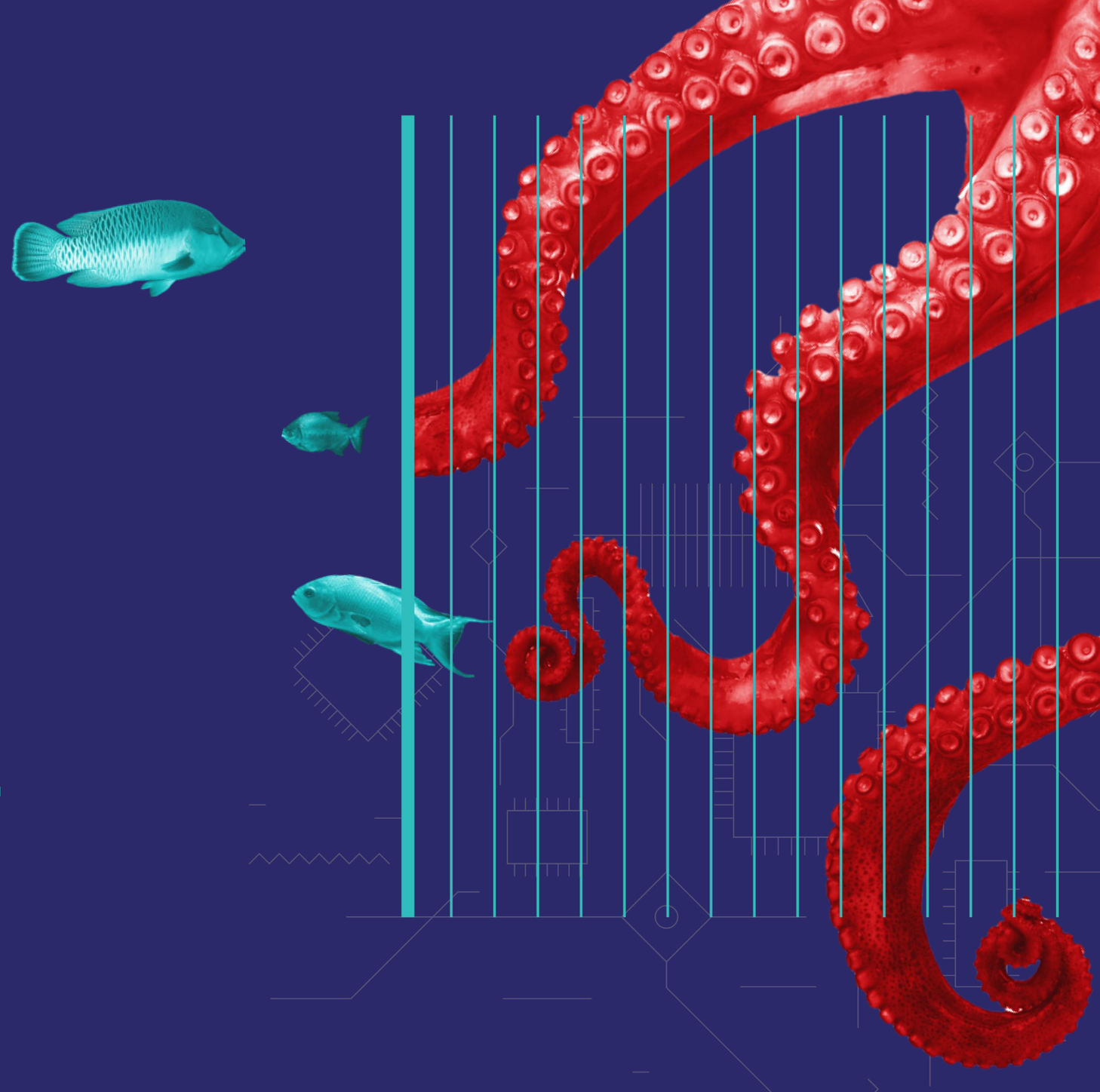
