cesnet

CESNET PassiveDNS: Ako byť archeológom a bezpečnostným analytikom naraz?

Radko Krkoš
CESNET

LinuxDays 2019
Praha

Domain Name System

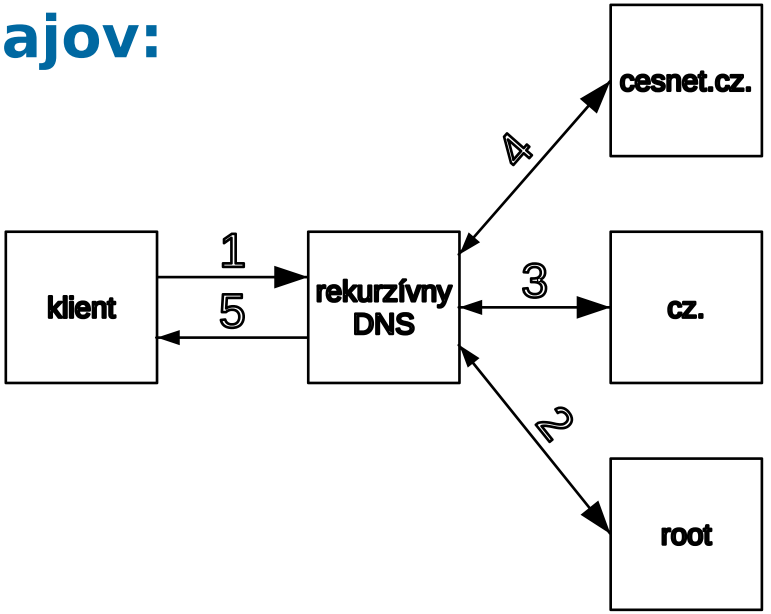
- Decentralizovaný hierarchický systém pre preklad mien,
- Typy záznamov (record types):
  - A / AAAA – meno na IPv4 / IPv6 adresu
  - PTR – reverzný záznam (adresa na meno: in-addr.arpa, ip6.arpa),
  - CNAME, DNAME,
  - MX, NS,
  - ďalšie: TXT, niekoľko ohľadom DNSSEC...

Získanie prekladovej dvojice:

- nslookup
- dig

```
bash-4.3$ dig cesnet.cz

; <<>> DiG 9.11.9 <<>> cesnet.cz
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23222
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;cesnet.cz.                     IN      A

;; ANSWER SECTION:
cesnet.cz.              0       IN      A       195.113.144.230

;; Query time: 4 msec
;; SERVER: 195.113.144.194#53(195.113.144.194)
;; WHEN: Sat Oct 05 08:58:40 CEST 2019
;; MSG SIZE  rcvd: 54
```

- **Ukladanie histórie DNS,**
- **Snímok stavu v nejakom čase (intervale) v minulosti,**
- **Analytika nad časovou radou údajov:**
  - Objemná báza dát,
  - Prúdové spracovanie.



CESNET PassiveDNS

- **Riešenie vyvinuté na mieru potrebám CESNETu,**
- **Poskytované ako služba pre:**
  - Bezpečnostné aplikácie (Mentat, NERD – reputačná databáza),
  - Projekty bezpečnostného výskumu,
  - Komunitu,
- **Technológie:**
  - PostgreSQL, Python, Flask, Apache.
  - dpkt, dnslib.

