Infrastruktura DNS

Ondřej Caletka

cesnet

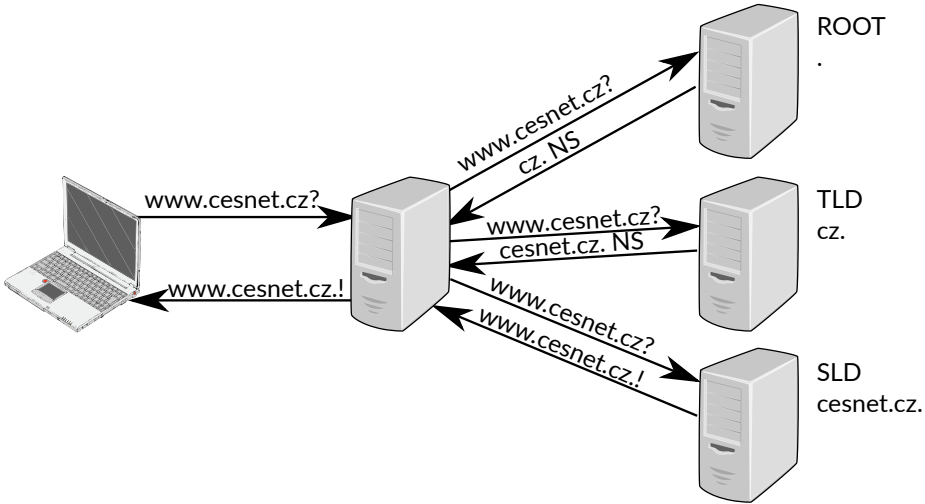
25. dubna 2018

DNS: minutes to learn, a lifetime to master

Shane Kerr

cesnet

O službě DNS


ROOT
.
TLD
cz.
SLD
cesnet.cz.
www.cesnet.cz?
cz. NS
www.cesnet.cz?
www.cesnet.cz?
cesnet.cz. NS
www.cesnet.cz.!
www.cesnet.cz?
www.cesnet.cz.!
stub resolver
rekurzivní resolver
autoritativní server

Klíčové prvky

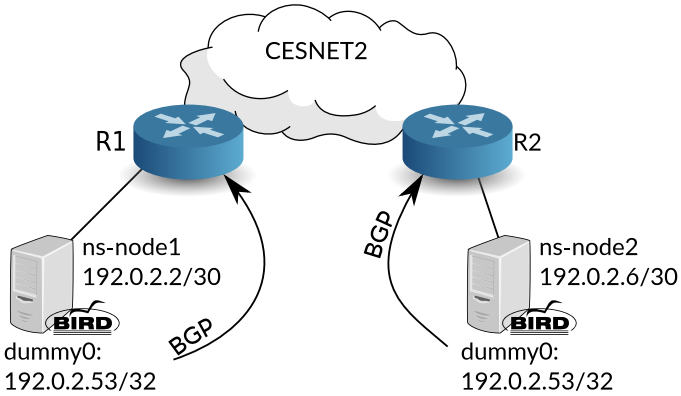
- rekurzivní servery (resolvery)
  - pouze pro interní použití
  - validace DNSSEC podpisů
  - požadavek na vysokou dostupnost dané IP adresy
- autoritativní servery
  - veřejná služba
  - několik replik kvůli robustnosti
  - ideálně globální anycast – řešení, které používá kořenová zóna
  - správně nastavená doba života záznamů

cesnet

Vysoká dostupnost rekurzivních serverů

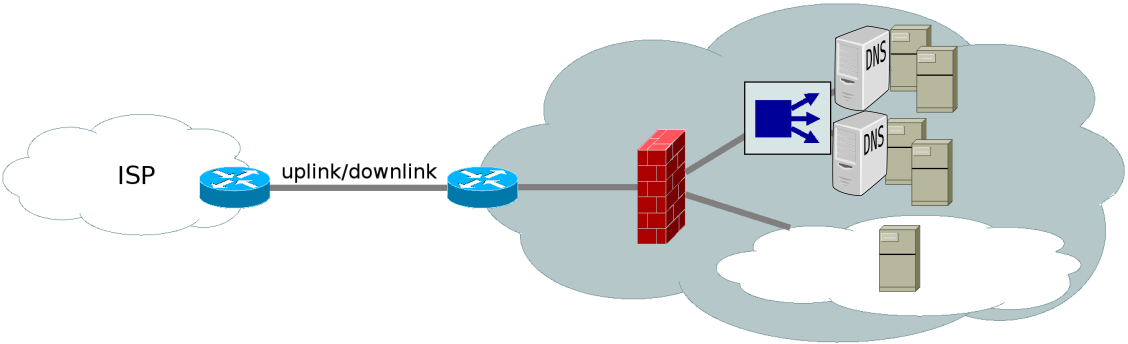
hodí se zejména v kombinaci s GNU stub resolverem

