# PassiveDNS

Radko Krkoš, krkos@cesnet.cz
Andrea Kropáčová, andrea@cesnet.cz
CESNET, z. s. p. o.

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI
2007–13
OP Výzkum a vývoj pro inovace

# PassiveDNS

- sběr veřejných DNS data na rekurzivních DNS serverech
- zjišťuje se na co se lidé ptají
- nezjišťuje se, kdo se ptá (ochrana soukromí)
- záznamy se ukládají do databáze spolu s časovou značkou

- vytváření „historie DNS dat“
- možnost pokládat dotazy

# 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 |

# Stav

- Spolupráce s CERT.AT
- Export dat z ns.ces.net a ns.cesnet.cz (adns1 a adns2) do kolektoru provozovaného CERT.AT
- Dotazovací rozhraní
  - GUI (o přístupu rozhoduje CERT.AT)
  - Whois
- Aktuální využití dat
  - Při procesu incident handling (CESNET-CERTS)
  - Dohledávání historie změny DNS záznamů
  - Dohledávání zrušených záznamů

# Cíle

- Vlastní kolektor dat, vlastní server
- Export dat ze síťových sond a DNS serverů
- Služba
- Vlastní dotazovací rozhraní
  - více otevřené – členům CERT/CSIRT, správcům, bezpečnostním složkám
  - s rozšířenou funkcionalitou
- Zdroj dat a informací pro
  - správce, bezpečáky
  - automatizovaně pro systémy
  - pro další výzkum (např. vliv regionu na DNS historii)

# Plán

- Listopad 2016
  - Formát vstupních dat
  - Implementace rozhraní mezi DNS a kolektorem
  - Testování nové verze pro CERT.AT
- Prosinec 2016
  - Instalace vlastního serveru
- Leden/únor 2017
  - SW od CERT.AT
  - Vlastní vývoj?
- Do konce roku 2017
  - První verze GUI nad vlastním systémem a daty?

# Služby

- Služba umožňující vyhledávání
  - GUI
  - whois
- Zdroj dat pro ostatní systémy
  - Sondy, NERD, Warden, Mentat
- „DNS Monitor“
  - Dlouhodobé sledování vybraných entit s následnou notifikací v případě změny
  - Periodické sledování vzniku určitého jména v doméně (vznik záznamu)
  - Pokročilé analýzy

# Sondy

- Na perimetru sítě CESNET2
- IPFIXCol
  - Nový modul pro DNS data (do NEMEA)
- Update firmware v sondách

- Předpokládané problémy k řešení:
  - Detekce neplatných transakcí
  - Skladování neautoritativních odpovědí?
  - Podvrhnuté odpovědi

# Diskuse

- Další funkcionality a služby
  - požadavky na GUI?
  - ???
- Musíme zvážit jaké informace předávat do
  - Warden?
  - Mentat?
  - NERD?
  - PROKI?
  - Co může být zajímavé pro správce?

Děkuji za pozornost.