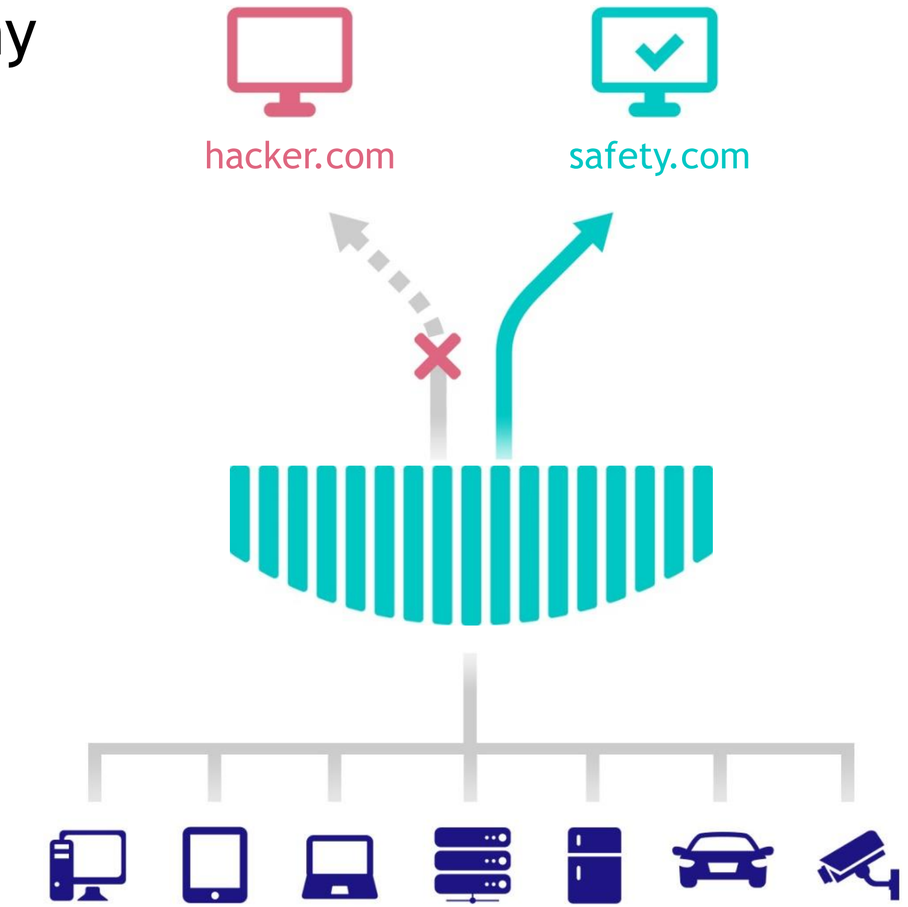
whalebone

