DNS flag day

Nějak bylo, nějak bude

2019-05-28

Obsah

- 2019 – shrnutí
- 2020? – první informace
- Dotazy

DNS flag day 2019

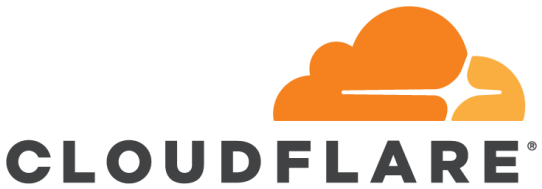
2019: Problémy s EDNS

- Způsobeny
  - zastaralým softwarem
  - nekorektním firewallem
- Hlavní problém – timeouty
  - dotaz s DO bitem → timeout
  - dotaz s EDNS → timeout
- Timeout
  → problém s EDNS nebo ztráta paketu???
  - opakování, **latence pro uživatele**

2019: Teorie

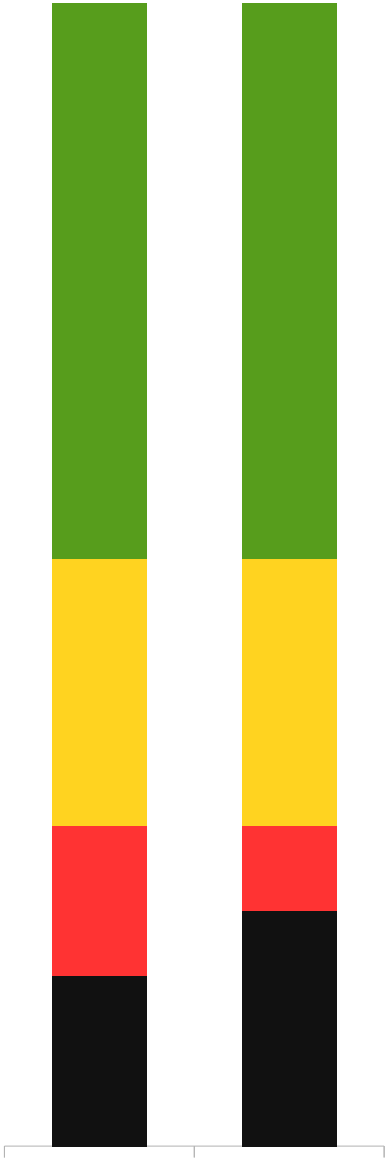
- Nesprávné implementace Extended DNS
- Hacky z roku **1999** způsobovaly problémy i v roce **2018!**
- Náklady na straně standardních implementací
  - Nejen kód
- **Nestandardní implementace nebyly motivovány k opravě**
- Plán: Odstranit nestandarní "workaroundy" pro EDNS

2019: Zapojené organizace



2019: T_0 - 3 měsíce, vzorek 23 M domén

Režim	Liberální (<= 2018)	Striktní (2019+)
Perfektní	48.61 %	
Kompatibilní	23.37 %	
Pomalé	13.15 %	7.48 %
Nefunkční	14.87 %	20.55 %
Ohrožené		+5.68 %



