

DNS intelligence: czas życia nowych domen

Paweł Foremski

*Senior Distributed Systems Engineer
Farsight Security, Inc.*

www.farsightsecurity.com



PLNOG 21
Kraków, 1-2 X 2018



Agenda

Wstęp - “DNS intelligence”:

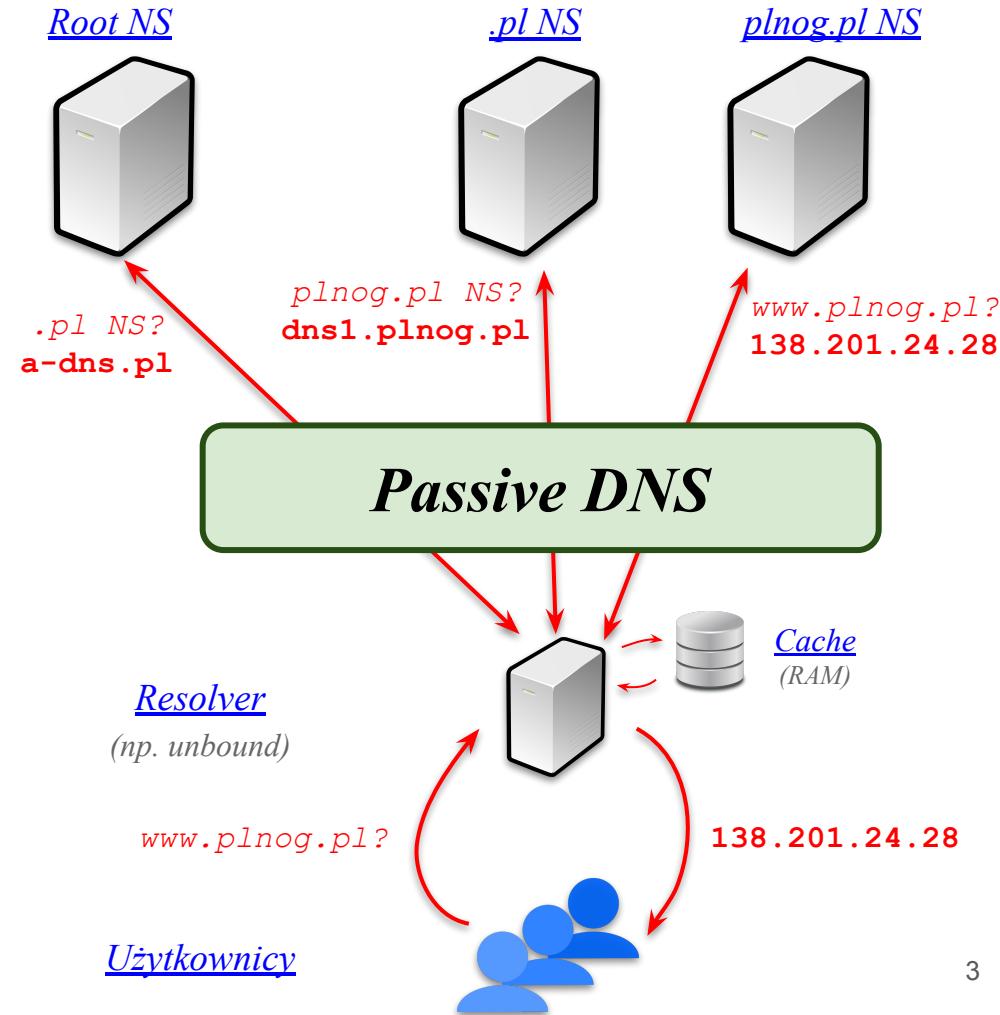
1. Co to jest “passive DNS”?
2. Czym zajmuje się Farsight Security?
3. DNSDB, czyli cały DNS w jednej bazie
4. NOD: Newly Observed Domains

Czas życia nowych domen:

