DDoS v DNS

Principy a protiopatření

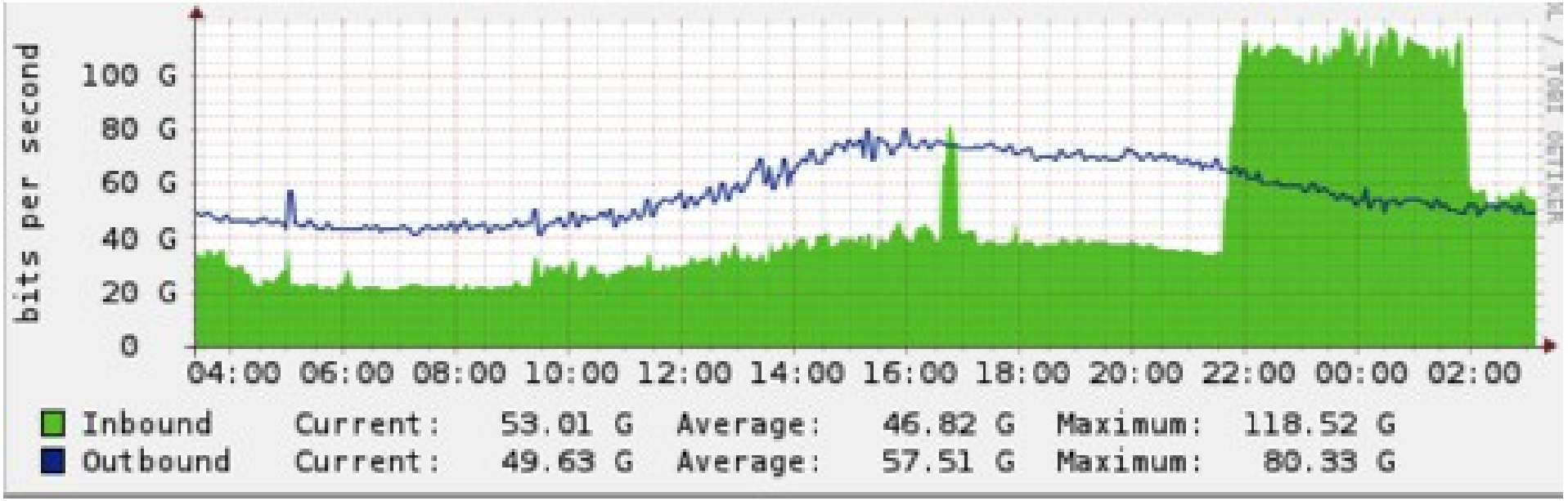
Ondřej Surý • ondrej.sury@nic.cz • 20.5.2013

CZ.NIC | SPRÁVCE DOMÉNY CZ

DNS DDoS – akce

DNS DDoS – reakce

DNS DDoS – výsledek



DNS DDoS – detailněji

- Dva (hlavní) faktory
  - **Podvržení zdrojové adresy**
  - Amplifikace odražených paketů