Search Match Analytics REST API Logout

PassiveDNS Search

Query:
2001:718:1:101::4
Query type: (•) IP ( ) domain

Date limit:
Since: mm / dd / yyyy
Until: mm / dd / yyyy

Search

Elapsed time: 0.008925s

Page 1

IP	Domain	RTYPE	First seen	Last seen	Count	Source
2001:718:1:101::4	cesnet.cz	AAAA	2019-07-15 16:11:16.296404	2019-10-05 07:22:59.108922	962	ns.ces.net
2001:718:1:101::4	www.cesnet.cz	AAAA	2019-07-15 16:00:02.477826	2019-10-05 07:10:02.566047	1279	ns.ces.net
2001:718:1:101::4	25let-internetu.cz	AAAA	2019-09-06 10:18:46.502550	2019-09-06 10:18:46.502550	1	adns1.cesnet.cz
2001:718:1:101::4	cesnet.cz	AAAA	2019-07-15 21:10:20.583655	2019-10-05 08:06:30.476706	722	adns1.cesnet.cz
2001:718:1:101::4	e-infra.cz	AAAA	2019-09-10 11:32:54.816126	2019-09-10 11:32:54.816126	1	adns1.cesnet.cz
2001:718:1:101::4	vyzkumne-infrastruktury.cz	AAAA	2019-08-27 10:08:30.895255	2019-08-27 10:08:30.895255	1	adns1.cesnet.cz
2001:718:1:101::4	vyzkumneinfrastruktury.cz	AAAA	2019-09-06 09:15:36.271939	2019-09-06 09:15:36.271939	1	adns1.cesnet.cz
2001:718:1:101::4	www.cesnet.cz	AAAA	2019-07-15 16:30:30.578538	2019-10-05 08:41:20.409157	1399	adns1.cesnet.cz
2001:718:1:101::4	cesnet.cz	AAAA	2019-07-15 16:01:59.404677	2019-10-05 03:00:09.445737	327	adns2.cesnet.cz
2001:718:1:101::4	www.cesnet.cz	AAAA	2019-07-15 15:56:06.326259	2019-10-05 07:09:17.931027	1112	adns2.cesnet.cz

Previous page Next page

Prístup k službe

- **Česká akademická federácia identít eduID.cz**
  - Členovia (poskytovatelia identít): https://www.eduid.cz/cs/members
    - Ústavy AV ČR, vysoké školy a univerzity, verejné knižnice, nemocnice,
  - eduID.cz Hostel,
  - CZ.NIC mojeID.

cesnet eduid.cz

- **URL:**

  https://passivedns.cesnet.cz/api/v1/

  - /ip/<ip>[/<prefix>]
  - /domain/<domain>
  - /match?ip=<ip>&domain=<domain>
- **Filtrovanie podľa času:**
  - since,until=2019-01-01T10:00:00.123456
- **Prístupový token.**

https://passivedns.cesnet.cz/api/v1/ip/195.113.144.0/24?since=2019-10-06T12:00:00&token=eliska1234

Analytické dotazy

- **S existujúcim bezpečnostným využitím:**
  - Adresy s najväčším počtom rôznych záznamov.
  - Dvojice vyskytujúce sa v najviac DNS transakciách (najčastejšie prekladané).
- **Ďalšie podľa potreby:**
  - Vzniknú z výskumu,
  - Vzniknú z potrieb bezpečnostných analýz,
  - Vyžiadanie používateľom,

Zdroje dát

- **Rekurzívne DNS servery CESNETu:**
  - ns.ces.net: 8%
  - adns1.cesnet.cz: 90%
  - adns2.cesnet.cz: 2%
- **7 miliárd záznamov o DNS transakciách**
  - Pribúda asi 80 miliónov denne.
- **Pripravujeme: Sondy na perimetri siete CESNET2**
  - Sekundárne dáta.

cesnet

REKLAMNÁ PRESTÁVKA

- Alebo čo dodalo Oddělení komunikace

cesnet

THE CATCH

V rámci Evropského měsíce kybernetické bezpečnosti – spouštíme v říjnu další ročník hackerské soutěže The Catch – chcete se zúčastnit?

Začínáme 7.10.2019 ve 14.00 hodin

www.thecatch.cz

Potřebujete se rozcvičit? Přijďte k nám na CESNET stánek, kde pro Vás máme připravené The Catch Nano a můžete vyhrát třeba mikinu.

CESNET eNews

- Chcete se o akcích a novinkách ze sdružení CESNET dozvědět mezi prvními?

  Přihlaste se do našeho CESNET eNews – neposíláme ho příliš často.

  https://www.cesnet.cz/sdruzeni/zpravy/enews/

- **Hledáme nové posily do týmů:**

  Vývojář systémů pro sledování provozu a bezpečnosti sítě

  Vývojář cloudové platformy pro rozsáhlé vědecké výpočty

  Pracovník pro správu Linuxových systémů

- Také nás můžete sledovat na našem webu a sociálních sítích

@cesnet_news

cesnet

Ďakujem za pozornosť

Radko Krkoš
krkos@cesnet.cz