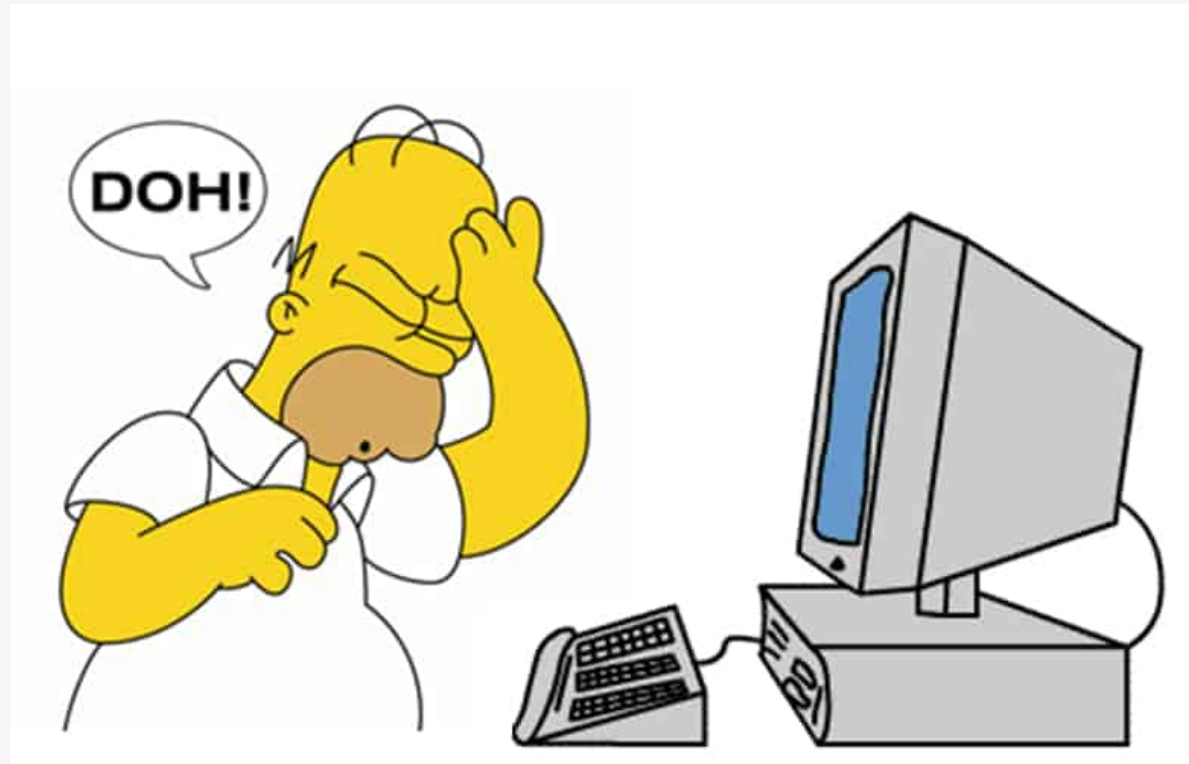




DNS over *

or

How HTTP is ruling the world

- 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 – 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