2019: T_0 - 3 měsíce: operátoři nedodržující standard

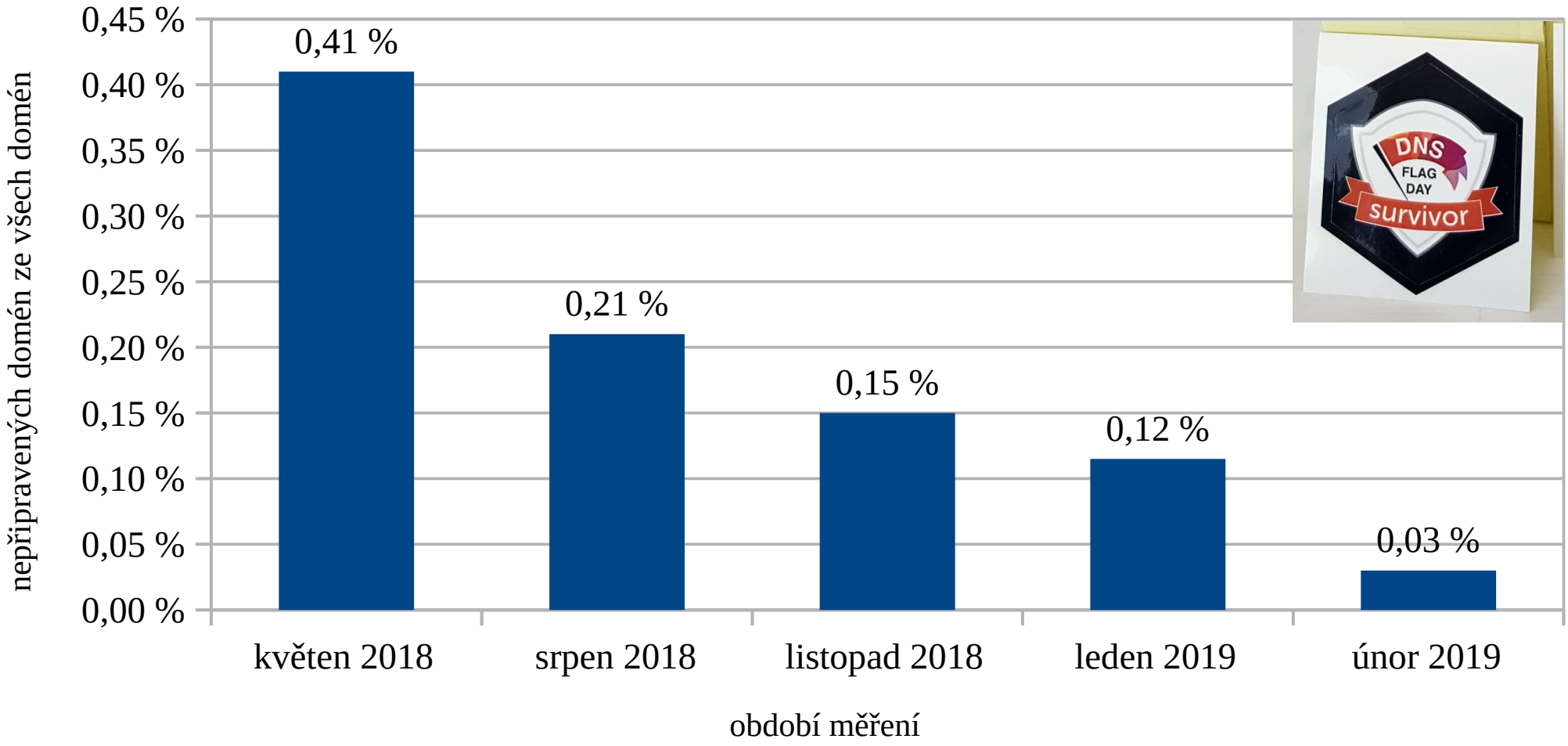
	doména operátora	podíl	ohrožené domény
	hichina.com.	35.78 %	469 611
Σ	dnspod.com.	25.66 %	336 797
	myhostadmin.net.	5.04 %	66 208
66 %	xincache.com.	4.82 %	63 246
	dnspod.net.	3.27 %	42 881
	dnsdun.net.	2.85 %	37 435
Σ	gmoserver.jp.	2.71 %	35 595
	registrar-servers.com.	1.64 %	21 533
	alidns.com.	1.63 %	21 369
85 %	metaregistrar.nl.	1.20 %	15 762

2019: Dopad

2019: Úspěch

- Drtivá většina domén opravena
  - Zbytek je "nezajímavý": parking, spekulanti ...
- Technická podpora neshořela :-)
- Žádné měřitelné problémy
  - DNS OARC 30 - DNS flag day panel discussion
- "Úklid v DNS" se podařil
- **Děkujeme za spolupraci!**

2019: Podíl nepřipravených CZ domén (EDNS)



DNS flag day 2020

2020: Problémy s IP fragmentací

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

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: Cíle

- Vyhnout se problémům s IP fragmentací
  - Timeout -> nefunkční server?
  - Timeout -> příliš velká odpověď?
  - Hádání EDNS buffer size ...
- Zlepšení bezpečnosti

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 ~= 1220 (= nefragmentovat)