5. Jaki % nowych domen przeżywa 7 dni?
6. Jak szybko te domeny znikają?
7. Dlaczego?
8. Wpływ TLD (.com, .pl, itp.)

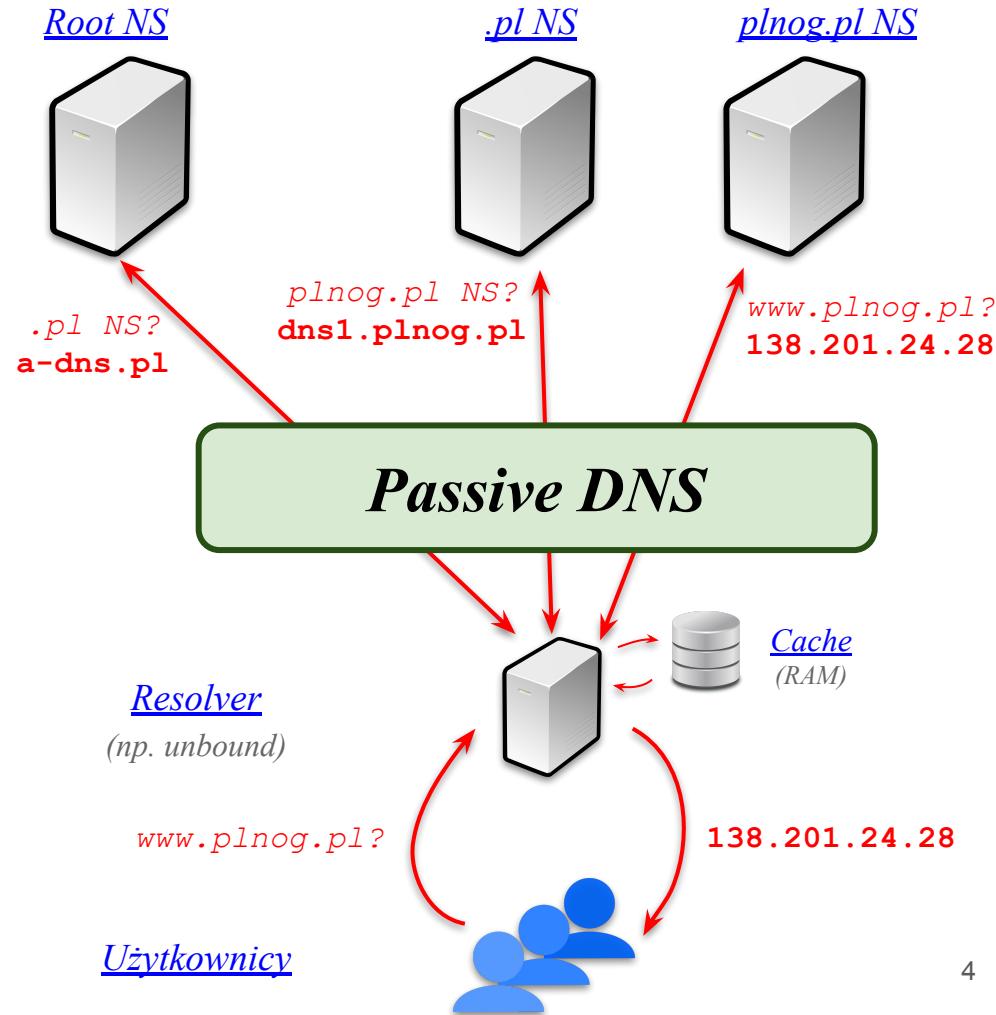
Passive DNS (pDNS)

- Technika pasywnej replikacji DNS
*F. Weimer, "Passive DNS Replication" (2005)
R. Edmonds, "ISC Passive DNS Architecture" (2012)*
- Cel: cały DNS w jednej bazie danych



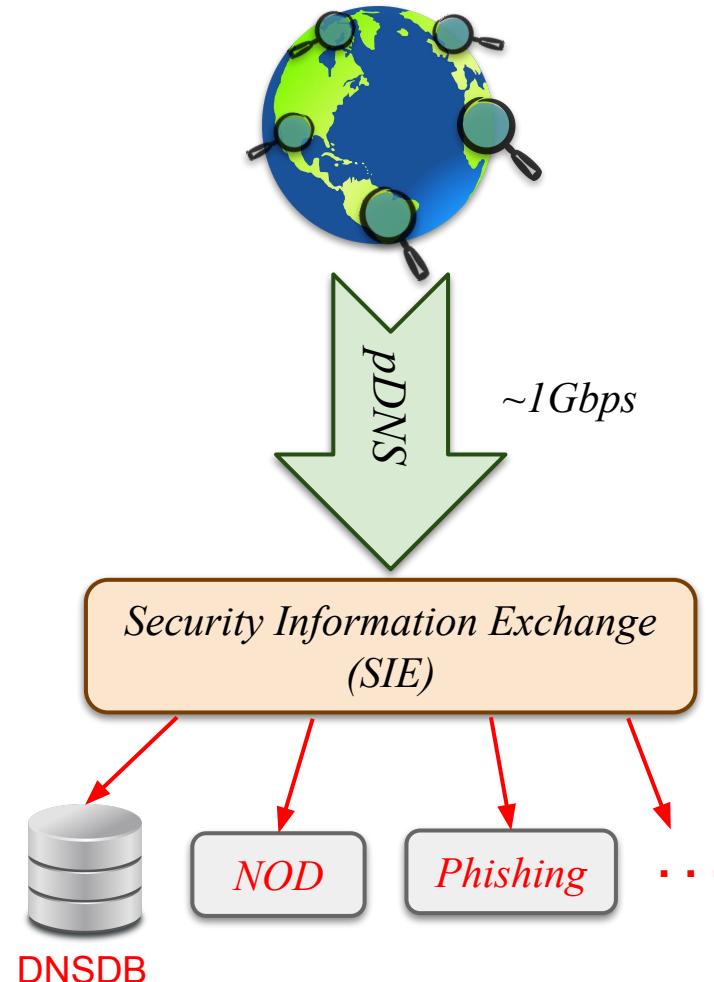
Passive DNS (pDNS)