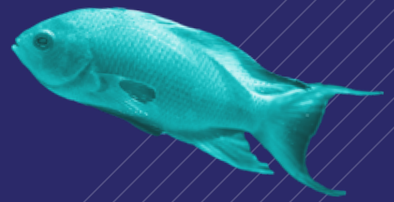


Novinky v DNS překladu a jeho šifrování

Vycházíme z vlastní praktické zkušenosti

- Whalebone poskytuje DNS překlad pro miliony zařízení
- Shoda se standardy, minimální latence a vysoká stabilita je priorita
- Anti-malware filtrační modul součástí resolveru
- Založeno na Knot Resolveru od CZ.NIC





DNSSEC

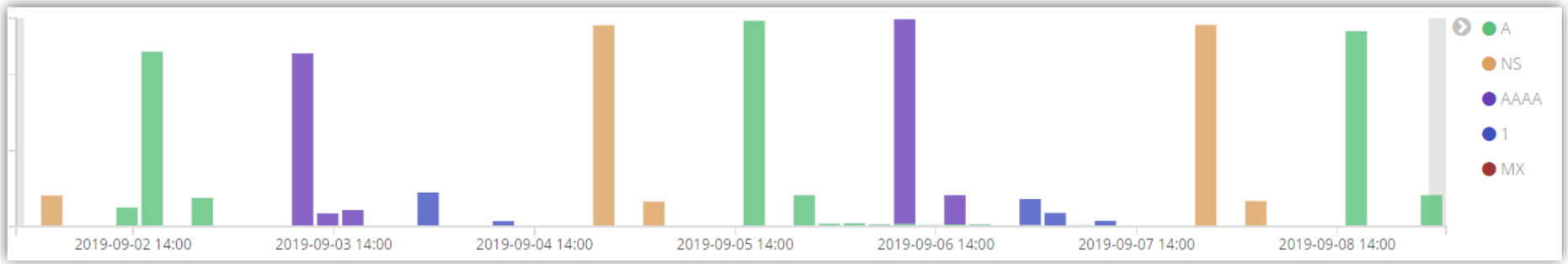
Random subdomain attacks

- Také označovány jako **„Slow drip attacks“**
- Na cílenou doménu útočí infikovaná zařízení skrze standardní resolvery ve své síti
- Generují velké množství dotazů na náhodné subdomény cílové domény. Pokud botnet dokáže vygenerovat dostatečné množství dotazů, zahltí úspěšně autoritativní servery
- Útok má negativní dopad i na resolver – spotřebovává cache a navyšuje odchozí provoz

xyz.ddostarget.com
abc.ddostarget.com
123.ddostarget.com
...

Útok na doménu weaverpublishing.com

weaverpublishing.com nameserver = ns1.weaverpublishing.com
weaverpublishing.com nameserver = ns2.weaverpublishing.com



mx2.mx2.mx1.mx1.mx1.mx2.mx2.mx1.mx1.mx2.mx1.mx2.mx2.mx2.mta-sts.mx2.mx2.webmail.weaverpublishing.com.
mx2.mx2.mx2.mx2.mx1.mx2.mx2.mx2.mx2.mx1.mx2.mx1.mx2.mx2.mx2.weaverpublishing.com.
mx2.mx2.mx2.mx2.mx1.mx2.mx2.mx2.mx2.mx1.mx2.mx1.mx2.mx2.mx2.weaverpublishing.com.
mx2.mx2.mx2.mx2.mx2.mx2.mx1.mx2.mx1.mx2.mx2.mta-sts.mx2.mx1.mx2.mx2.mx2.weaverpublishing.com.
mx2.mx2.mx2.mx2.mx2.mx2.mx1.mta-sts.mx2.mx1.mx1.mx1.mx1.mx2.mx1.webdisk.weaverpublishing.com.
mx2.mx2.mx2.mx2.mx2.mx2.mx1.mta-sts.mx2.mx1.mx1.mx1.mx1.mx2.mx1.webdisk.weaverpublishing.com.
mx2.mx2.mx2.mx2.mx2.mx2.mx1.mx2.mx1.mx2.mx2.mta-sts.mx2.mx1.mx2.mx2.mx2.weaverpublishing.com.
mx2.mx2.mx2.mx2.mx2.mx2.mx2.mx1.mx2.mx2.mx1.mta-sts.mx1.mx2.mx2.mx1.cpanel.weaverpublishing.com.
mx2.mx2.mx2.mx2.mx2.mx2.mx2.mx1.mx2.mx2.mx1.mta-sts.mx1.mx2.mx2.mx1.cpanel.weaverpublishing.com.
mx2.mx2.mx2.mx2.mx2.mx1.mx2.mx2.mx2.mx2.mx2.mx1.mx2.mta-sts.mx1.mx2.mx2.autodiscover.weaverpublishing.com.
mx2.mx2.mx2.mx2.mx2.mx1.mx2.mx2.mx2.mx2.mx2.mx1.mx2.mta-sts.mx1.mx2.mx2.autodiscover.weaverpublishing.com.
mx2.mx2.mx2.mx2.mx2.mx1.mx2.mx2.mx2.mx2.mx2.mta-sts.mx2.mx1.mx1.mx1.mx2.mail.weaverpublishing.com.

Virgin Media's promotional contest as for **Monday 9 September 2019**

Dear client Virgin Media,

we would like to thank you for your loyalty to **Virgin Media**, therefore, we offer you a chance to win a **Samsung Galaxy S10**.

Win a Galaxy S10!

↓ All you have to do is choose the correct gift box ↓

19 821 people like that.

