# Novinky v DNS

Ondřej Caletka


11. února 2015

# Obsah

# Root DNSSEC KSK rollover

- Podpis kořenové zóny před pěti lety – 15. 7. 2010
- Rolování kořenového klíče podle potřeby, nebo jednou za pět let
- Vyžaduje aktualizaci *trust anchor* ve všech validátorech
- Proběhne automaticky ve většině případů (RFC 5011)
- Testovací prostředí na `http://keyroll.systems/`
- Podrobnosti rolování zatím nejsou stanoveny

# Dynamické IPv6 záznamy

- běžná praxe v IPv4 spočívá ve vygenerování všech možných DNS záznamů
- pro IPv6 nemožné, soubor pro jednu podsíť /64 by zabíral stovky EiB ($2^{60}$)
- řešením je dynamické generování, podporované v Knot DNS 1.5+

## Příklad

```
example.cz {
    file "/etc/knot/empty.zone";
    query_module {
        synth_record "forward dyn- 60 2001:db8:1::/64";
        synth_record "forward dyn- 60 192.0.2.0/24";
    }
}
```

# DNS Water Torture – princip

- Nová forma útoku, zneužívající otevřené rekurzivní resolvery
- Pro rekurzivní resolver připomíná Slowloris útok
- Postihuje zároveň rekurzivní i autoritativní servery
- Útočící botnet pokládá dotazy ve stylu `<random string>.www.obet.com`
- Dotaz je vždy přeposlán autoritativnímu serveru
- Autoritativní server se buď pod náporem zhroutí, nebo zasáhne rate limiting
- Rekurzivní server čeká na odpověď a zkouší dotazy opakovat

https://www.nanog.org/sites/default/files/nanog63-dnstrack-winstead-attacks.pdf

CESNET

# DNS Water Torture – důsledky a obrana

## Důsledky

- Zahlcení serverů dotazy
- DoS rekurzivních resolverů, např. BIND:
  - maximum 1000 současně probíhajících rekurzí
  - každá rekurze používá jeden file descriptor
  - pro víc než ~4000 rekurzí přestává být spolehlivý

## Obrana

- Definování prázdných SLD zón obětí na rekurzoru
  - a. k. a. cenzura DNS
  - riziko zablokování významných domén jako `in-addr.arpa`, nebo `co.uk`
- Použít unbound s výkonovými optimalizacemi