- Technika pasywnej replikacji DNS
*F. Weimer, "Passive DNS Replication" (2005)
R. Edmonds, "ISC Passive DNS Architecture" (2012)*
- Cel: cały DNS w jednej bazie danych
- Sensory na resolverach DNS rejestrują tzw. "cache miss traffic"
 - Nie rejestrują ruchu użytkowników
- Ruch z wszystkich sensorów agregowany
- Przetwarzanie potokowe:
 - Deduplikacja
 - Weryfikacja
 - Filtrowanie
- Zapis do bazy / dalsze przetwarzanie



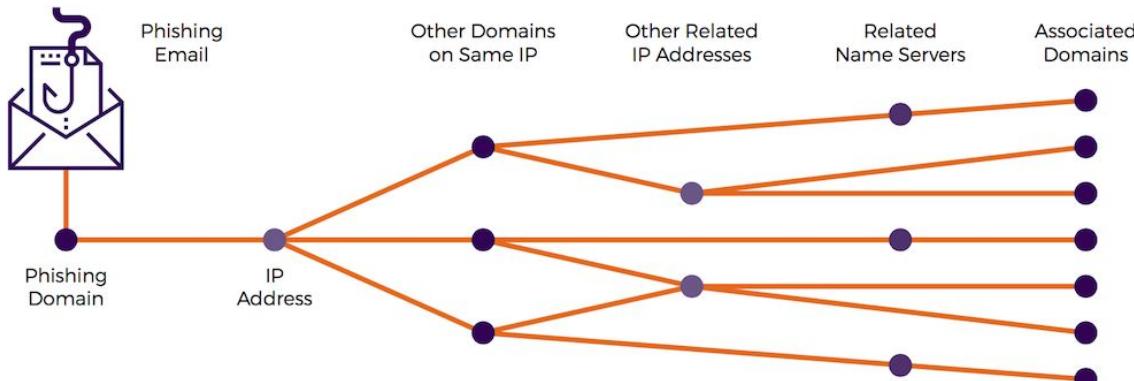
Farsight Security

- Założenie: Paul Vixie, 2013
 - DNS, DNSSEC, BIND, cron, F root, ...
- Sensory pDNS na całym świecie:
 - 2TB danych / dzień
 - 200K+ obserwacji / sekundę
 - Przetwarzane w czasie rzeczywistym
 - Partnerska wymiana danych (SIE)
- Zastosowania pDNS:
 - DNSDB
 - NOD, NOH, DNS Changes
 - DNS Errors (NXDOMAIN)
 - Detekcja phishingu (IDN)



DNSDB

- Największa baza pDNS, >100 mld rekordów
- Historia DNS od 2010
- Dostęp przez:
 - REST API
 - Interfejs WWW / CLI
 - Integracje (Maltego, Splunk, ...)
 - Eksport offline (wysyłamy dyski :))
- Zapytania w “przód” (“forward”), np.
 - `plnog.pl/A` -> historia adresów IPv4
 - `*.pl` -> wszystkie domeny .pl
 - `plnog.*` -> `plnog.net`, `plnog.org`, ...
- Zapytania w “tył” (“inverse”), np.
 - `138.201.24.28` -> inne domeny na serwerze
 - `*.plnog.pl/CNAME` -> wskaźniki na `*.plnog.pl`



DNSDB za free! ;)

www.farsightsecurity.com

The screenshot shows the Farsight Security homepage. At the top, there is a dark header bar with the Farsight Security logo on the left. To the right of the logo are navigation links: Solutions, Resources, Blog, Partners, Community, and Company. A search bar is located at the top right, featuring a magnifying glass icon. Below the header, there is a large, semi-transparent background image of a world map. In the center of the map, there is a white network icon consisting of a central circle connected to five smaller circles. Below this icon, the text "Power your Security Operations with DNSDB Free Trial API" is displayed in white. At the bottom of the page, there is a green button with the text "TRY FOR FREE". A red arrow points from the text above to the "FREE TRIAL" button in the header.

