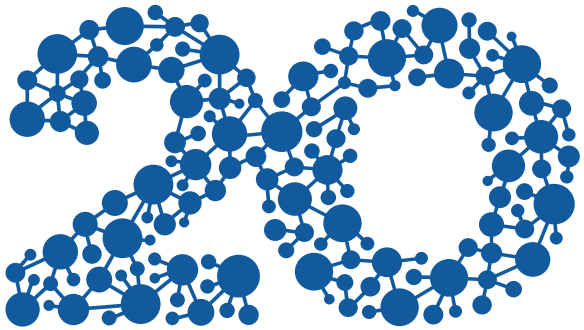
Útoky na DNS

Ondřej Caletka



1996–2016
CESNET
SPOLUPRÁCE
VÝZKUM
KOMUNITA

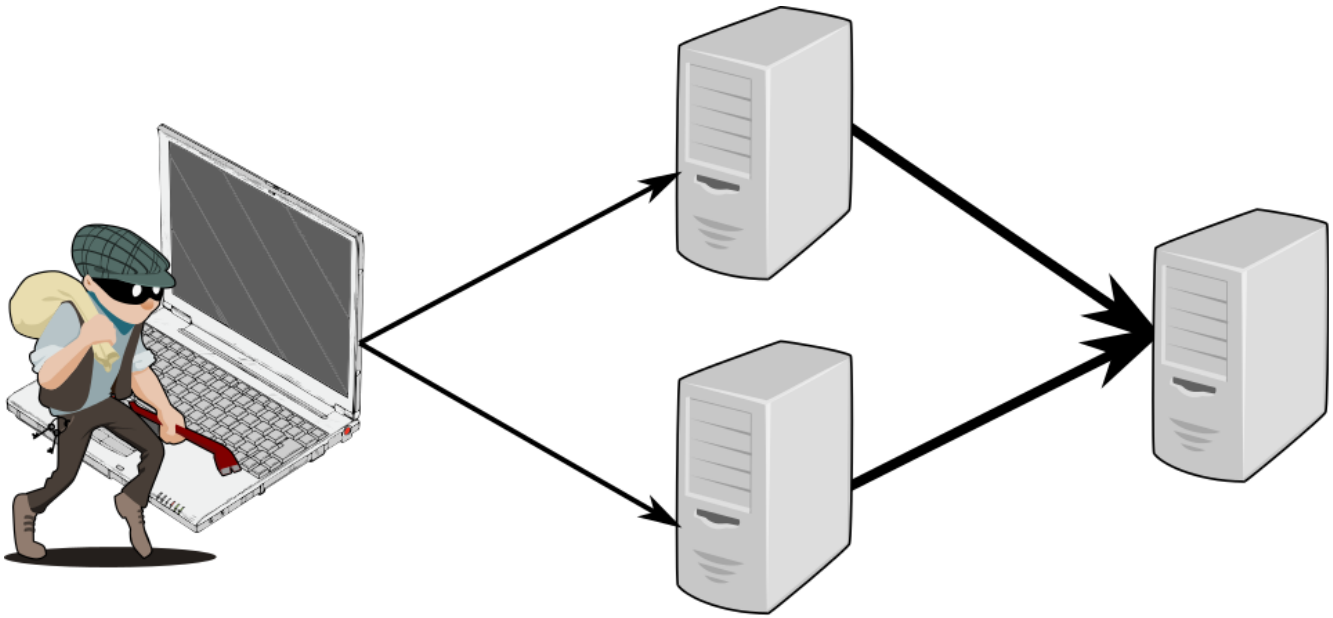
9. února 2016

DNS: minutes to learn, a lifetime to master

Shane Kerr

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 zesilovacím 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	
TCP	1	1

zdroj: US-CERT TA14-017A

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?"

Jak problém řešit?

1. zabránit falšování zdrojových adres
   - BCP 38, BCP 84
   - **TODO:** přemluvit 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

Omezení zesilovacího 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.

DNS cookies pro efektivnější RRL

- návrh rozšíření protokolu DNS 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