# Passive DNS

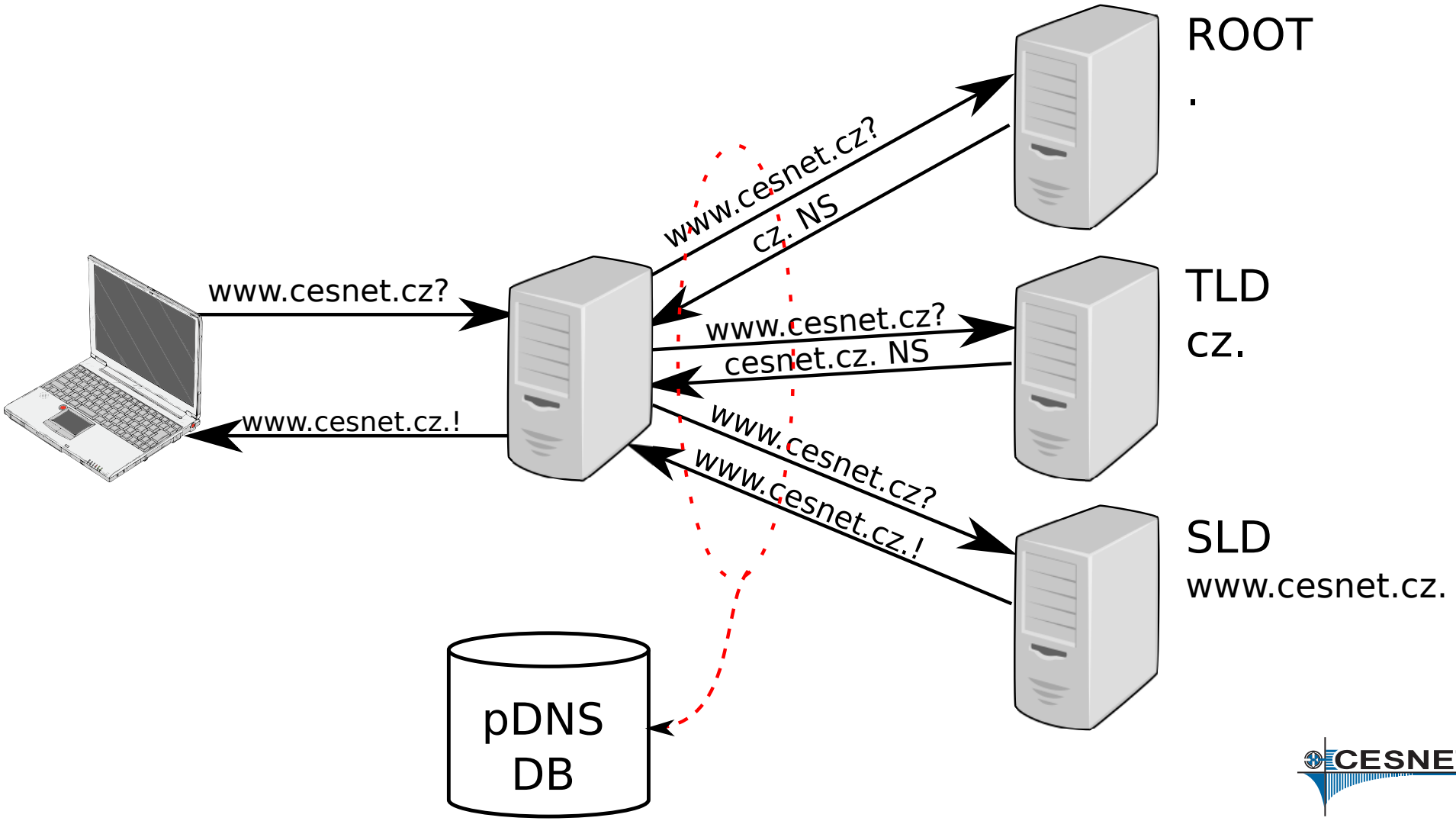
# Myšlenka passive DNS

- Sbírat veřejná DNS data na rekurzivních DNS serverech
- Zjišťovat, na co se lidé ptají
- Nezjišťovat, kdo se ptá (ochrana soukromí)
- Ukládat do databáze spolu s časovou značkou
- Získat tak informace o **historii DNS dat**
- Mít možnost pokládat **inverzní DNS dotazy**

# Dva přístupy k passive DNS

1. Zachytávání před rekurzivním serverem
   - zaznamenávání každé uživatelské aktivity
   - přesné sledování četnosti dotazů
2. Zachytávání za rekurzivním serverem
   - menší objem dat díky cache
   - implicitní ochrana soukromí

# Passive DNS za rekurzivním serverem

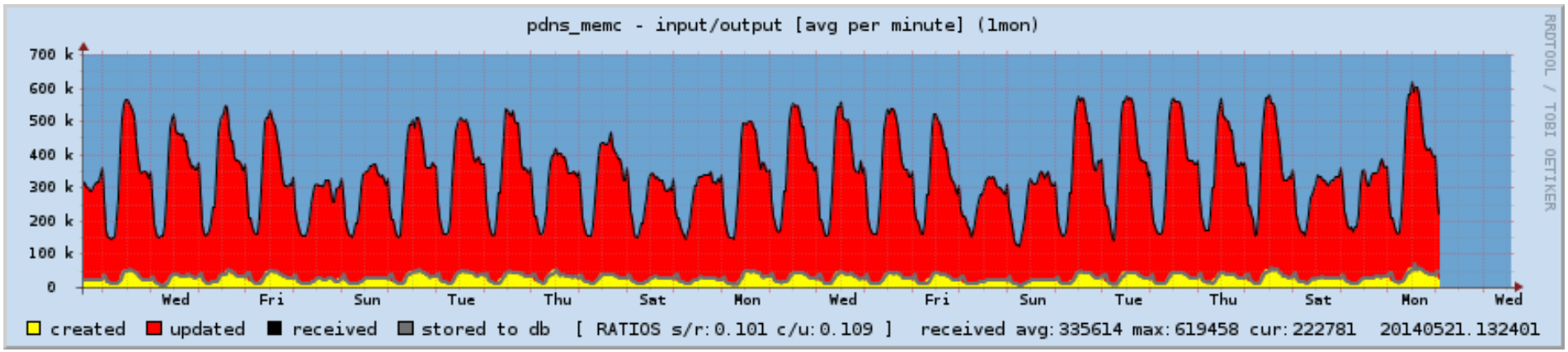


# Technické provedení

- Senzor sbírá DNS provoz pomocí PCAP knihovny v blízkosti DNS serveru
- Je možné jej buď spustit na stejném stroji jako DNS server, nebo klonovat data switchi
- Data se zapisují do binárních souborů po minutách
- Soubory jsou posílány pomocí SCP do databáze