Newsletter | +1-650-489-7919

Search site

FARSIGHT SECURITY

Solutions ▾ Resources ▾ Blog Partners Community Company ▾

FREE TRIAL

Power your Security Operations with DNSDB
Free Trial API

TRY FOR FREE

DNSDB deep dive ;) (<https://github.com/dnsdb/dnsdbq>)

```
pawel@rd2:~$ dnsdbq -r plnog.pl/A -s
;; record times: 2010-06-24 14:07:11 .. 2010-07-13 09:46:52
;; count: 14; bailiwick: plnog.pl.
plnog.pl. A 89.161.170.67          AS12824 (home.pl)
;; record times: 2010-07-21 21:08:57 .. 2012-07-24 11:13:36
;; count: 4092; bailiwick: plnog.pl.
plnog.pl. A 91.207.11.13          AS48047 (kr-cpd.pl)
;; record times: 2012-07-24 16:33:54 .. 2014-03-17 13:32:32
;; count: 3663; bailiwick: plnog.pl.
plnog.pl. A 31.172.177.106        AS50481 (3S Fibertech)
;; record times: 2014-03-17 16:01:23 .. 2016-07-04 07:11:23
;; count: 12597; bailiwick: plnog.pl.
plnog.pl. A 31.172.177.102
;; record times: 2016-07-05 03:49:38 .. 2017-02-08 12:21:09
;; count: 482; bailiwick: plnog.pl.
plnog.pl. A 148.251.239.198      AS24940 (Hetzner, Fun. Proidea)
;; record times: 2017-02-10 01:16:38 .. 2018-09-28 11:29:17
;; count: 4761; bailiwick: plnog.pl.
plnog.pl. A 138.201.24.28        AS24940 (Hetzner, Proidea sp zoo)
pawel@rd2:~$
```

```
pawel@rd2:~$ dnsdbq -i 138.201.24.28/29 -s | sort | egrep '^[a-zA-Z0-9]+\.\pl\.'|more
bytemycode.pl. A 138.201.24.28
devopsdays.pl. A 138.201.24.28
event-wifi.pl. A 138.201.24.29
events-wifi.pl. A 138.201.24.29
eventy-wifi.pl. A 138.201.24.29
gamechangers.pl. A 138.201.24.28
hackyeah.pl. A 138.201.24.28
ictforum.pl. A 138.201.24.28
infraxstructure.pl. A 138.201.24.28
networkers.pl. A 138.201.24.29
networkki.pl. A 138.201.24.29
networkowo.pl. A 138.201.24.29
plnog.pl. A 138.201.24.28
proidea.pl. A 138.201.24.28
security-audit.pl. A 138.201.24.29
security-audits.pl. A 138.201.24.29
upcfuturemakers.pl. A 138.201.24.28
upcthinkbig.pl. A 138.201.24.28
pawel@rd2:~$
```

NOD: Newly Observed Domains

- Natychmiastowe powiadomienia o nowych domenach w całym DNS
 - Użycie domeny, nie rejestracja
- Strumień real-time (nie baza)
- Efektywne domeny drugiego rzędu (eSLD)
 - [www.plnog.pl](#) -> [plnog.pl](#)
 - [old.www.firma.com.pl](#) -> [firma.com.pl](#)
 - [app.cloudapp.net](#) -> [app.cloudapp.net](#)
 - FQDN -> [eSLD](#)
- Około 150 tysięcy nowych domen drugiego rzędu dziennie (~2 / sek.)

Dla porównania:

- NOH: Newly Observed Hostnames
- Powiadomienia o nowych FQDN (Fully Qualified Domain Names)
 - [www.plnog.pl](#)
 - [old.www.firma.com.pl](#)
 - itp.
- Około 12 milionów nowych FQDN dziennie (~150K / sek.)

Ile nowych domen przeżywa tydzień?

