Falšování DNS s RPZ i bez

Ondřej Caletka

7. února 2017

Paul Vixie

- člen Síně slávy Internetu
- autor nejpoužívanějšího DNS serveru BIND
- zakladatel ISC, Farsight Security
- autor různých DNS rozšíření (DDNS, RRL,...)
- autor myšlenky DNS blacklistů
- autor návrhu **Response Policy Zones**

Vraťte mi zpátky DNS

- domény jsou příliš levné
- velká část doménových jmen neslouží dobré věci
  - spamming, phishing, šíření malware
  - C&C adresy botnetů
  - algoritmicky generované adresy (DGA)
- váš vlastní DNS server se účastní nekalé činnosti
  - pomáhá botnetům předávat zprávy
  - komplikuje dohledatelnost

Paul Vixie: Taking back the DNS

Response Policy Zone

- funkce také nazývána DNS firewall
- probíhá standardizace v IETF
- princip obdobný DNS blacklistům
- obsah zóny je rekurzivním serverem konzultován při každém dotazu
- není-li nic nalezeno, pokračuje rekurze normálně
- při nalezení shody je další zpracování řízeno typem záznamu v RPZ
- zóna musí být lokálně dostupná rekurzivnímu resolveru

Příklad zóny RPZ

```
$ORIGIN RPZ.EXAMPLE.ORG.
@     SOA   ns.example.org admin.example org 1 27700 7200…
      NS    localhost.

1.example.com         CNAME   .  ; return NXDOMAIN
*.1.example.com       CNAME   .  ; return NXDOMAIN

2.example.com         CNAME   *.  ; return NODATA

3.example.com         CNAME   rpz-drop. ; drop the query

4.example.com         CNAME   catchall.example.org. ;redirect
```

Akce RPZ

NXDOMAIN `CNAME .`
NODATA `CNAME *.`
DROP `CNAME rpz-drop.`
TCP-only `CNAME rpz-tcp-only.`
Passthru `CNAME rpz-passthru.`
Local data ostatní záznamy
Wildcard CNAME `CNAME *.<target domain>`

- přeloží se jako `CNAME <původní dotaz>.<target>`

Spouště (levé strany) RPZ

QNAME <dotazované doménové jméno>
Client IP <mask>.<B4>.<B3>.<B2>.<B1>.rpz-client-ip
Response IP <mask>.<B4>.<B3>.<B2>.<B1>.rpz-ip
NSDNAME <jméno NS serveru>.rpz-nsdname
NSIP <IP adresa NS serveru>.rpz-nsip

- IP adresy se spolu s maskou zapisují převráceně, podobně jako u reverzních DNS záznamů: <B1>.<B2>.<B3>.<B4>/<mask>
- spouště mají definované priority

Příklad konfigurace RPZ v BIND

```
options {
    …
    response-policy {
        zone "rpz.ten.cz";
    };
};

zone "rpz.ten.cz" {
    type slave;
    masters { 2001:718:1:101::144:228; };
};
```

Co se může pokazit

- RPZ se standardně uplatňuje pouze pro dotazy s RD=1, tedy od klientů požadujících rekurzivní zpracování
- RPZ se nepoužije, pokud klient vyžádá DNSSEC data pomocí DO=1
  - má se za to, že pokud o ně žádá, pak je i ověřuje
  - některé implementace při nevalidních datech rapidně opakují dotazy

Jak zajistit autenticitu RPZ zóny?

- DNSSEC se nedá použít pro AXFR
- TSIG používá sdílené tajemství, nevhodné pro veřejnou službu

CESNET

Podpora v alternativních resolverech

Unbound

- je plánována (leden 2016); zatím není
- podpora konfiguračních voleb `local-data:`
- konfiguraci lze generovat z RPZ zóny regulárním výrazem

Knot DNS resolver

- částečná podpora implementována
- vyžaduje určitý formát zónového souboru
- problematická aktualizace zóny

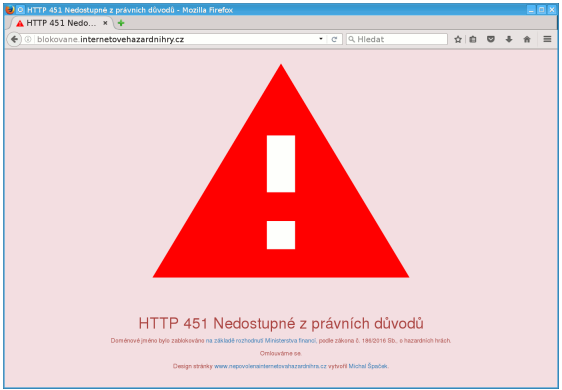
RPZ policy for unbound – transform RPZ zone into local zone statements

Jak správně blokovat

- pozor na správnou interpretaci `NODATA` vs. `NXDOMAIN`
  - `NXDOMAIN` **znamená neexistenci jakékoli subdomény**
- wildcard na pravé straně (`CNAME *.target.`) umožní zjistit konkrétní blokované jméno logováním dotazů
  - zejména při blokování podle jiného kritéria
  - má význam jen při současném logování DNS dotazů
  - nemá vliv např. na HTTP hlavičky
- webserver, na který je přesměrováno, musí reagovat shodně na libovolnou URL
  - pro zákonné blokování ideálně vracet `HTTP 451 Nedostupné z právních důvodů`

Testovací prostředí rpz.ten.cz

- veřejně dostupný testovací blacklist
- přesměrovává závadný obsah na `*.poker.cesnet.cz`
- zatím jediná testovací doména:
  `blokovane.internetovehazardnihry.cz`



Shrnutí

- mocná technologie s ohromnými možnostmi
- efektivně eliminuje i např. botnety, které používají každý den jiné doménové jméno
- snadná konfigurace v BIND
- obtížná podpora alternativních resolverů
- nedostupnost důvěryhodných veřejných RPZ blacklistů

Děkuji za pozornost

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

Prezentace je již nyní k dispozici ke stažení.