Amplifikace DNS paketů

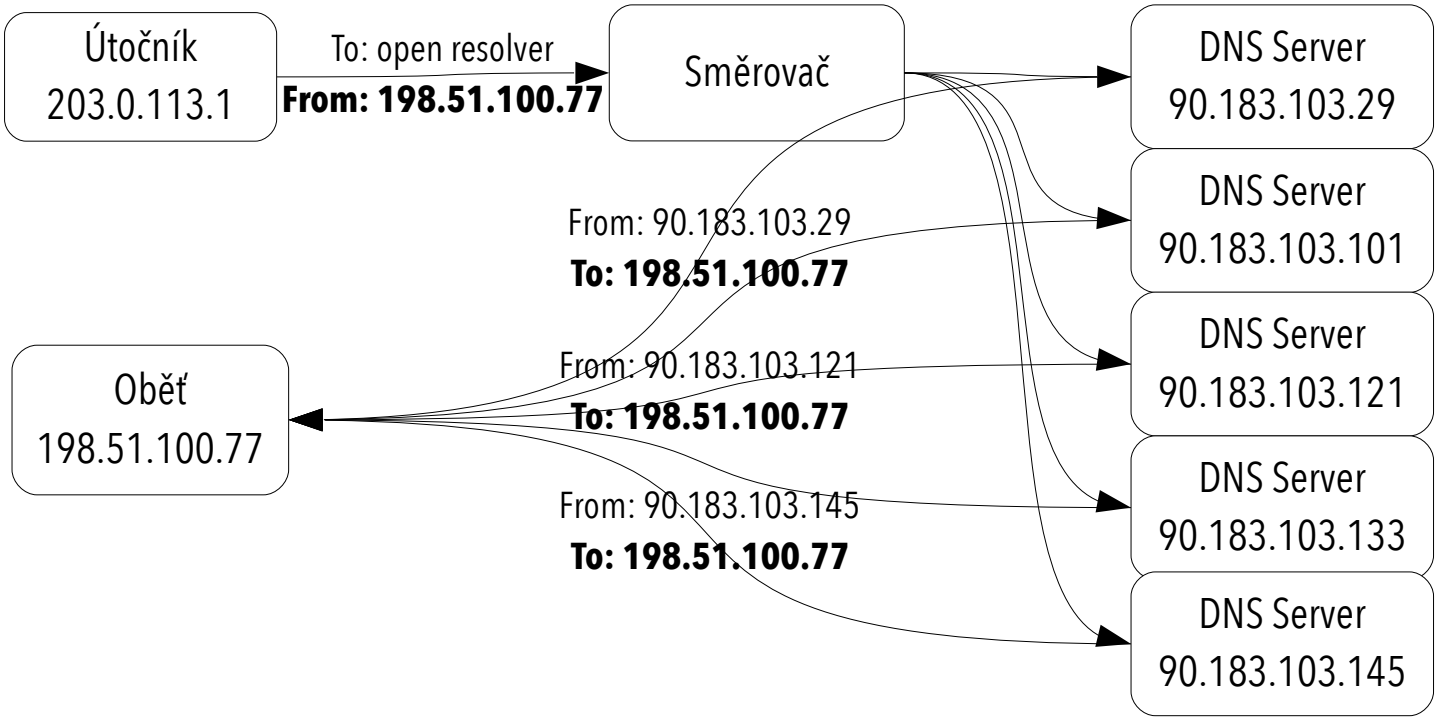
```
dig +ignore IN ANY ietf.org.
```

- Malý DNS dotaz
  - Velikost DNS obsahu je < 30 bajtů
- Velká DNS odpověď
  - Velikost DNS obsahu je ~ 4k
- Nárust o dva řády!

Podvržení zdrojové adresy

- Podvržení zdrojové adresy je velmi snadné
  - Platí pro všechny IP protokoly (TCP, UDP, ICMP, …)
- UDP je nestavový protokol (nemá handshake)
  - Ohroženy jsou všechny UDP protokoly (např. NTP)