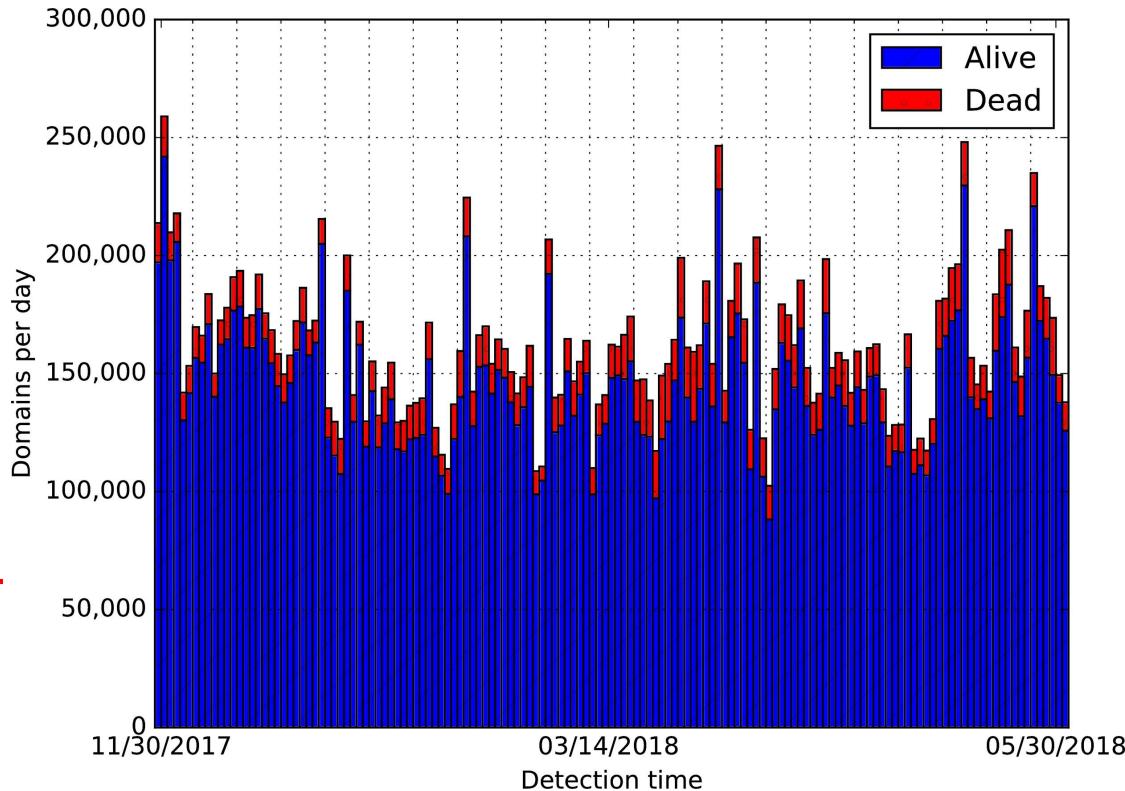
- Pomysł: odpytywać każdą nową domenę od momentu wykrycia przez 7 dni
 - Na poziomie TLD (**delegator**)
 - Na poziomie ISP (**authoritative NS**)
 - W **blacklistach** (Spamhaus, SURBL, Swinog)
- Rosnące interwały zapytań
 - +1024s, +2048s, +4096s, +8192s, +8192s, ...
 - W praktyce: **20 powtórzeń w 7 dni**
- Uznaj pierwszy błąd za “uśmiercenie”
 - TLD/ISP: zwraca NXDOMAIN (skasowana)
 - Blacklista: zwraca SUCCESS (zablokowana)
- Jaki % przeżyje?

Parę szczegółów:

- Infrastruktura: własna sieć resolwerów rozproszona na kilku kontynentach
 - System kolejkowania, monitorowania
 - Agregacja wyników w bazie SQL
- Pomijamy “wildcard” TLDs, np. **.ws**
 - “Nieśmiertelne” domeny *<random>.ws*
- Szczegółowy opis metodologii w artykule:
P. Foremski, P. Vixie, “The Modality of Mortality in Domain Names”, Virus Bulletin Conference, VB2018 Montreal

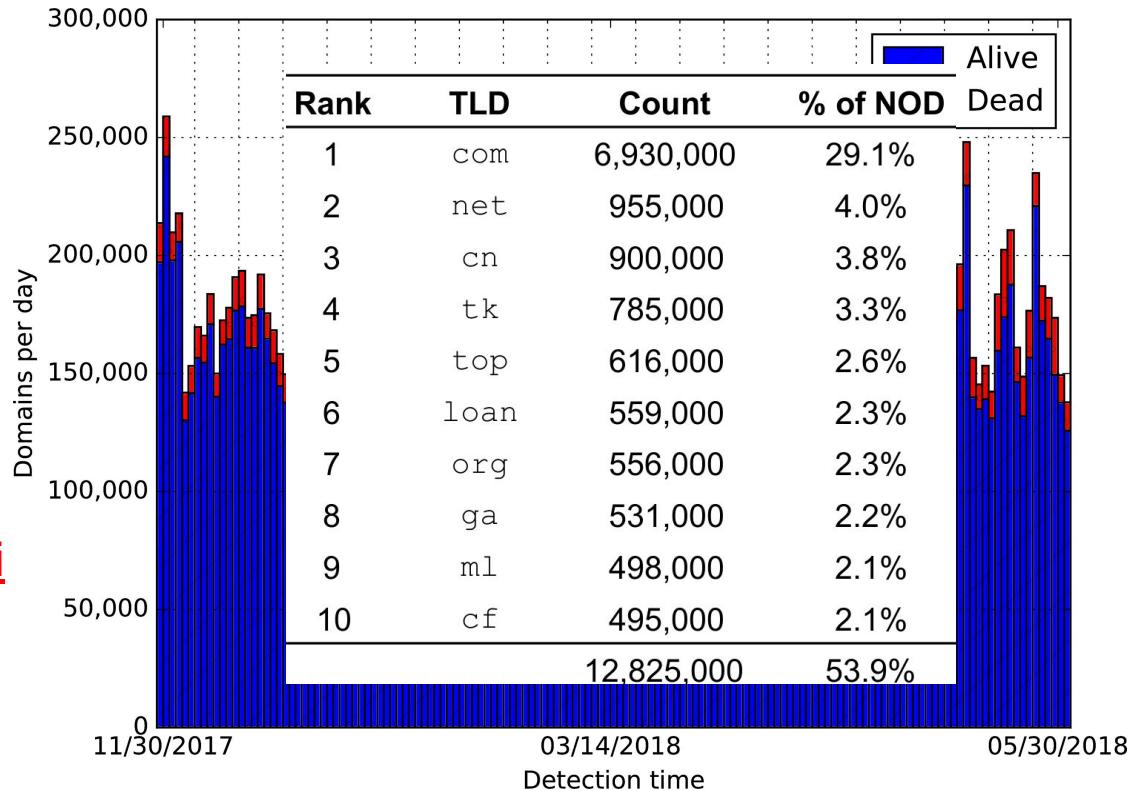
Ile % przeżywa?