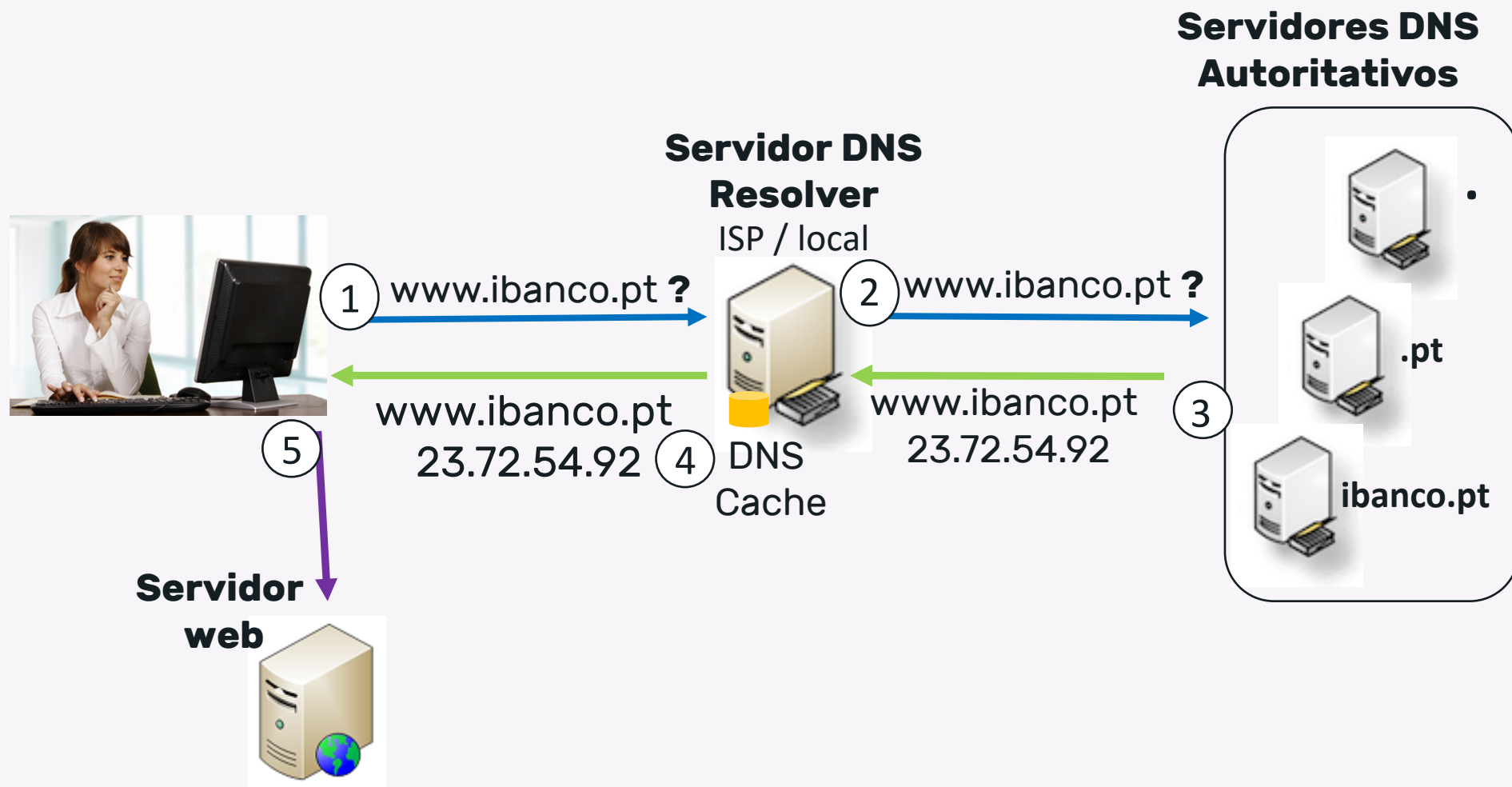
www.google.pt – 216.58.201.163

rtp.pt. – 94.46.160.136

– 94.46.160.176

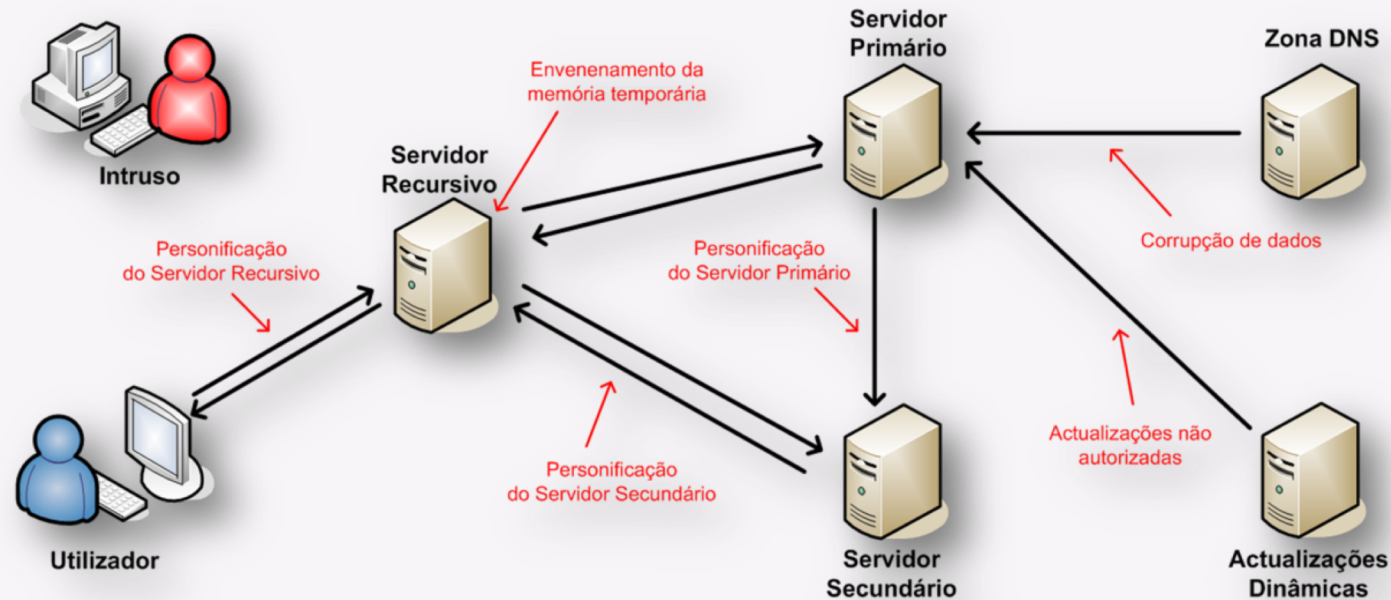
– 94.46.160.126

Resolução DNS



Resolução DNS

- Fragilidades de segurança no DNS

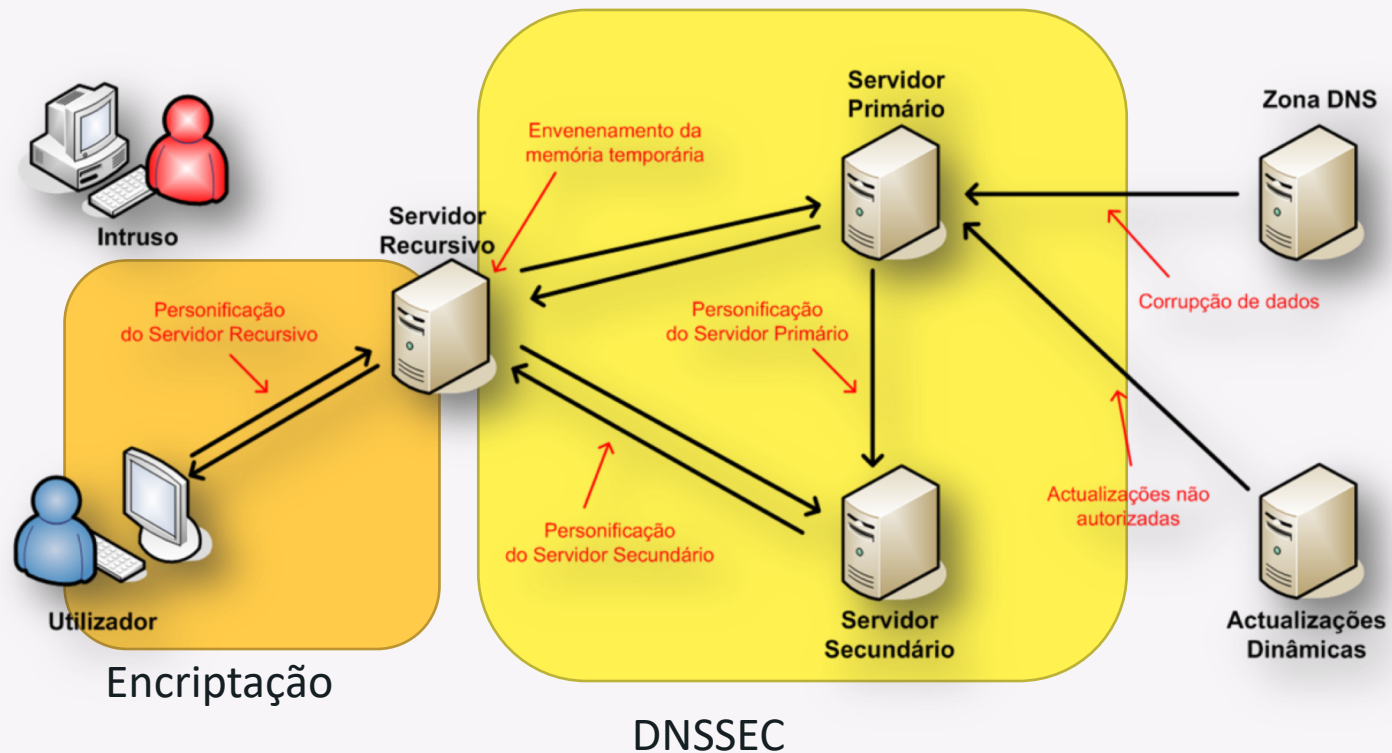


Protocolo criado para ser simples e prático mas:

- **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 standardização 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 oportunístico
 - Firefox – TRR
- Possível alteração para o pacote de DNS se tornar JSON

EDITION: EU ▼

ZDNet 🔍

CENTRAL EUROPE MIDDLE EAST SCANDINAVIA AFRICA UK ITALY SPAIN MORE ▼ NEWSLETTERS ALL W

MUST READ: [Best Black Friday 2019 smartphone deals](#)

Here's how to enable DoH in each browser, ISPs be damned

DoH support is already present in all major browsers. Users just have to enable it and configure it.