- tradiční HA pomocí linux-HA, pacemaker…
- anycasting v rámci vlastní sítě – zabezpečí i proti výpadku směrovače



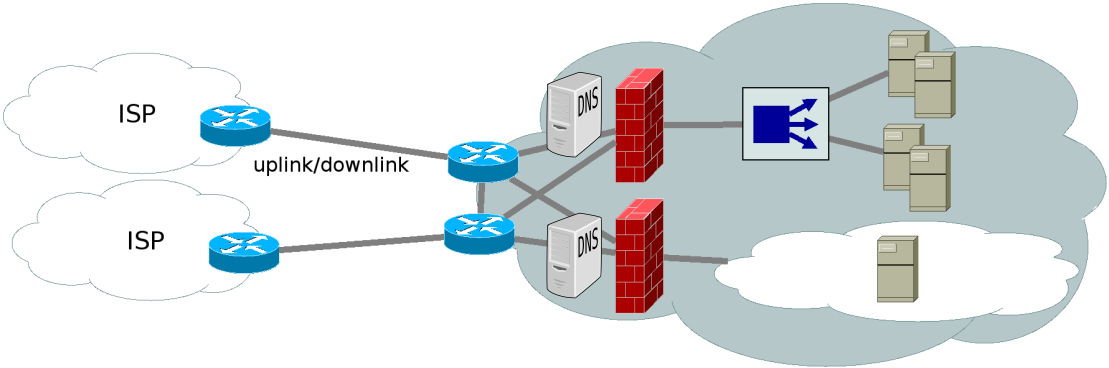
cesnet

Špatné umístění autoritativních serverů



cesnet

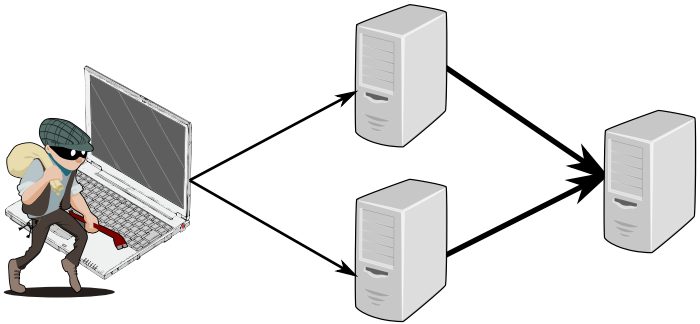
Lepší umístění autoritativních serverů



cesnet

Odrazný a zesilující útok

- založeno na falšování zdrojových adres
- útočník posílá dotazy jménem oběti
- obět dostává nevyžádané odpovědi



Příčinou je falšování zdrojových adres

- k útoku lze použít *jakýkoli* protokol
- rozdíly v paketovém a bajtovém zesilujícím faktoru

protokol	zesílení bajtů	zesílení paketů
DNS	28–54	1–5
NTP	556,9	100
SNMPv2	6,3	
SSDP	30,8	
Quake	63,9	
Steam	5,5	
Memcached	až 51000	až 25000
TCP	1	1

zdroj: US-CERT TA14-017A

cesnet

DNSSEC za nic nemůže

There's a lot of urban legend out there about how DNSSEC makes DDoS worse because of DNSSEC's larger message size, and while this makes intuitive sense and "sounds good", it is simply false. (...) In short, no attack requires DNSSEC, and thus any focus on DNSSEC as a DDoS risk is misspent energy.

zdroj: Paul Vixie na dotaz „What kinds of security vulnerabilities does providing DNSSEC expose?"

cesnet

Jak problém řešit?

