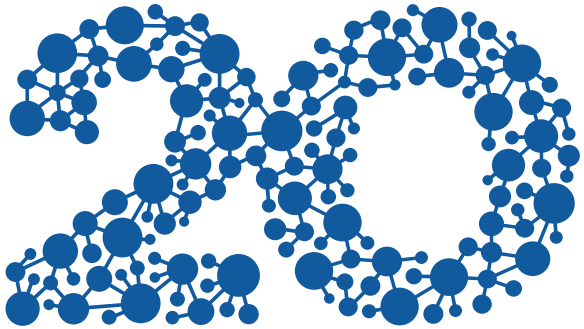
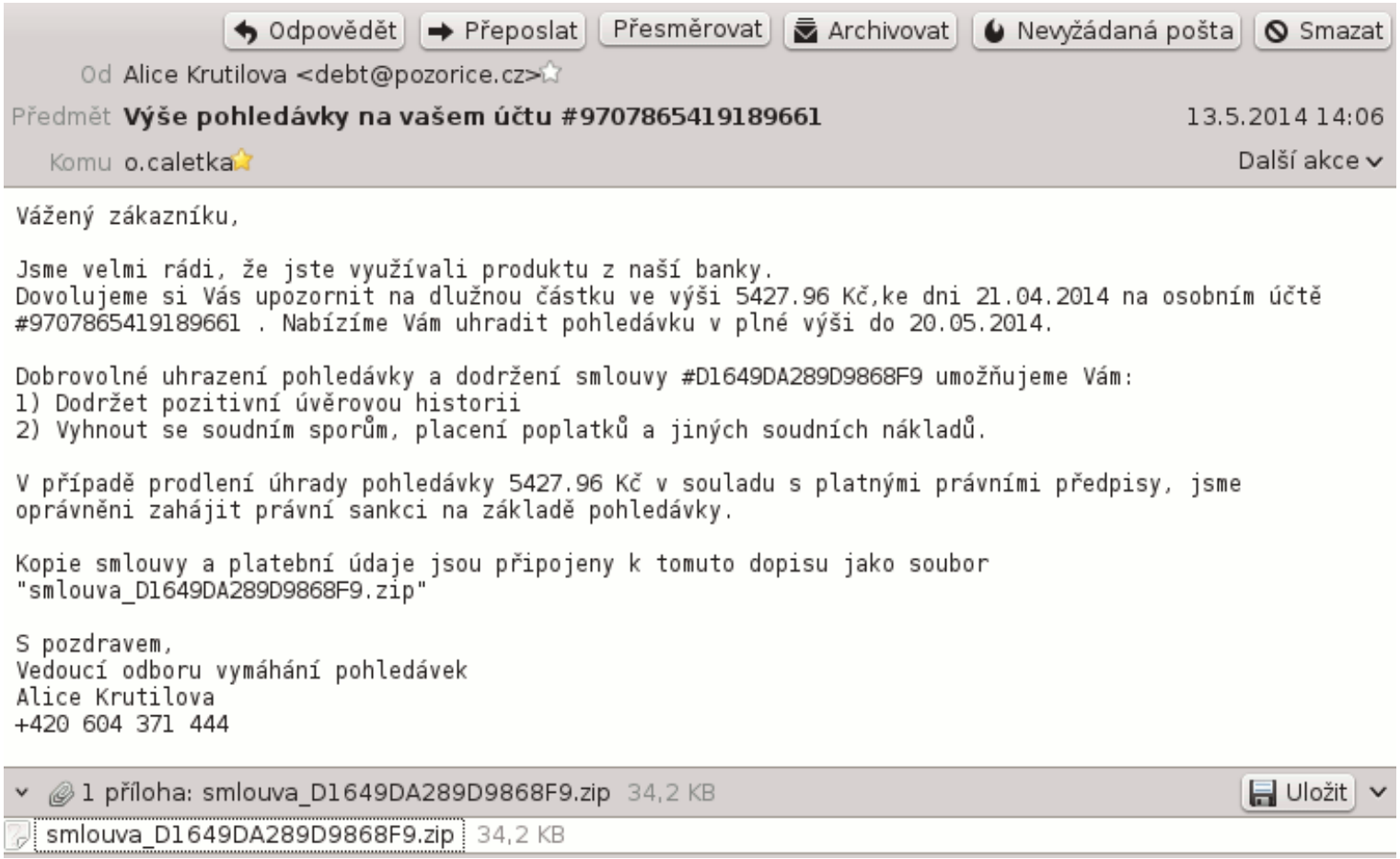
Passive DNS

Ondřej Caletka



11. října 2016



Odpovědět | Přeposlat | Přesměrovat | Archivovat | Nevyžádaná pošta | Smazat

Od Alice Krutilova <debt@pozorice.cz>

Předmět **Výše pohledávky na vašem účtu #9707865419189661** 13.5.2014 14:06

Komu o.caletka Další akce

Vážený zákazníku,

Jsme velmi rádi, že jste využívali produktu z naší banky.
Dovolujeme si Vás upozornit na dlužnou částku ve výši 5427.96 Kč,ke dni 21.04.2014 na osobním účtě
#9707865419189661 . Nabízíme Vám uhradit pohledávku v plné výši do 20.05.2014.