# Databáze pDNS

1. ISC/Farsight DNSDB.info
2. BFK
3. CERT.at
   - založeno na PosgreSQL
   - miliarda položek v databázi
   - 100 GB RAM, data na SSD discích



# Webové rozhraní pDNS@CERT.at

**CERT.at / ACOnet**
**DNS History**

www.google.at | Go | Reset [X]

Format: Whois csv HTML
Options: Sensor info Exact domain
List only: NXDOMAIN A NS CNAME SOA PTR MX TXT AAAA
First seen: >= <=
Last seen: >= <=
Sort: desc , desc , desc

```
% CERT.at / ACOnet DNS replicator WHOIS server, version 2.0.
% (C) 2011 All rights reserved.
% Authors: L. Aaron Kaplan <kaplan AT cert.at>
%          Achim Adam      <achim.adam AT univie.ac.at>
%
% 419 elements, 0.1437s
```

| LEFT | RTYPE | RIGHT | FIRST-SEEN | LAST-SEEN | COUNT-SEEN |
|---|---|---|---|---|---|
| www.google.at | A | 74.125.232.223 | 2012-09-21 06:05:39 | 2012-09-21 06:05:39 | 48 |
| www.google.at | A | 74.125.232.215 | 2012-09-21 06:05:39 | 2012-09-21 06:05:39 | 48 |
| www.google.at | A | 74.125.232.216 | 2012-09-21 06:05:39 | 2012-09-21 06:05:39 | 48 |
| www.google.at | A | 74.125.232.248 | 2012-09-21 12:39:39 | 2012-09-21 12:39:39 | 349 |
| www.google.at | A | 74.125.232.247 | 2012-09-21 12:39:39 | 2012-09-21 12:39:39 | 349 |
| www.google.at | A | 209.85.148.94 | 2012-09-11 17:27:31 | 2012-09-27 11:11:29 | 5 |
| www.google.at | A | 74.125.135.94 | 2012-09-10 13:06:35 | 2012-10-17 18:16:55 | 5 |
| www.google.at | A | 74.125.232.56 | 2012-11-22 18:40:04 | 2012-11-22 18:40:04 | 2 |
| www.google.at | A | 74.125.232.55 | 2012-11-22 18:40:04 | 2012-11-22 18:40:04 | 2 |
| www.google.at | A | 74.125.232.63 | 2012-11-22 18:40:04 | 2012-11-22 18:40:04 | 2 |
| www.google.at | A | 74.125.227.56 | 2012-11-22 18:40:31 | 2012-11-22 18:40:31 | 1 |
| www.google.at | A | 74.125.227.63 | 2012-11-22 18:40:31 | 2012-11-22 18:40:31 | 1 |
| www.google.at | A | 74.125.227.55 | 2012-11-22 18:40:31 | 2012-11-22 18:40:31 | 1 |
| www.google.at | A | 74.125.129.94 | 2012-11-22 18:40:36 | 2012-11-22 18:40:36 | 1 |
| www.google.at | A | 74.125.224.120 | 2012-11-22 18:40:41 | 2012-11-22 18:40:41 | 1 |
| www.google.at | A | 74.125.224.119 | 2012-11-22 18:40:41 | 2012-11-22 18:40:41 | 1 |
| www.google.at | A | 74.125.224.127 | 2012-11-22 18:40:41 | 2012-11-22 18:40:41 | 1 |
| www.google.at | A | 74.125.230.215 | 2012-10-23 08:26:04 | 2012-11-28 11:41:30 | 3 |
| www.google.at | A | 74.125.230.216 | 2012-10-23 08:26:04 | 2012-11-28 11:41:30 | 3 |
| www.google.at | A | 74.125.230.223 | 2012-10-23 08:26:04 | 2012-11-28 11:41:30 | 3 |

CESNET

# Příklady použití

- Odhalení řídicích serverů botnetů, ve spolupráci s NetFlow také odhalení infikovaných stanic
- Odpověď na otázky:
  - jde o zneužití legitimní služby, nebo o cílený hosting škodlivého obsahu?
  - jaké další weby jsou hostovány na stejné IP adrese?
- Kontrola neoprávněného využití adresního prostoru (například sítě CESNET2)
- Výzkum nad globálními DNS daty
  - které domény jsou hostovány pouze na území jednoho státu?
  - jak často se mění data v různých doménách?