- Wykryto 23.8M nowych domen drugiego rzędu (NODs)
- Czas: 12/2017 - 05/2018
- 21.6M przeżyło (90.7% wszystkich NODs)
- 2.2M “zmarło” szyciej niż 7 dni (9.3% wszystkich NODs)



Ile % przeżywa?

- Wykryto 23.8M nowych domen drugiego rzędu (NODs)
- Czas: 12/2017 - 05/2018
- 21.6M przeżyło (90.7% wszystkich NODs)
- 2.2M “zmarło” szybciej niż 7 dni (9.3% wszystkich NODs)

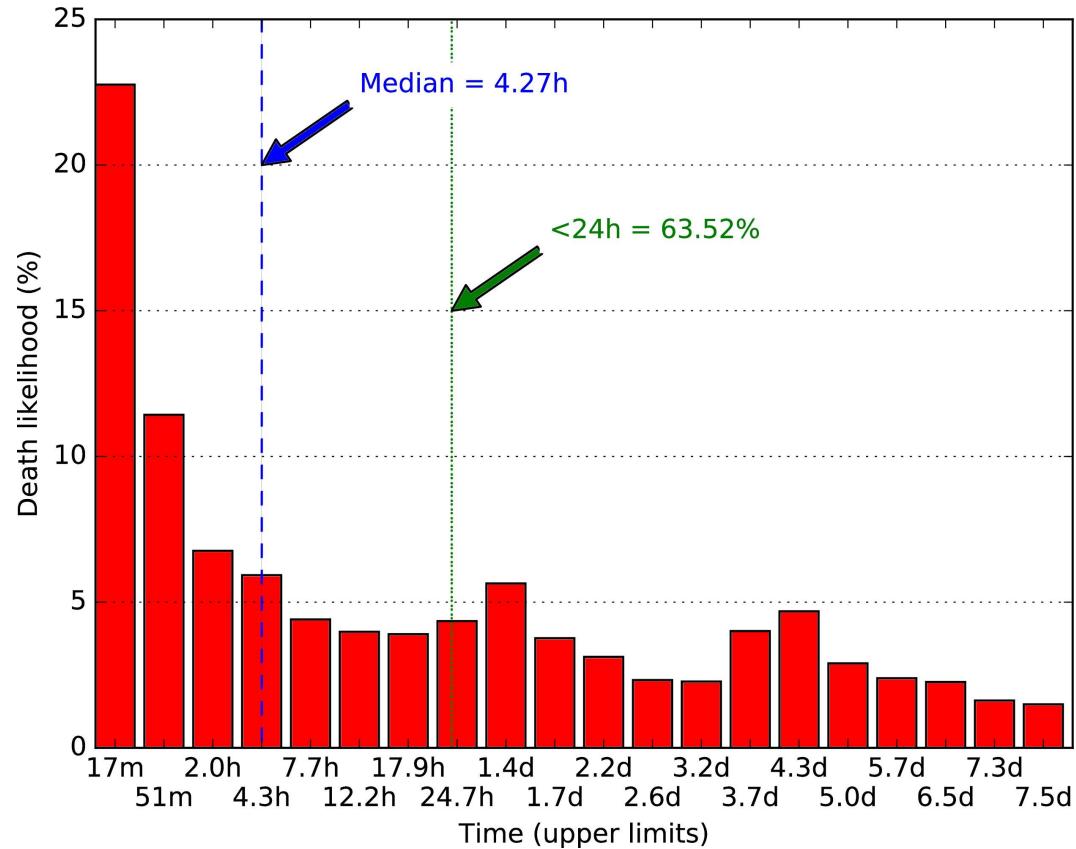


Czas życia

(analiza 2.2M "uśmierconych" NODs)

- Większość znika w ok. 4 godziny
- >60% znika w 24 godziny
- Trzy "momenty śmierci":
1h 1.5d 4d