The Register
Biting the hand that feeds IT

DATA CENTRE SOFTWARE SECURITY DEVOPS BUSINESS PERSONAL TECH SCIENCE EMERGENT TECH BOOTNOTES LECTURES

Data Centre > **Networks**

Microsoft joins Google and Mozilla in adopting DNS over HTTPS data security protocol

Some concerned it hands too much power to too few

By [Kieren McCarthy](#) in San Francisco 19 Nov 2019 at 08:01 59 🗨️ SHARE ▼

MOST READ

Gospel according to HPE: And lo, on the 32,768th hour did thy SSD give up the ghost

We are absolutely, definitely, completely and utterly out of IPv4 addresses, warns RIPE

EDITION: EU ▼

ZDNet 🔍

CENTRAL EUROPE MIDDLE EAST SCANDINAVIA AFRICA UK ITALY SPAIN MORE ▼ NEWSLETTERS ALL W

MUST READ: [Best Black Friday 2019 smartphone deals](#)

Mozilla to gradually enable DNS-over-HTTPS for Firefox US users later this month

DoH tests haven't found any issues. Mozilla to start rolling out DoH to a small set of US users, then gradually roll it out for to more users.

MORE FROM CATALIN CIMPANU

TECH • INTERNET PRIVACY

Google and Mozilla Fight With Internet Providers Over a New Protocol That Makes Browsing More Private and Secure

By [David Z. Morris](#) November 6, 2019

f t in

Porquê?

- Privacidade



Porquê?

- Rapidez



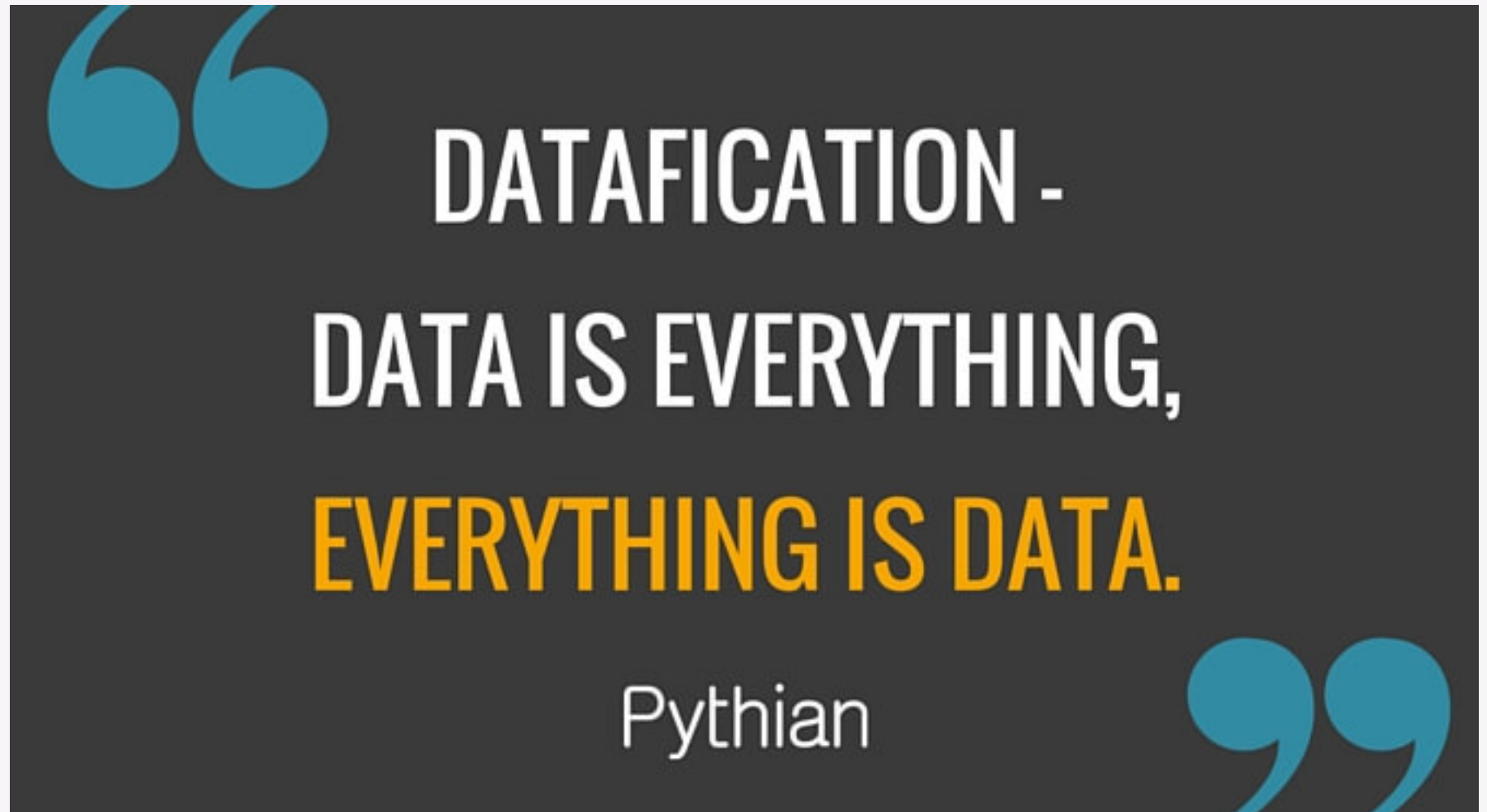
Porquê?