1. zabránit falšování zdrojových adres
   - BCP 38, BCP 84
   - nutno přesvědčit všechny na světě
   - *pozitivní vliv NATů*
2. omezit zbytné velké odpovědi
   - přidat další komplexitu do existujících protokolů
3. dělat obojí *aspoň* napůl
   - bráníme falšování ve vlastní síti, abychom nebyli zdrojem útoku
   - zabezpečujeme služby, aby neodrážely víc, než je nezbytně nutné

cesnet

Omezení zesilujícího efektu

- rekurzivní servery
  - povolujeme pouze z vlastní sítě
- autoritativní servery
  - zapínáme response rate limiting
  - omezujeme výchozí velikost UDP bufferu

Response Rate Limiting

Obecná technika limitování odpovědí autoritativních serverů na opakující se dotazy ze stejné adresy. Implementováno nativně v Knot DNS, NSD a BIND 9.9.

cesnet

DNS cookies pro efektivnější RRL

- RFC 7873 rozšiřuje DNS protokol o jednoduchou autentizaci klientů a serverů s postupným zaváděním
- klient vygeneruje a pošle s dotazem $ccookie = \mathrm{f}(csecret, server\ IP)$
- server vygeneruje a vrátí s odpovědí $scookie = \mathrm{f}(ssecret, ccookie, client\ IP)$
- klient dále přidává *ccookie* i *scookie* k dotazům, takže je jisté, že nejde o zfalšovanou adresu
- pokud cookie nesouhlasí, je příchozí dotaz podroben RRL a případně zahozen
- prozatím těžko použitelné kvůli *rozbitým* autoritativním serverům

cesnet

Společně proti porušování DNS standardů

- dohoda výrobců nejznámějších resolverů
  - ISC (Bind)
  - NLnetLabs (Unbound)
  - PowerDNS
  - CZ.NIC Labs (Knot DNS Resolver)
- cílem je eliminovat špatné implementace EDNS0 (z roku 1999) na autoritativních serverech
- resolvery vydané po 1. únoru 2019 nebudou obsahovat *workaroundy*
- chování autoritativního serveru je možné otestovat na `https://ednscomp.isc.org`

Root.cz: Společně za zlepšení stability, rychlosti a další rozšiřitelnosti DNS ekosystému

cesnet

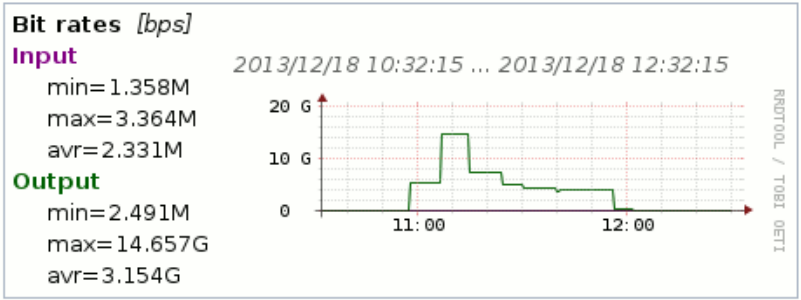
Omezení velikosti UDP odpovědi

- rozšíření EDNS0 zvětšuje délku UDP zpráv nad 512 B
  obvykle na 4096 B
- omezením velikosti k ~1 kB snížíme účinnost zesilujícího útoku
- také se tím zlepší situace resolverům s nefunkčním *Path MTU Discovery*
- příliš nízká hodnota může naopak rozbít resolvery bez TCP konektivity
  - obzvláště při použití DNSSEC
  - takto postižených uživatelů je ~2 % (měření Geoffa Hustona)

cesnet

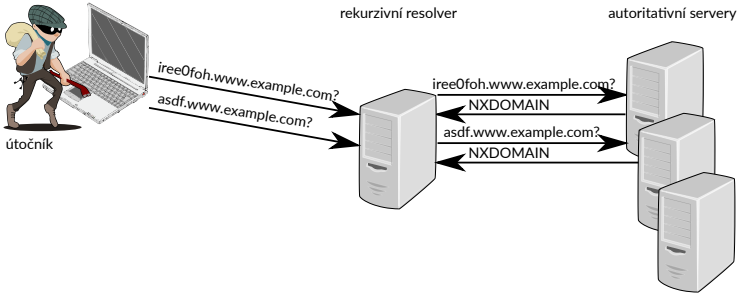
Když jste pod útokem

- incident 18. 12. 2013 11:00 – 12:00 CET
- zahlcení hlavního DNS resolveru UDP pakety na náhodná čísla portů, *obsahující* `128 × 0x00`
- provoz přicházel ze všech zahraničních linek z náhodných adres
- pro oběť bez jednoduché možnosti obrany