# Přístup k databázi

- Přístup k pDNS databázi CERT.at je omezen pro:
  - výzkumníky
  - CERT/CSIRT komunitu
  - provozovatele senzorů
- Existuje návrh standardního formátu pro snadnou kombinaci dat z různých Passive DNS systémů
- Zapojení dalších českých ISP je vítáno
- ☞ Kontaktujte L. A. Kaplana – `kaplan@cert.at`

# DNSSEC jako bezpečné uložiště

# Problém důvěryhodnosti PKI modelu

- Mnoho *důvěryhodných* certifikačních autorit
- Různé úrovně ověření, stejný cílový efekt
  - Důkladné ověření (Extended Validation, €€€)
  - Základní oveření (Organization Validation, €€)
  - Bez ověřování identity (Domain control Validation, €)
- Kterákoli autorita může vydat certifikát pro jakékoli jméno
- Na druhou stranu
  - Nízký počet vydaných falešných certifikátů
  - Velmi účinné útoky bez nutnosti falešných certifikátů (phishing, rom-0,…)

# Certificate pinning s DANE

- Možnost určit, který certifikát má být pro dané jméno platný
- Vyžaduje DNSSEC
- Čtyři typy použití (Usage) TLSA záznamu
  - 0 kontrola certifikační autority
  - 1 kontrola koncové entity
  - 2 vložení certifikační autority
  - 3 vložení koncové entity

## Příklad TLSA záznamu

```
_443._tcp.www IN TLSA 0 0 1 5C4…6099
```

CESNET

# DANE jako zvýšení zabezpečení PKIX

- Omezení množiny povolených certifikačních autorit (`Usage: 0`), nebo certifikátů (`Usage: 1`)
- Vynucení certifikační autority s přísnou politikou
- PKIX validace je stále nutná

*Tip:* Umístěte do DNS otisk certifikátu své nejbližší autority. Tu pak pomocí CNAME odkazujte ze všech svých služeb.

```
terenasslca2 IN TLSA 0 0 1 2FF183…BE43
_443._tcp.www  IN CNAME terenasslca2
_443._tcp.www2 IN CNAME terenasslca2
_143._tcp.imap IN CNAME terenasslca2
```

# DANE jako alternativa k PKIX

- Vynucení konkrétní autority (Usage: 2), nebo certifikátu (Usage: 3), bez vazby na PKI
- Možnost ušetřit za DV certifikáty
- V režimu vkládání nové autority je nutné, aby server kořenový certifikát posílal během hanshake
- Zatím spíše nepoužitelné, málo validujících klientů

# DANE pro bezpečné předávání pošty

- PKIX neumožňuje šifrované předávání pošty
  - Často nevalidní certifikát
  - Nezabezpečená vazba doména $\rightarrow$ MX záznam
  - Není k dispozici uživatel, který by odsouhlasil varování
- DNSSEC a DANE dokáží bezpečnost vynutit
  - Bezpečená vazba doména $\rightarrow$ MX záznam
  - Otisk certifikátu v DNS, nezávislost na PKI
  - Zpětně kompatibilní bez možnosti downgrade útoků
    - Bez TLSA: oportunistické šifrování bez kontroly
    - S TLSA: šifrování vynuceno
    - Selhání DNSSEC: zpráva odložena
- Podporováno v Postfixu od verze 2.11
- Problémy pouze při použití `djbdns` a wildcard záznamů s DNSSEC

# Generování TLSA záznamů

- CLI utilitka swede, popř. webové generátory
- Usage zvolte 0-3 podle zamýšleného účelu
- Selector zvolte 0 pro otisk celého certifikátu
- Mtype zvolte 1 pro SHA-256 otisk
- Otestujte pomocí swede a gnutls-cli

```
$ gnutls-cli --dane www.cesnet.cz
…
- Status: The certificate is trusted.
- DANE: Certificate matches.
```

# Validace TLSA záznamů

- Rozšíření od CZ.NIC pro prohlížeče
- Neovlivňuje chování prohlížeče, neumí nahradit PKIX
- Odhalí sítě, které rozbíjejí DNSSEC

# SSHFP záznamy pro bezpečné SSH

- SSH standardně vede seznam známých serverů
- DNS záznam typu SSHFP umožňnuje ukládat otisky serverových klíčů do DNS
- Validující klient pak ověří identitu serveru automaticky

## Vytvoření záznamu

```
$ ssh-keygen -r server.example.com
```

## Zapnutí validace

```
$ echo 'VerifyHostKeyDNS yes' >> ~/.ssh/config
```

http://www.root.cz/clanky/dnssec-jako-bezpecne-uloziste-ssh-klicu/

CESNET

# Závěr

Děkuji za pozornost

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