DNS Flag Day 2020

Bude! 1. října 2020

2020-09-08
petr.spacek@nic.cz

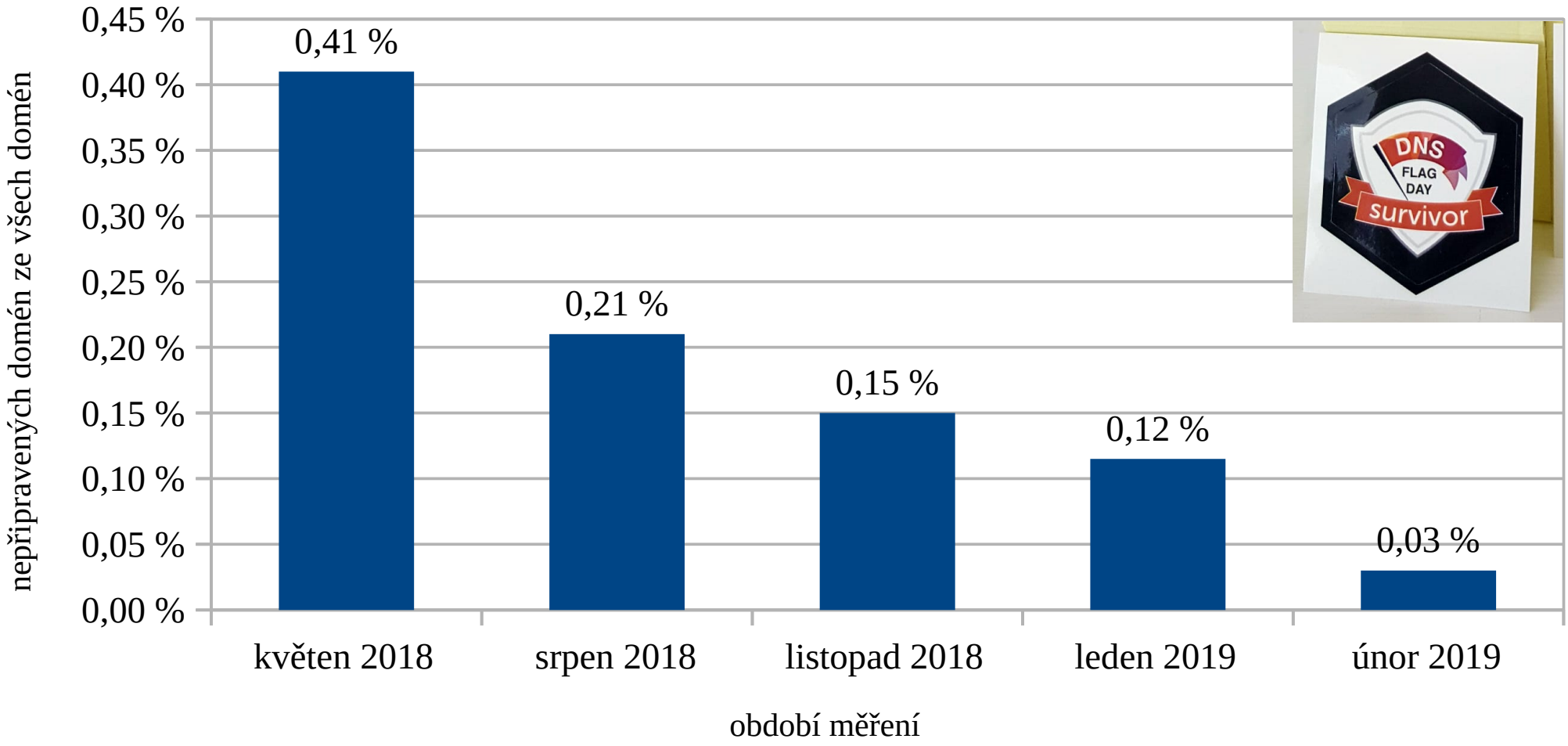
Obsah

- Teorie
- 2019
- 2020
- Dotazy

DNS Flag Day: Teorie

- DNS standard je složitý 
- Některé implementace ho nedodržují ⇒ nekompatibility
- Historicky byly přidávány hacky pro "kompatibilitu"
- Rozbité implementace nebyly motivovány k opravě
- Náprava: Koordinovaně odstraňovat hacky
  - Rozbité implementace musí být opraveny
- **Nemá vliv na korektní implementace**

2019: Podíl nepřipravených CZ domén (EDNS)



2019: Úspěch

- Drtivá většina domén opravena
  - Zbytek je "nezajímavý": parking, spekulanti, ...
- Žádné měřitelné problémy
- "Úklid v DNS" se podařil
- **Děkujeme za spolupraci!**

DNS flag day 2020

2020: Cíle

- Zlepšit spolehlivost DNS resolverů
- Zmenšit latenci
- Zlepšit bezpečnost
- *Vyhnout se problémům s IP fragmentací*
  - Timeout ⇒ nefunkční server?
  - Timeout ⇒ příliš velká odpověď?
  - Hádání max. velikosti, která ještě projde (EDNS buffer size)

2020: Odstranění UDP fragmentů

- **Pro velké DNS odpovědi** se přepne na TCP
  - Bez změny pro malé odpovědi – stále UDP
- Existující standard
  - RFC 7766: DNS Transport over TCP (a předchůdci)
- Technická změna
  - EDNS buffer size ~= 1232 bytů (= nefragmentovat na IP vrstvě)
  - Pro malý počet odpovědí přepnutí na TCP
- 1. října 2020

2020: Proč TCP?