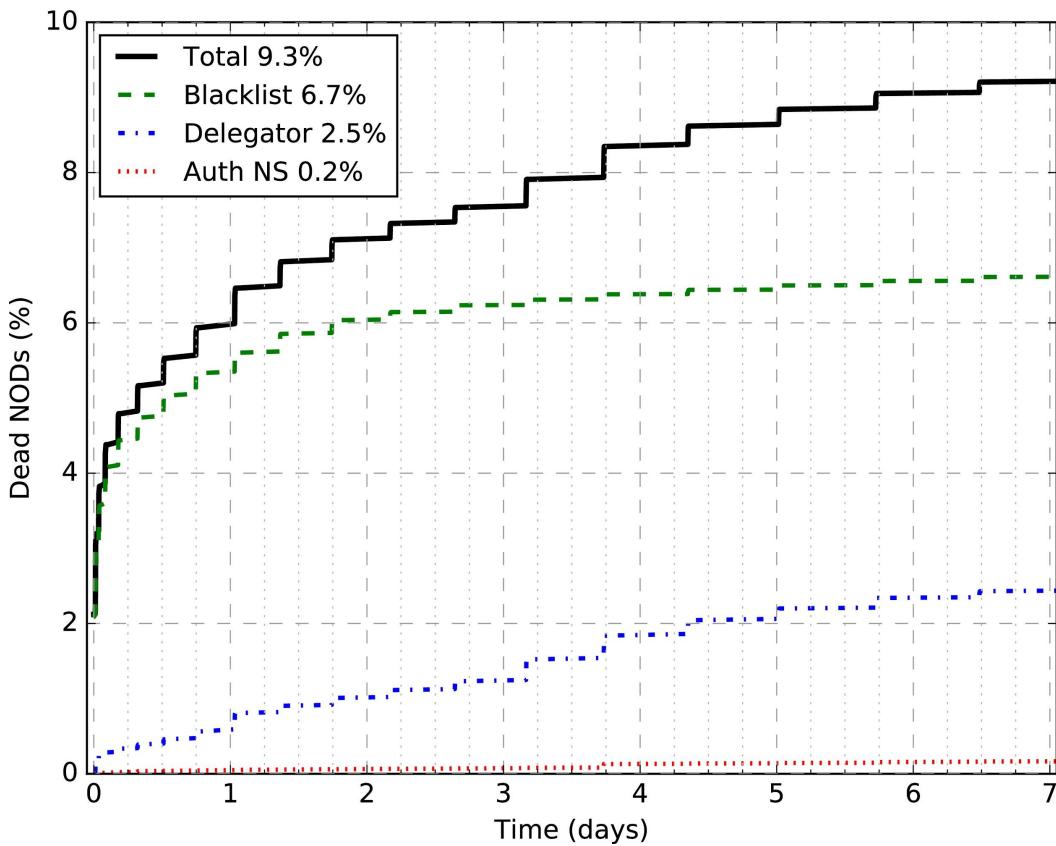
"Im nowsza domena, tym większa szansa, że zniknie *naprawdę* szybko"



Dlaczego?

(pierwsza przyczyna “śmierci”)

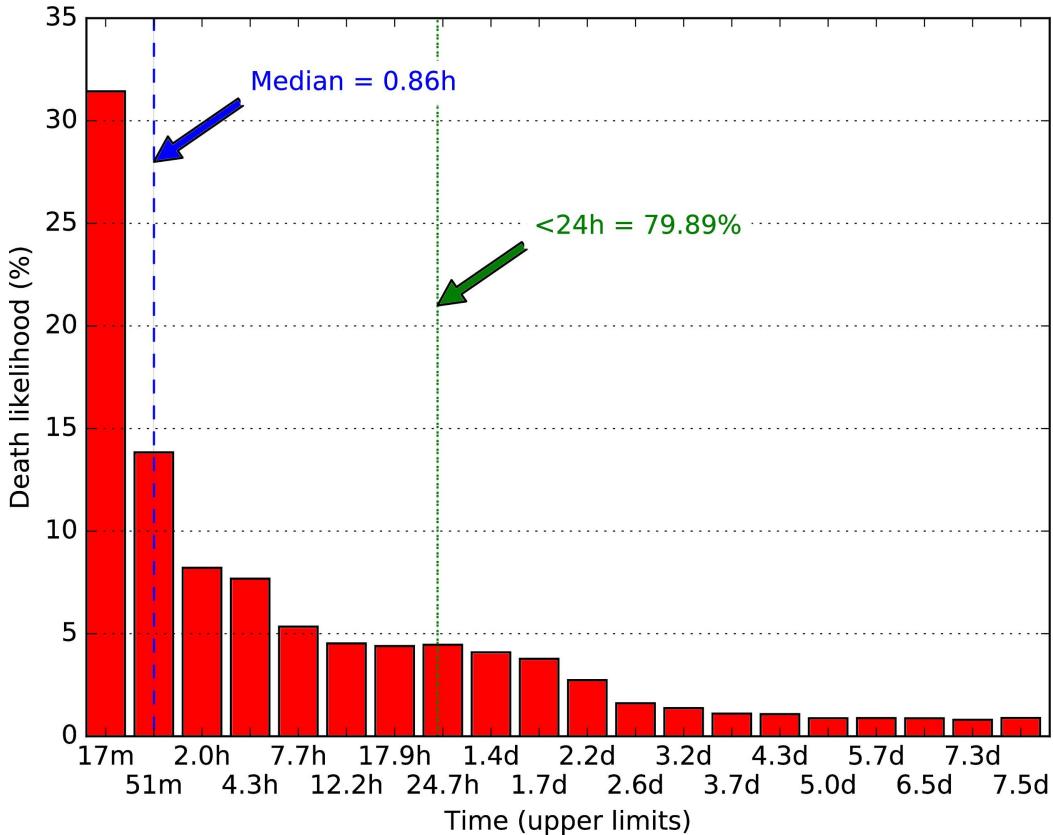
- Blacklisty to główna przyczyna (6.7% NODs)
- Poziom TLDs (delegator) to druga przyczyna (2.5% NODs)
- Nowe domeny bardzo rzadko znikają u ISP (0.2% NODs)
- Każda przyczyna ma inną dynamikę czasu