Podvržení zdrojové adresy v DNS



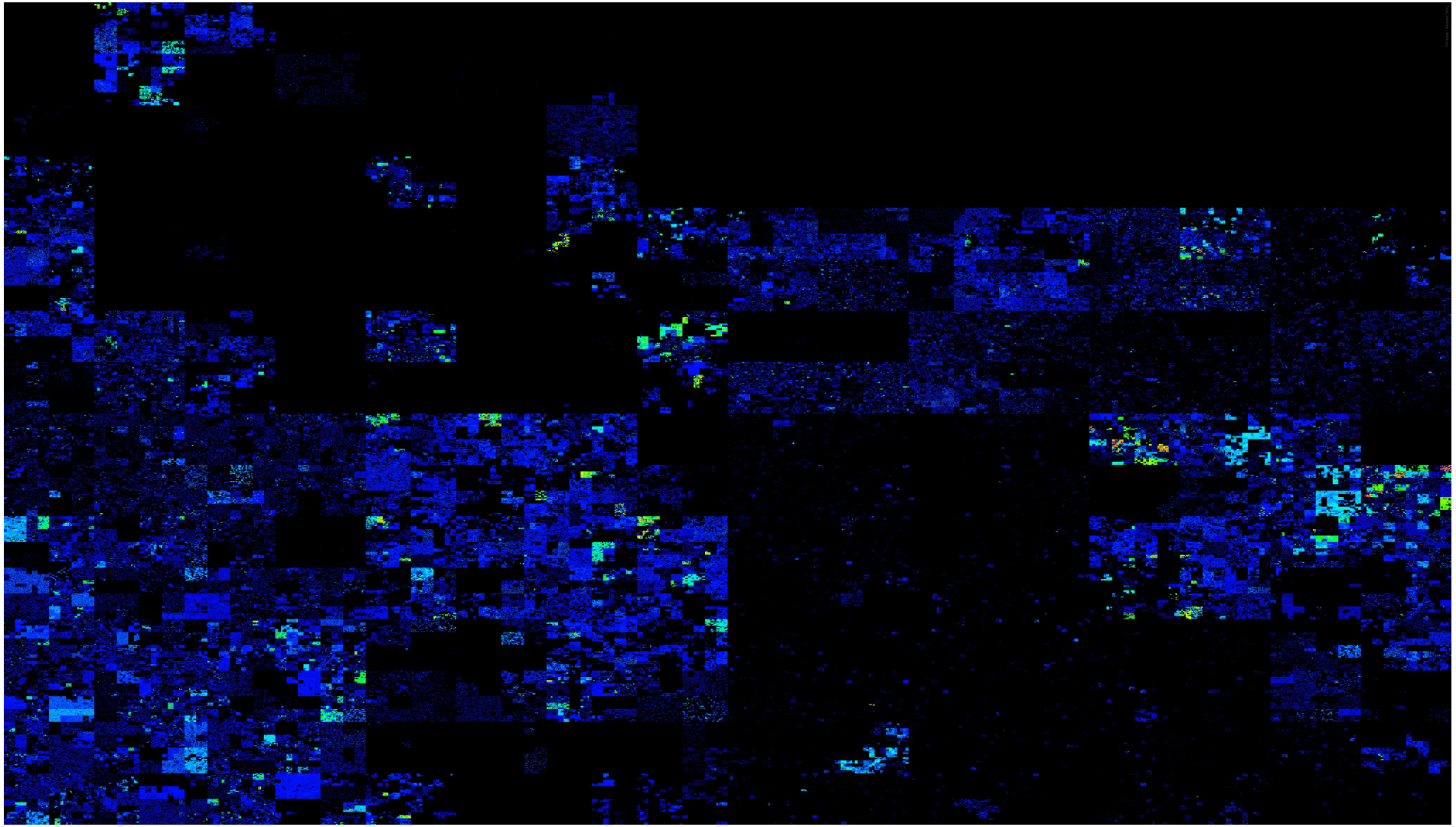
Co situaci ještě zhoršuje?

- **Otevřené resolvery**
- Mnoho dat v DNS

Otevřené resolvery

- Špatně (benevolentně) nakonfigurované
- Zjednodušují situaci pro útočníka
  - Stačí se ptát na jednu známou adresu

Řekni mi zrcadlo...



25 miliónů otevřených resolverů

Kolik potřebujeme na 100 Gbps?

- Amplifikace 100x
  - ~30 bajtů na dotaz
  - ~3000 bajtů na odpověď
- Potřebná kapacita: 1 Gbps
- Počet zapojených resolverů: ~30 000
  - 2,7 Mbps dotazů na resolver

Mnoho dat v DNS

- Útočník musí znát existující domény
- IN ANY
  - Data navíc
- DNSSEC
  - RRSIG
  - DNSKEY
  - Další data navíc

Co s tím?

- Zavírat otevřené resolvery
- Response Rate Limiting
- Vypnout IN ANY (UDP)
- **Ingress filtering (BCP 38)**

Otevřené resolvery

- Zkontrolovat konfiguraci DNS serveru/firewallu
  - **Odpovídat jen na dotazy z vlastní sítě**
  - Nebo alespoň rate-limiting na dotazy zvenčí
- Open Resolver Project
  - Možnost kontroly vlastní sítě
  - http://openresolverproject.org/

Response Rate Limiting

- Odpověď na útoky používající autoritativní servery
- Vidí do DNS paketů, omezuje počet odpovědí
- SLIP
  - Každá n-tá odpověď má +TC (truncate bit)
  - Resolver by měl zkusit dotaz přes TCP
- Podpora: Knot DNS (1.2.0), NSD, BIND 9 (patch)
- Specifikace: http://www.redbarn.org/dns/ratelimits

Vypnutí IN ANY

- IN ANY dotazy by měly být používány pouze pro debug (hanba qmailu…)
- Blokování UDP/ANY dotazů
  - REFUSED (např. UltraDNS)
  - Prázdná odpověď s +TC (truncate)
    - Knot DNS (1.1.0)

Ingress Filtering

- Na směrovačích omezíme zdrojové adresy
  - Ven ze sítě pouštíme pouze adresy vlastní
  - Vše ostatní zahazujeme
- Velmi jednoduché a efektivní řešení
- Bohužel velmi málo používané
- Efekt „to není můj problém“
- **Nejdůležitější!**

Děkuji za pozornost

Ondřej Surý • ondrej.sury@nic.cz