- Nepotřebuje IP fragmentaci
- Ztěžuje podvrhávání
  - Validace domény při žádosti o WebPKI certifikát
- Existují standardy i implementace
- Nezbytný krok k
  - DNS-přes-TLS (DoT)
  - DNS-přes-HTTP (DoH)

2020: Motivace 1/2

- Velké DNS odpovědi přes UDP ⇒ IP fragmentace
- IP fragmentace **nefunguje spolehlivě**
  - Viz http://www.potaroo.net/ispcol/2017-08/xtn-hdrs.html
  - "Some 37% of endpoints used IPv6-capable DNS resolvers that were incapable of receiving a fragmented IPv6 response.”
  - **Reálné problémy, špatně se ladí**
- IETF: "IP fragmentace **je mrtvá"**
  - https://tools.ietf.org/html/draft-bonica-intarea-frag-fragile-03
  - ⇒ **nutnost adaptovat DNS implementace**

2020: Motivace 2/2

- Velké DNS odpovědi přes UDP ⇒ IP fragmentace
- IP fragmentace **není bezpečná**
  - Viz např. výzkum od JPRS (Kazunori Fujiwara)
    https://indico.dns-oarc.net/event/31/contributions/692/

2020: Problémy s IP fragmentací

- Způsobeny
  - rozbitou síťovou vrstvou
  - firewallem
  - DNS software bez podpory TCP ☢️
- Hlavní problém – timeouty
  - DNS dotaz ⇒ velká odpověď ⇒ timeout
- Timeout
  ⇒ problém se serverem, nebo ztráta paketu???
  - opakování, **latence pro uživatele**

2020: Zdroje problémů

- Autoritativní server
  - Neposlouchá na TCP portu 53
  - Ignoruje EDNS buffer size
    - Posílá velké odpovědi, i když je klient výslovně nechce
- Rekurzivní a stub resolver
  - Ignoruje flag TC=1
    - Nepřepne na TCP
- Firewall
  - Blokuje TCP port 53

2020: Autoritativní servery

- Musí dodržovat RFC 7766: DNS Transport over TCP
- **Musí odpovídat na TCP portu 53**
  - **Nezapomeňte na firewall!**
- EDNS buffer size ~= 1232 bytů
  - Výchozí nastavení v nových verzích
- Musí respektovat EDNS buffer size of klienta
  - Standardní software beze změn

2020: Resolvery

- Musí dodržovat RFC 7766: DNS Transport over TCP
- **Musí odpovídat na TCP portu 53**
  - **Nezapomeňte na firewall!**
- EDNS buffer size ~= 1232 bytů
  - Výchozí nastavení v nových verzích
- Musí respektovat EDNS buffer size of klienta
- Musí podporovat fallback z UDP na TCP
  - Standardní software beze změn

2020: Akademické experimenty

- Výzkum: A. Koolhaas, T. Slokker. Defragmenting DNS: Determining the optimal maximum UDP response size for DNS
  - https://indico.dns-oarc.net/event/36/contributions/776/
- Menší hodnoty jsou spolehlivější
- Závěr: Různá nasazení ⇒ různé optimální hodnoty
- Problém: Software "nezná" svůj způsob nasazení
- Důsledek: 1232 bytů je bezpečná výchozí hodnota

2020: Zahraniční měření

- Měření na Google resolverech v srpnu 2020
- Realistický test
  - Neodhalí domény, které neposílají velké odpovědi
- Podíl rozbitých domén: na úrovni šumu
- Přepnutí na TCP: na úrovni šumu
- Závěr: Není vidět žádné rozbití
- https://github.com/dns-violations/dnsflagday/issues/139#issuecomment-673489183

2020: Měření CZ domén

0,06 %

- Konzervativní test, nejhorší případ
  - Včetně domén, které neposílají velké odpovědi
- 782 domén nepodporuje TCP (k 27. 8. 2020)
- Měřeno pomocí https://gitlab.labs.nic.cz/knot/edns-zone-scanner/

2020: Testování

- Všechny dotazy přes TCP musí fungovat
  - $ dig **+tcp @auth_IP** vasedomena.example.
    - TCP na autoritativní server
  - $ dig **+tcp @resolver_IP** vasedomena.example.
    - TCP na resolver
  - $ dig **@resolver_IP** test.knot-resolver.cz. TXT
    - fallback na TCP pro velké odpovědi
- **Webový test: https://dnsflagday.net/**

2020: Konfigurace resolverů

- BIND
  options { edns-udp-size 1232; };
- Knot Resolver
  net.bufsize(1232)
- PowerDNS Recursor
  udp-truncation-threshold=1232
  edns-outgoing-bufsize=1232
- Unbound
  server:
  edns-buffer-size: 1232

2020: Konfigurace autoritativních serverů

- BIND
  ```
  options { max-udp-size 1232; };
  ```
- Knot DNS
  ```
  server:
      max-udp-payload: 1232
  ```
- PowerDNS Authoritative
  ```
  udp-truncation-threshold: 1232
  ```
- NSD
  ```
  server:
      ipv4-edns-size: 1232
      ipv6-edns-size: 1232
  ```

2020: Kontakty

- **Web https://dnsflagday.net/2020/**
- Twitter https://twitter.com/dnsflagday
- Oznámení e-mailem: https://lists.dns-oarc.net/mailman/listinfo/dns-announce
- Dotazy: dns-operations@lists.dns-oarc.net

2020: Závěr

- Otestujte svoje domény
- Web tester: https://dnsflagday.net/2020/
- Zprovozněte DNS-přes-TCP před 1. říjnem 2020
  - Google začně zmenšovat EDNS buffer size
  - Nové verze resolverů změní výchozí velikosti
- **Dotazy?**