Pauline Collet

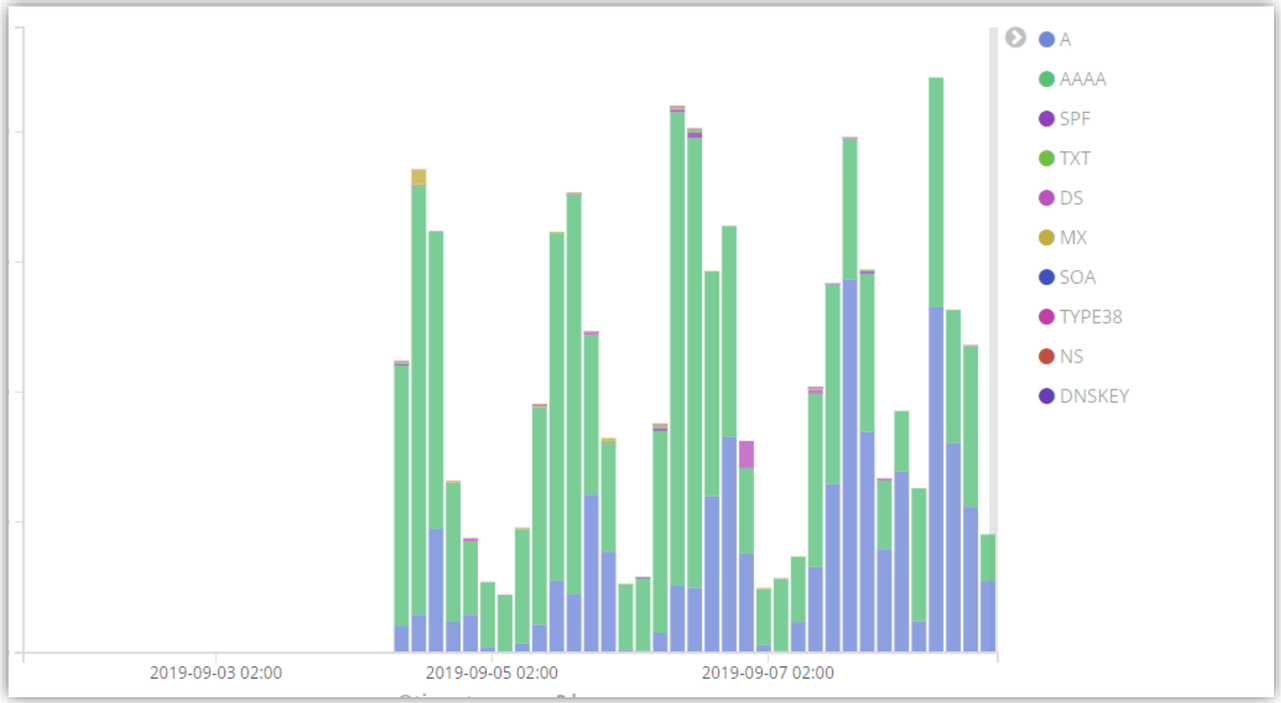
I'm so happy that I won!! I've just paid 1£ and now I'm waiting for my new Galaxy to come :)

Reply · Like · 4 minutes ago

Selhání DNSSEC validace

1. Domény s expirovaným DNSSEC klíčem
2. Chybně nakonfigurované domény (včetně TLD!)
3. Útoky

ISP je typicky první na ráně, když se hledá viník, přestože za to většinou nemůže



Nasazení DNSSECu na TLD .sk

- Spuštění DNSSECu na .sk provázely problémy
  - 8 serverů se správnou konfigurací
  - 6 serverů s chybnou konfigurací
- Překlad náhodně končil selháním DNSSEC validace
- Zákazníci se začali ozývat svým ISP
- Problém nebylo jednoduché spolehlivě reprodukovat, ale problém se podařilo najít díky nástroji DNSViz a spolupráci s CZ.NIC

- Po nahlášení SK.NIC byla oprava provedena velmi rychle, ale nebyl poskytnut žádný další komentář

Problémy s DNSSEC aggressive cache

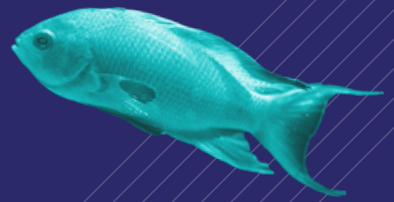
- F5 BIG-IP balancery – obvykle používané bankami, velkými službami a státními organizacemi
- Chybná implementace „proof of non-existence“
- Dotaz na neexistující query type způsobil, že balancer vrátil resolveru informaci „Existují pouze záznamy typu TXT“, což je pro resolver signál, že může vracet NXDOMAIN pro ostatní typy DNS záznamů
- Řešení:
  - Existuje patch i workaround od F5
  - Knot Resolver 4.2 již nevěří takto striktním odpovědím