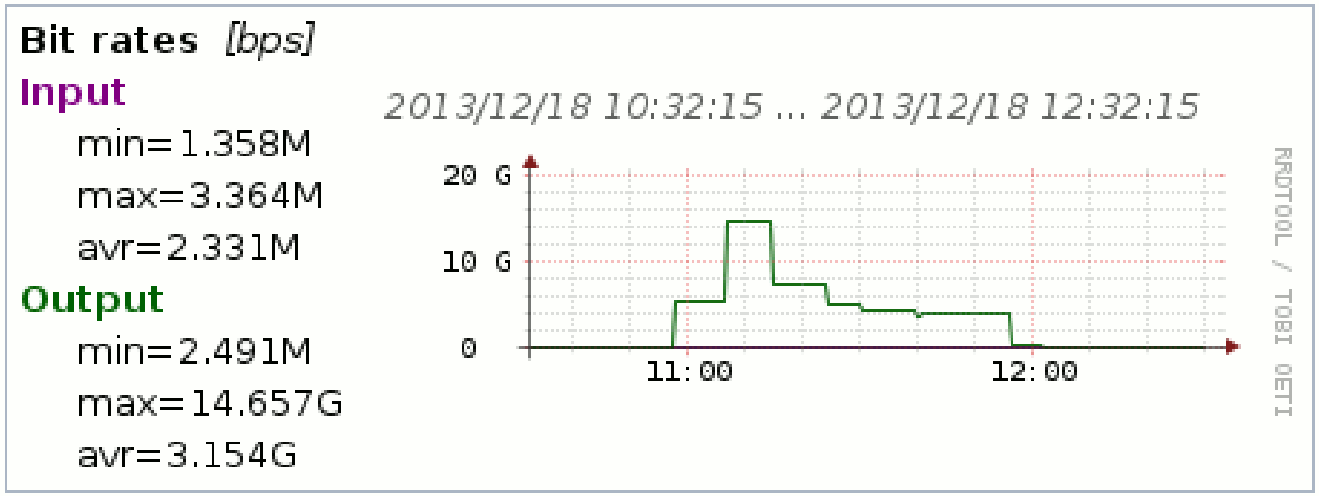
`https://tools.ietf.org/html/draft-ietf-dnsop-cookies-09`

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)