Dobrovolné uhrazení pohledávky a dodržení smlouvy #D1649DA289D9868F9 umožňujeme Vám:
1) Dodržet pozitivní úvěrovou historii
2) Vyhnout se soudním sporům, placení poplatků a jiných soudních nákladů.

V případě prodlení úhrady pohledávky 5427.96 Kč v souladu s platnými právními předpisy, jsme
oprávněni zahájit právní sankci na základě pohledávky.

Kopie smlouvy a platební údaje jsou připojeny k tomuto dopisu jako soubor
"smlouva_D1649DA289D9868F9.zip"

S pozdravem,
Vedoucí odboru vymáhání pohledávek
Alice Krutilova
+420 604 371 444

1 příloha: smlouva_D1649DA289D9868F9.zip 34,2 KB Uložit

smlouva_D1649DA289D9868F9.zip 34,2 KB

1996–2016 CESNET

LAB Forenzní laboratoř

1996–2016 CESNET

Výsledky forenzní analýzy

- jedná se o node botnetu
- komunikuje s řídicím serverem pomocí adresy `picapicachu.net`

`$ dig picapicachu.net`

```
; <<>> DiG 9.9.4 <<>> picapicachu.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 11631
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;picapicachu.net.               IN      A
```

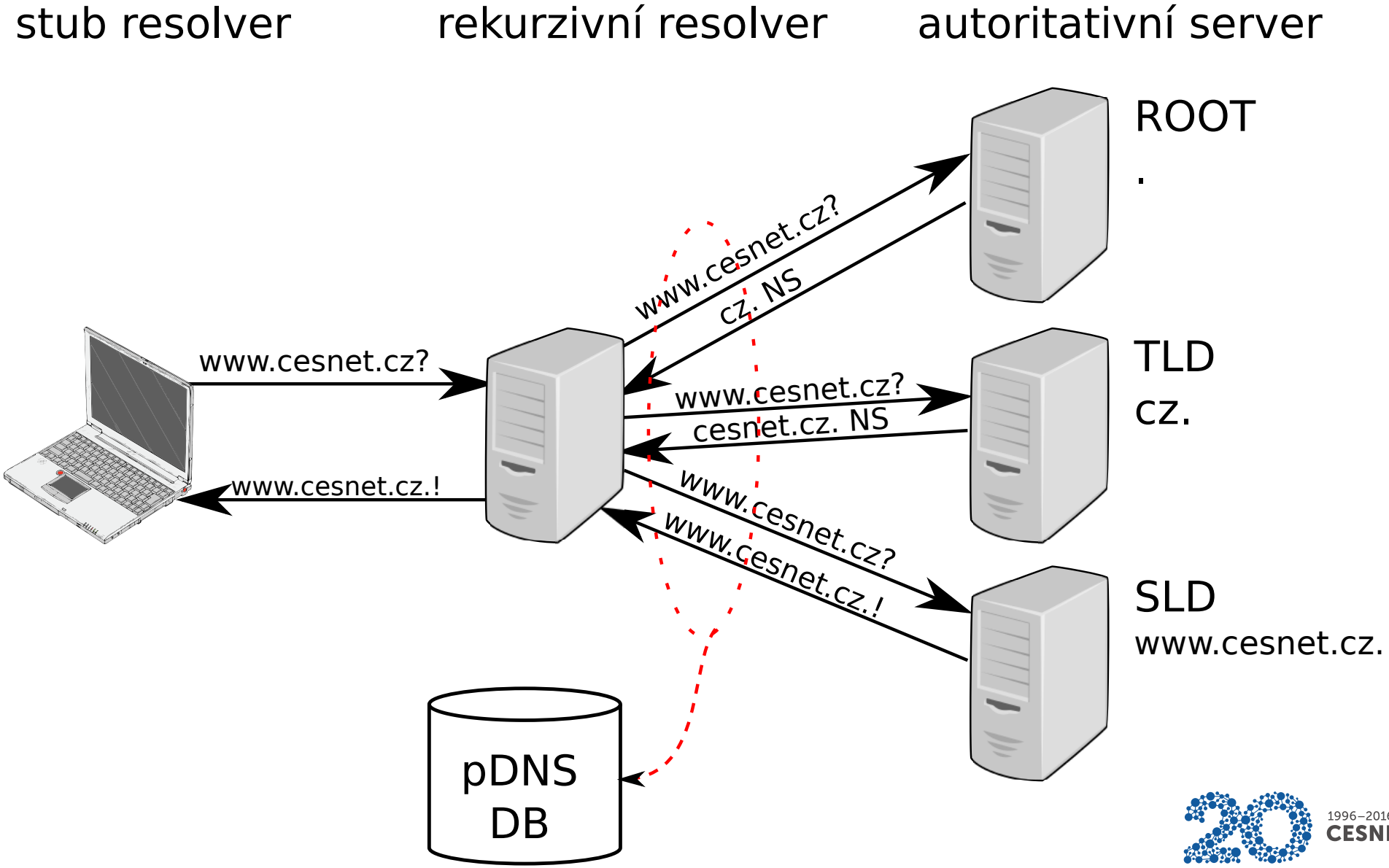
Myšlenka passive DNS

- 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 (NMSG) souborů po minutách