- Bloqueios no DNS



Porquê?

- Mas também... Dados



- Leva à centralização da Internet

Porquê?



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

First malware to abuse DNS over HTTPS poses challenge for defenders

John Leyden 04 July 2019 at 13:41 UTC

[Malware](#) [DDoS](#)



The First Malware Abuses DNS over HTTPS (DoH)



By [Jessica Foreman](#) 

Posted on September 3, 2019

ANTI-CORRUPTION DIGEST

[Home](#) [Anti-Corruption](#) [Governance and Ethics](#) [Anti-Money Laundering](#) [Cyber Risk](#) [Security Risks](#)

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

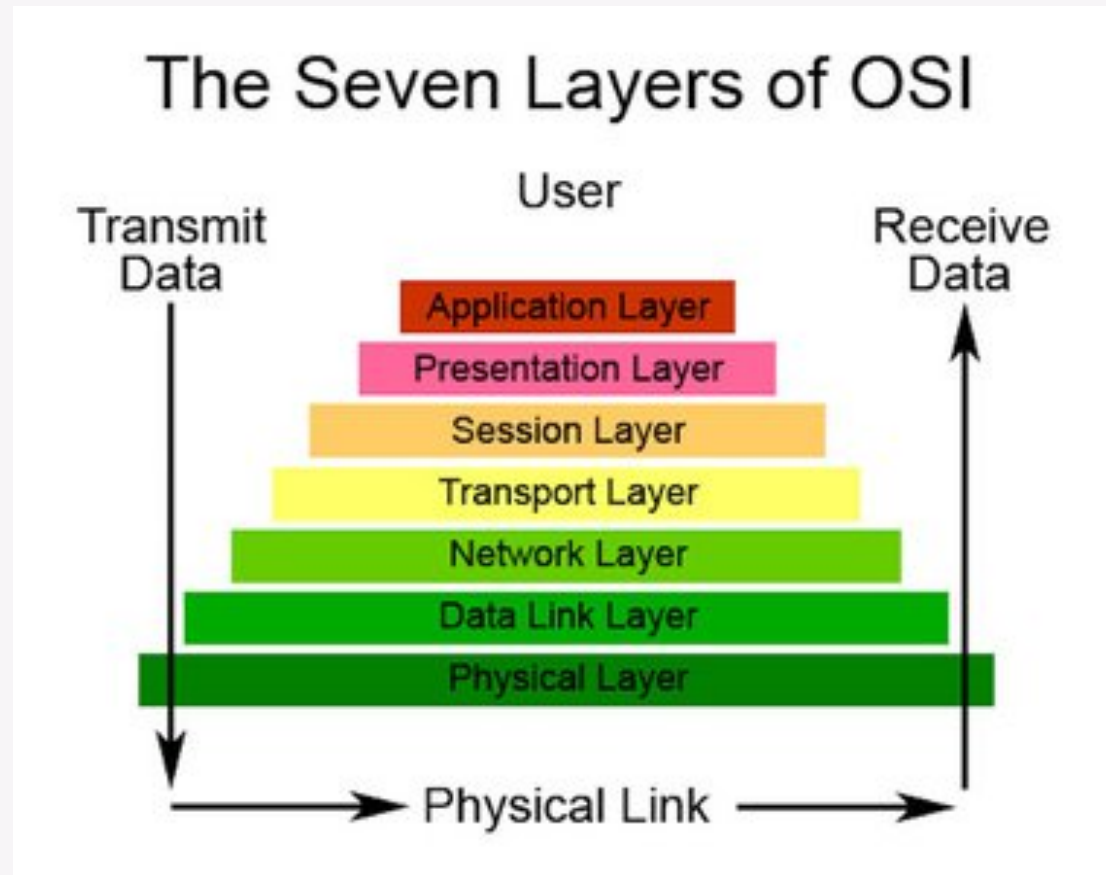
by Paul Mackessey | Jul 4, 2019 | [Security Risks](#) | [0 comments](#)