Útok náhodnými dotazy

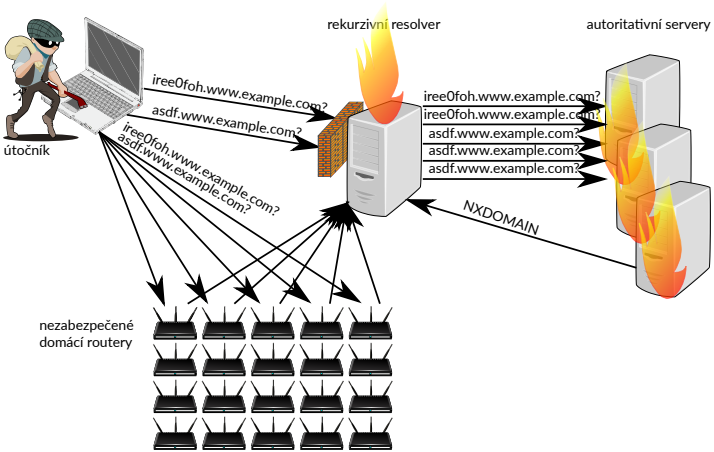
- útočící botnet pokládá dotazy ve stylu `<random string>.www.example.com`
- dotaz je vždy přeposlán autoritativnímu serveru
- autoritativní server se pod náporem hroutí
- rekurzivní server čeká na odpověď a zkouší dotazy opakovat



https://www.root.cz/clanky/utok-na-dns-nahodnymi-dotazy/

Přetížení rekurzivních serverů

- `fetches-per-server` v BIND
- `ratelimit` v Unbound



cesnet

Přetížení autoritativních serverů

Otázka: Proč používáme Anycast DNS?
Odpověď: Pro odolnost vůči útokům, snížení latence je sekundární efekt.

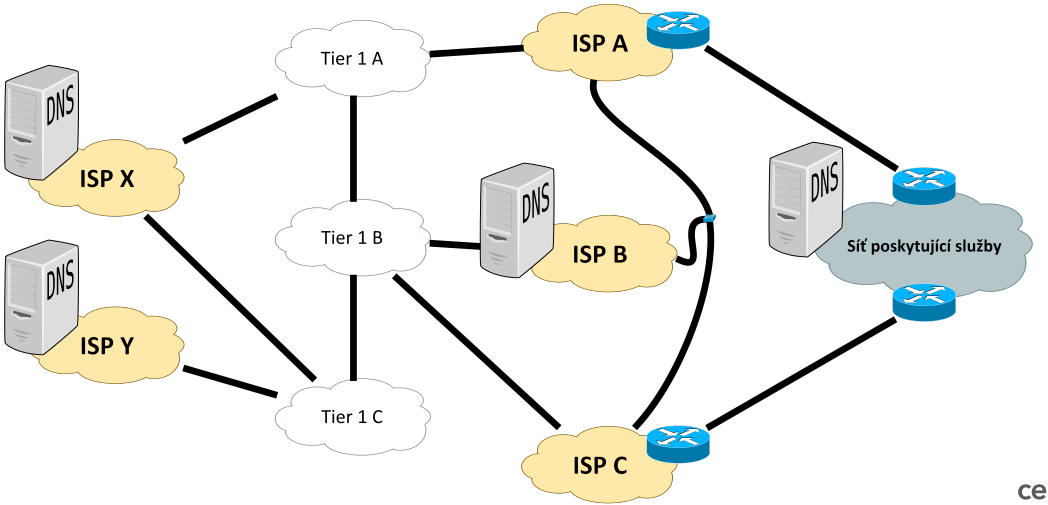
Otázka: Co tvoří většinu provozu?
Odpověď: **Odpad.**

Otázka: Kam bychom měli instalovat nové instance?
Odpověď: ~~Tam, kde chtějí správné odpovědi.~~ **ŠPATNĚ**
Odpověď: Tam, **odkud se hrne odpad**.

Zdroj: Randy Bush @ DNS-WG

cesnet

Ideální umístění autoritativních serverů



cesnet

Shrnutí pravidel pro kritické služby

- zabezpečit rekurzivní servery
  - aktivovat DNSSEC validaci
  - blokovat příchozí provoz z internetu, povolit pouze DNS odpovědi
- zabezpečit autoritativní servery
  - umístit **před** firewall
  - dostatečně dimenzovat linku
  - co nejvíce diverzitní repliky
  - zabezpečit zónové přenosy (TSIG)
- společné
  - zkontrolovat funkčnost TCP spojení
  - omezit velikost UDP zpráv (ideálně na polovině serverů)
  - zkontrolovat průchodnost ICMP zpráv (objevování MTU cesty)

cesnet

Děkuji za pozornost

Ondřej Caletka
Ondrej.Caletka@cesnet.cz
https://**Ondřej.Caletka.cz**

Prezentace je již nyní k dispozici ke stažení.