- soubory jsou posílány pomocí SCP do databáze

Technické provedení

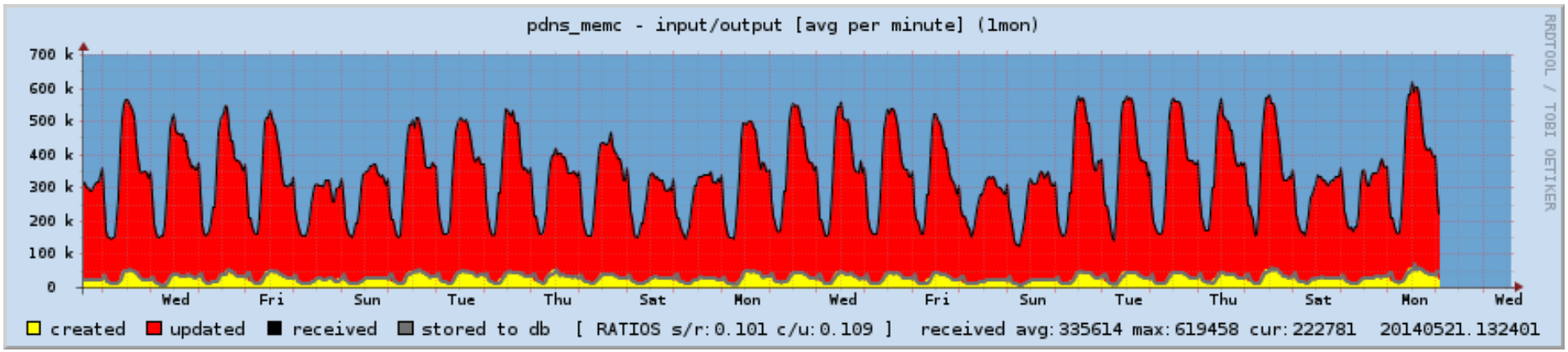
- starý software, vyvinutý kolem 2005
- původně ISC, následně odštěpeno do Farsight security
- málo udržované, slabá dokumentace

Nové rozhraní DNSTAP

- standardizovaná forma binárních DNS logů
- podpora v Unbound a Knot DNS
- eliminuje dvojí parsování DNS zpráv

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



1996–2016 CESNET

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

1996–2016 CESNET

Příklady použití

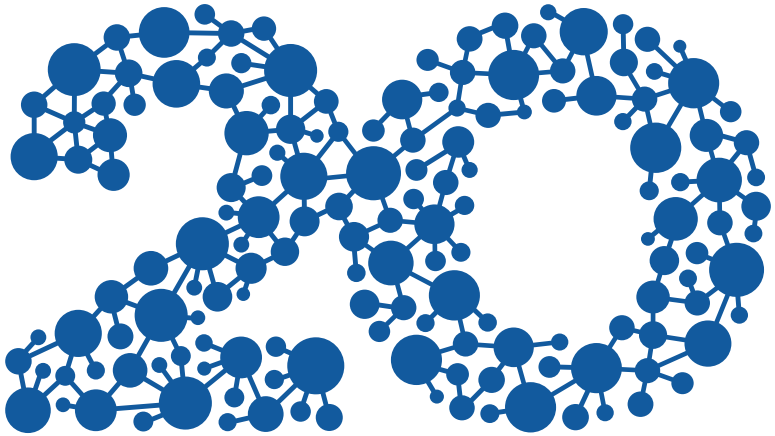
- odhalení řídicích serverů botnetů, ve spolupráci s NetFlow také odhalení infikovaných stanic
- odpověď na otázky:
  - jde o zneužití legitimní služby, nebo o cílený hosting škodlivého obsahu?
  - jaké další weby jsou hostovány na stejné IP adrese?
- kontrola neoprávněného využití adresního prostoru (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?

Získání přístupu

- 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

Děkuji za pozornost

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



1996–2016
CESNET
SPOLUPRÁCE
VÝZKUM
KOMUNITA