2020: Možné problémy

- Autoritativní server
  - Neposlouchají na TCP 53
  - Ignoruje EDNS buffer size
- Rekurzivní a stub resolver
  - Ignoruje bit TC=1
- Firewall
  - TCP port 53

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)

2020: Autoritativní servery

- Musí dodržovat RFC 7766: DNS Transport over TCP
- **Musí odpovídat na TCP portu 53**
  - **Nezapomeňte na firewall!**
- EDNS buffer size ~= 1220
  - Výchozí nastavení bude změněno
- Musí respektovat EDNS buffer size of klienta
  - Standardní software beze změn

2020: Předběžná měření - autoritativní strana

- ~ 7 % domén je na rozbitých serverech
  - Zahrnuje zaparkované domény atd.
  - Není doména jako doména
- Opakují se jména známá z 2019
- 1 operátor > 70 %
- 9 operátorů > 90 %

2020: Chybějící TCP, 2019/5, 34 M domén, 59 TLD

Režim	Velké fragmenty	TCP vyžadováno
Perfektní	67.52 %	67.52 %
Pomalé	12.83 %	5.76 %
Nefunkční	19.65 %	26.72 %
Ohrožené		+7.07 %

email, solutions, tel, date, review, one, link, services, company, agency, group, guru, news, network, photography, studio, jobs, business

net, co, xyz, se, cz, loan, online, club, site, icu, nz, shop, ltd, cl, mobi, app, live, pro, website, space, nu, fun, store, win, tech, men, life, blog, stream, world, dev, wang, bid, rocks, cat, tokyo, xxx, today, design, trade, xin

2020: Operátoři nedodržující standard, 2019/5

	doména operátora	podíl	ohrožené domény
Σ	hichina.com	67.84 %	1 610 817
	name-services.com	6.74 %	160 070
	foundationapi.com	3.66 %	86 970
70 %	xincache.com	2.63 %	62 479
	alidns.com	2.16 %	51 309
	123-reg.co.uk	2.04 %	48 411
Σ	domainparkingserver.net	1.69 %	40 036
	ztomy.com	1.27 %	30 238
	mytrafficmanagement.com	1.23 %	29 285
90 %	myhostadmin.net	1.05 %	24 856

2020: Resolvery

- Musí dodržovat RFC 7766: DNS Transport over TCP
- **Musí odpovídat na TCP portu 53**
  - **Nezapomeňte na firewall!**
- EDNS buffer size ~= 1220
  - Výchozí nastavení bude změněno
- Musí respektovat EDNS buffer size of klienta
- Musí podporovat fallback z UDP na TCP
  - Standardní software beze změn

2020: Předběžná měření - resolvery

- ~ 2,5 % uživatelů za rozbitým resolverem
  - Není resolver jako resolver
- Viz http://www.potaroo.net/ispcol/2017-08/xtn-hdrs-2.html

2020: Podíl nepřipravených CZ domén (TCP)

0,09 %

- 1125 celkem (k 25. 5. 2019)
- 1 operátor > 44 %
- 2 operátoři > 55 %
- 10 operátorů > 75 %

2020: Testování

- **Webový nástroj připravujeme**
- 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

2020: Konfigurace resolverů

- BIND
  options { edns-udp-size 1220; };
- Knot Resolver
  net.bufsize(1220)
- PowerDNS Recursor
  udp-truncation-threshold=1220
  edns-outgoing-bufsize=1220
- Unbound
  server:
    edns-buffer-size: 1220

2020: Konfigurace autoritativních serverů

- BIND
  ```
  options { max-udp-size 1220; };
  ```
- Knot DNS
  ```
  server:
      max-udp-payload: 1220
  ```
- PowerDNS Authoritative
  ```
  udp-truncation-threshold: 1220
  ```
- NSD
  ```
  server:
      ipv4-edns-size: 1220
      ipv6-edns-size: 1220
  ```

2020: Co chybí

- Přesné datum
  - Probíhá měření
- Přesná hodnota EDNS buffer size
  - 1220, 1232, 1280, ...
  - Nová defaultní hodnota
- Webový tester
- *Princip zůstává*
  - **DNS přes TCP musí fungovat**

2020: Sledujte novinky

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