 Tags: [anti-corruption](#) | [corruption](#) | [Security Risk](#)

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

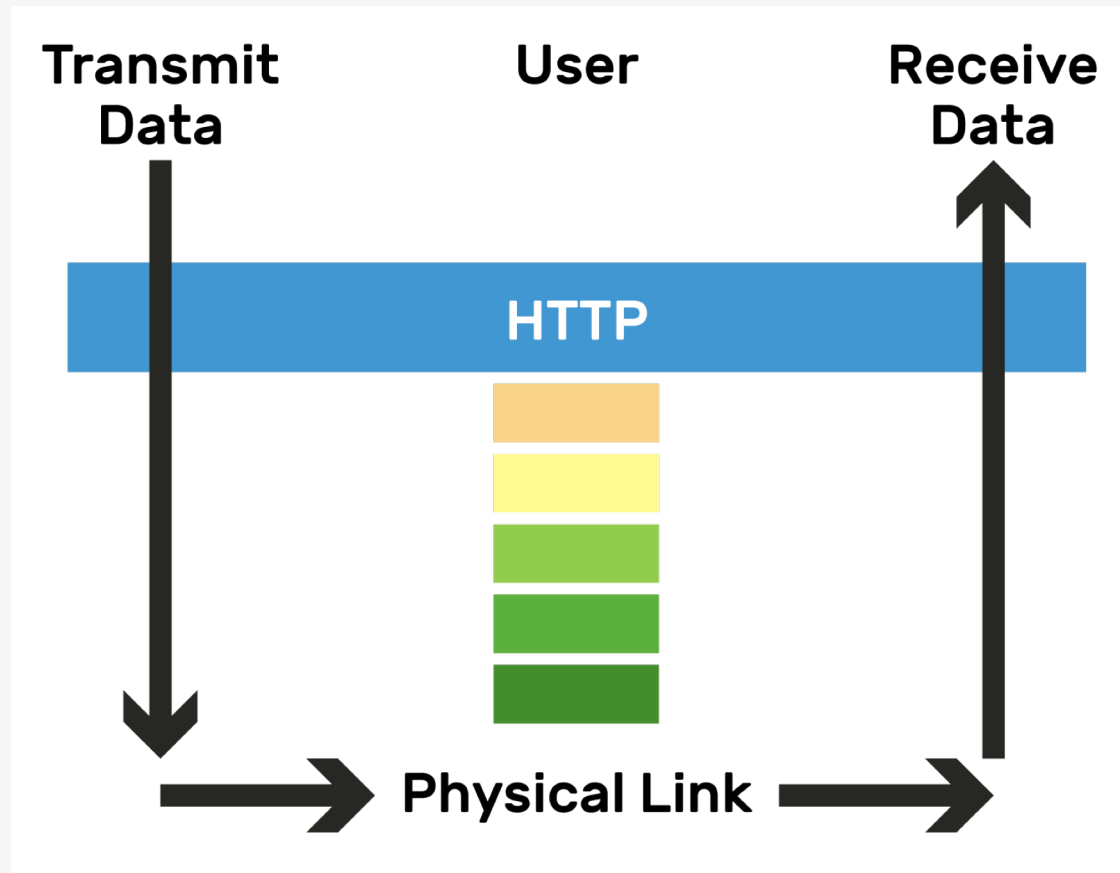
HTTP is ruling the world

- Modelo OSI



HTTP is ruling the world

- Internet real





Thank You!

Eduardo.duarte@dns.pt

www.dns.pt