Chyba v implementaci DNSSEC v BIG-IP load-balancerech od F5, Petr Špaček (CZ.NIC), https://blog.nic.cz/2019/07/10/chyba-v-implementaci-dnssec-v-big-ip-load-balancerech-od-f5/
Původní DVE vytvořený společností Whalebone za asistence CZ.NIC, https://github.com/dns-violations/dns-violations/blob/master/2018/DVE-2018-0003.md

DNSSEC – stojí za to?

- Odhadujeme, že k selhání DNSSEC validace dochází pouze v případě **0,01% všech DNS dotazů v našich sítích**
- DNSSEC validace je podmínkou pro připojení některých veřejných institucí
- DNSSEC chrání zákazníky před DNS cache poisoningem a útoky na DNS mimo síť ISP

- Když si nejste jisti, použijte DNSViz (Whalebone DNSViz přímo integruje):
  - Správně nakonfigurovaný DNSSEC: http://dnsviz.net/d/nic.cz/dnssec/
  - Problémy s DNSSEC: http://dnsviz.net/d/szn-broken-dnssec.cz/dnssec/



DNS over HTTPS

DNS over HTTPS (DoH)

- Aplikace nebo zařízení může komunikovat s DNS resolverem skrze HTTPS
- TLS vrstva zajistí autenticitu, integritu a důvěrnost přenášených dat – velký pokrok oproti DNS over UDP
  - Takto je možné efektivně ochranit „poslední míli“ mezi DNSSEC validujícím resolverem a klientem
- Resolver odpovídá na HTTPS
- Dotazy jsou zasílány jako GET parametr dotazu, např.:

```
GET /doh?dns=UE0BAAABAAAAAAAACmdtYWlsLWltYXABbAZnb29nbGUDY29tAAABAAE
```

DoH a důležití hráči na trhu

Od října aktivuje DoH ve Firefoxu jen v USA a jako resolver použije Cloudflare 1.1.1.1

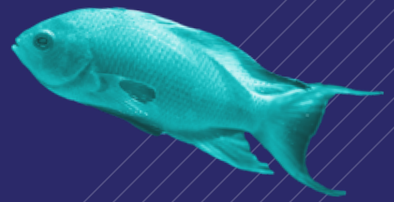
Chrome bude preferovat nastavení resolveru v zařízení, pokud bude resolver podporovat DoH

Aktivně pracuje na podpoře na úrovni svých OS, chce zachovat stávající logiku u ISP, korporátů, apod.

Zkoumá možnosti implementace do OS, spolupracuje s výrobci browserů a s velkými ISP na svých plánech

Další kroky na poli DoH

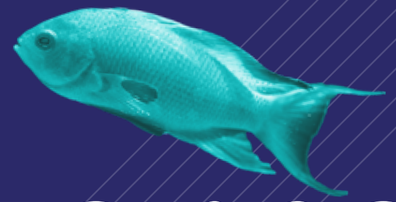
- Volání od více subjektů po definici Best Common Practices od IETF
- Existuje mnoho nedořešených problémů, ale není konsensus jak s nimi pokračovat, např.:
  - Únik informací v TLS handshake
  - User-Agent v HTTP requestu poskytuje více informací o klientovi než klasický DNS request
- Vznikají iniciativy, které chtějí usnadnit nasazení šifrovaní na DNS
  - Encrypted DNS Deployment Initiative (EDDI): https://www.encrypted-dns.org/participants



DNS a IPv6

IPv6 a DNS překlad

- Nasazení je instantní, stačí resolveru dát IPv6 adresu
- Stále velmi málo ISP plně podporuje DNS překlad na IPv6
- Velká výhoda je odbourání NATu v síti a s tím související zjednodušení topologie, řešení problémů, monitoringu, apod.



Děkuji za pozornost

Robert Šefr, CTO
robert.sefr@whalebone.io
@robcza

www.whalebone.io