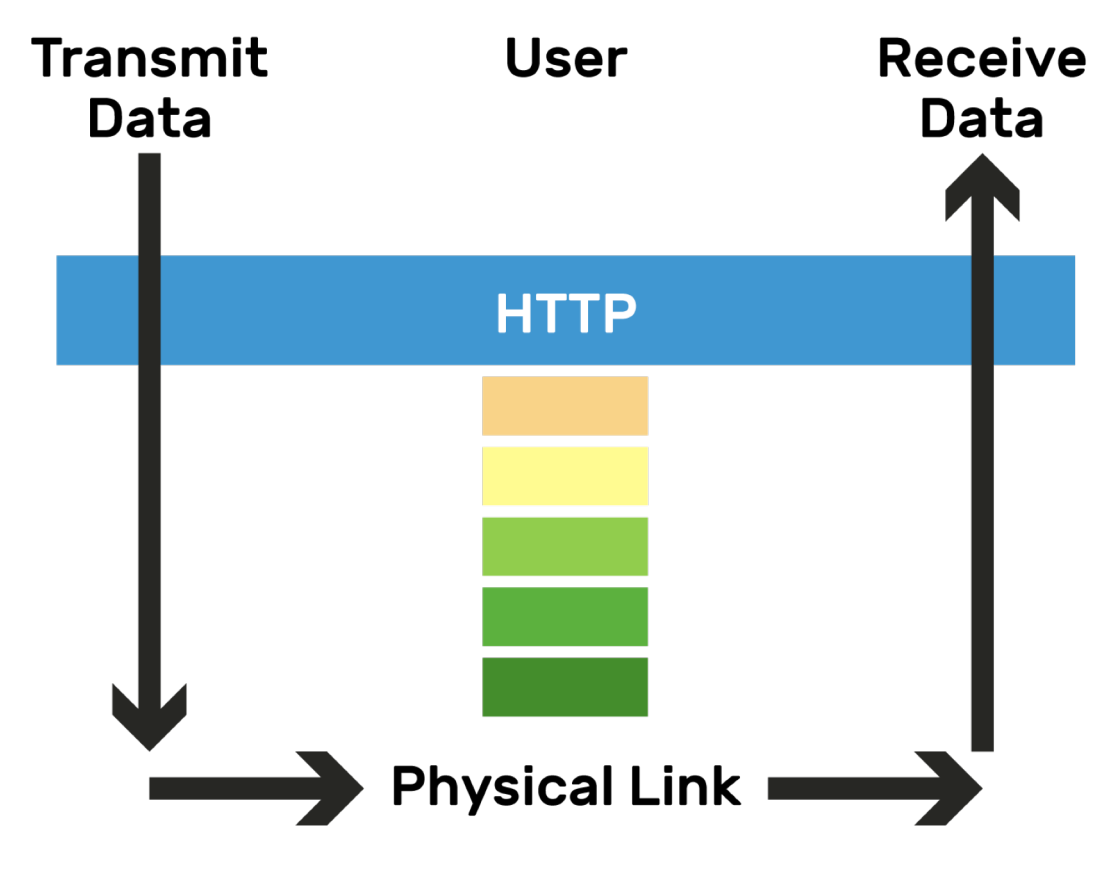
HTTP is ruling the world

- Modelo OSI



HTTP is ruling the world

- Internet real



Thank You!

Eduardo.duarte@dns.pt
www.dns.pt