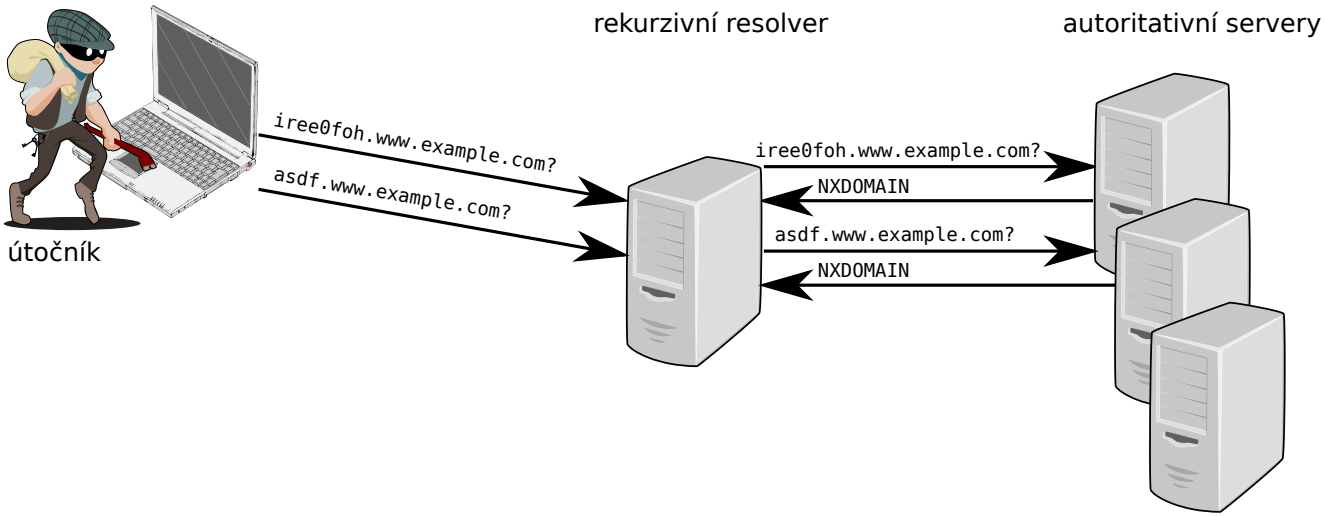
Když jste pod útokem

- 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 obět bez možnosti obrany



Útok náhodnými dotazy

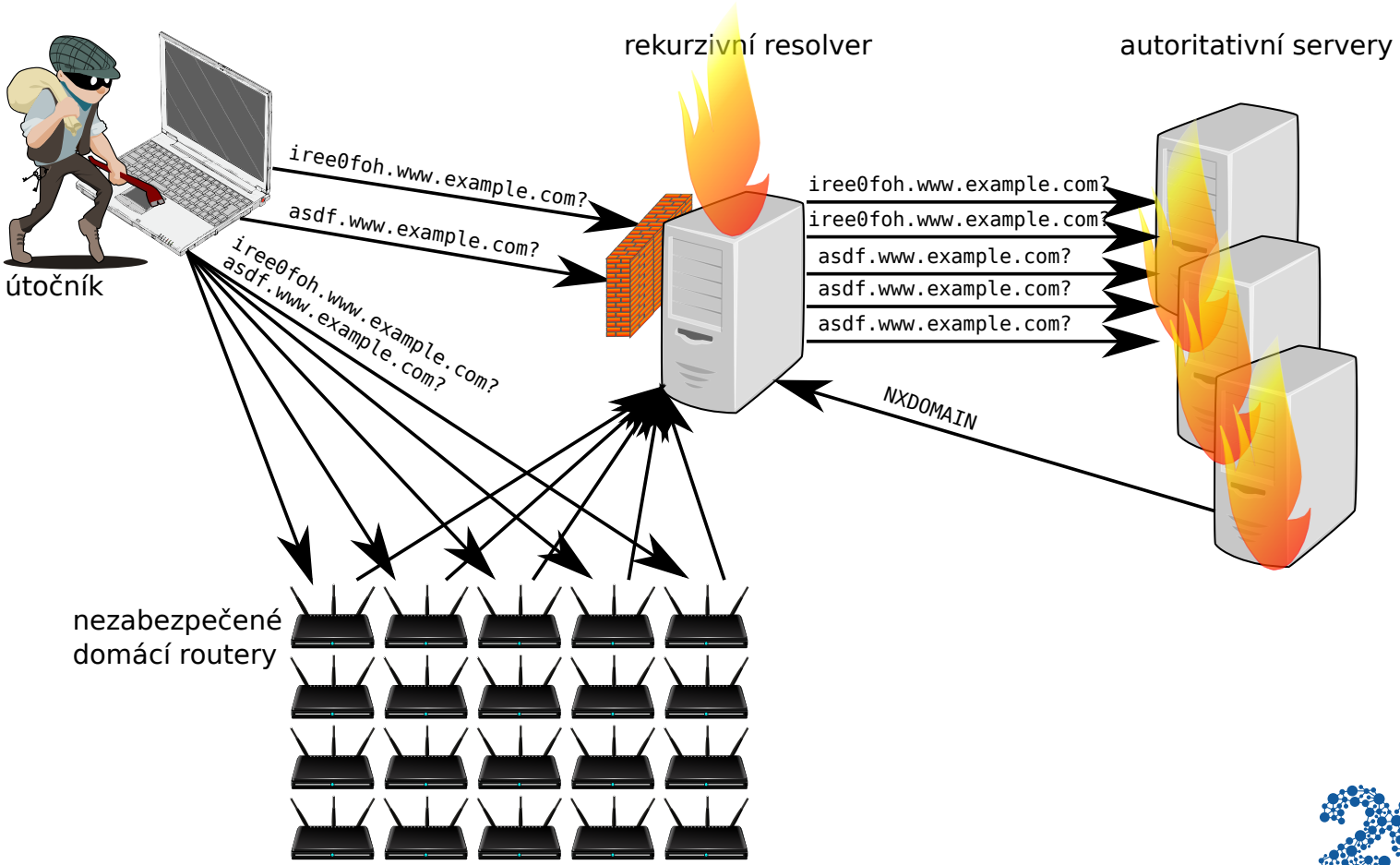
- postihuje zároveň rekurzivní i autoritativní servery
- útočící botnet pokládá dotazy ve stylu `<random string>.www.example.com`
- dotaz je vždy přeposlán autoritativnímu serveru
- autoritativní server se pod náporem hroutí
- rekurzivní server čeká na odpověď a zkouší dotazy opakovat



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

Přetížení rekurzivních serverů

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



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

Budujeme globální Anycast

Potřebné ingredience:

- 1× veřejné číslo AS
- 1× /24 IPv4 adresy
- 1× /48 IPv6 adresy (preferovaně tzv. PI adresy)
- n× geograficky rozmístěné DNS servery
  - v housingu s plnou IPv4 a IPv6 konektivitou
  - v housingu ochotném navázat se serverem BGP session *(zkusíme oslovit NRENy)*
  - ohlašující daný AS s danými IPv4 a IPv6 adresami
  - centrální provisioning a orchestrace

Inspirace: `https://noc.esgob.com/`

Útok nekonečnou delegací

- upravený autoritativní server
- posílá nové a nové reference
  - `1.example.com.` delegováno na `2.example.com.`
  - `2.example.com.` delegováno na `3.example.com.`
- omezení trvání/hloubky rekurze implementováno v serverech od prosince 2014
- v praxi jsme nezaznamemali

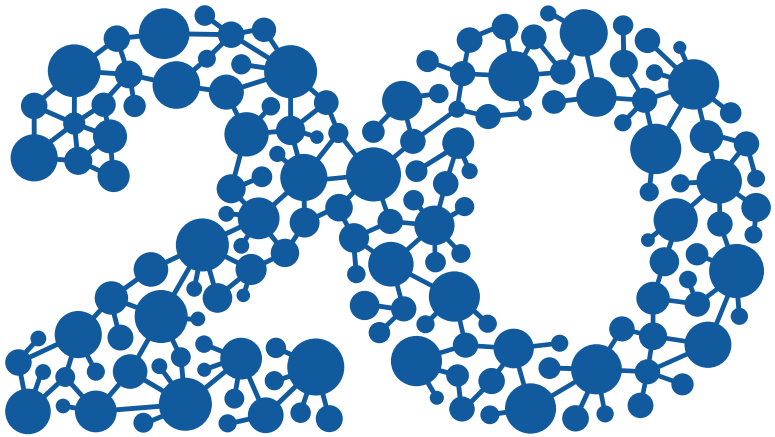
1996–2016 CESNET

`https://www.root.cz/clanky/utok-na-dns-nekonecnou-rekurzi/`

Závěr

Děkuji za pozornost

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



1996–2016
CESNET
SPOLUPRÁCE
VÝZKUM
KOMUNITA