Blacklisty DNSBL

(6.7% NODs)

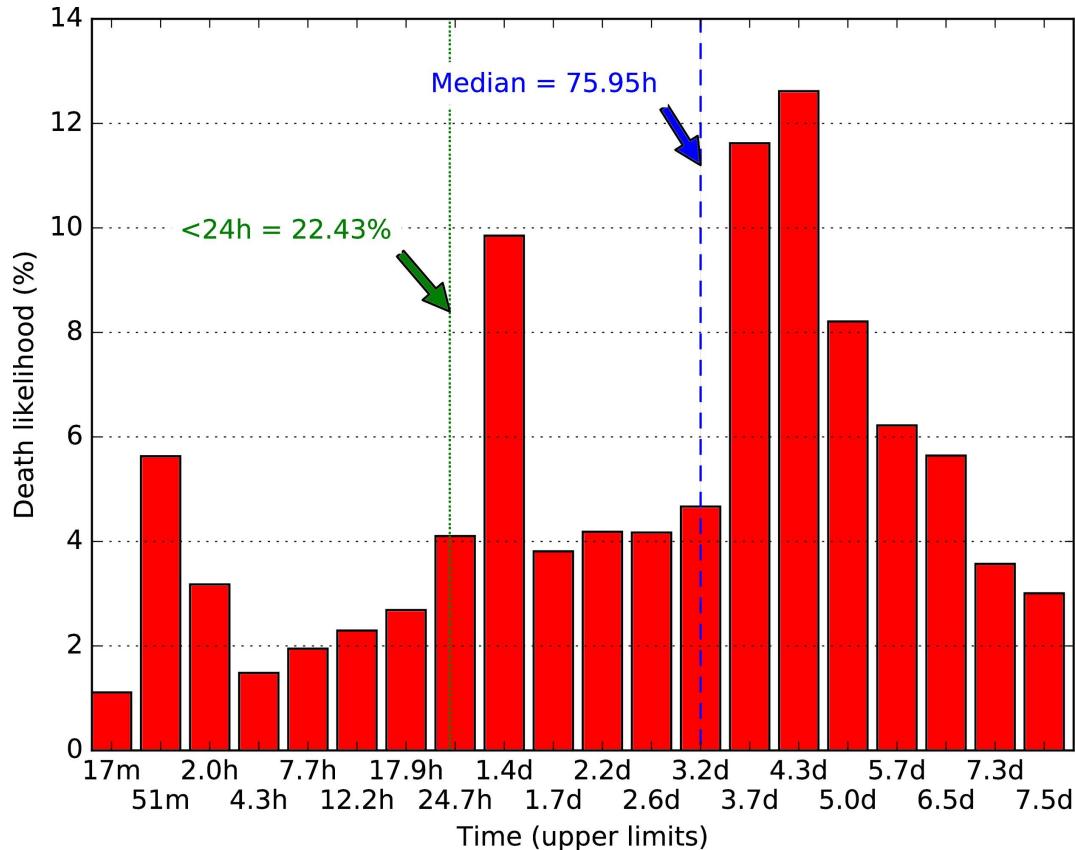
- W większości wypadków blacklisty “kasują” domenę poniżej 1h
- 80% pracy blacklist to 24h
- Rozkład +/- wykładniczy



Poziom TLD

(2.5% NODs)

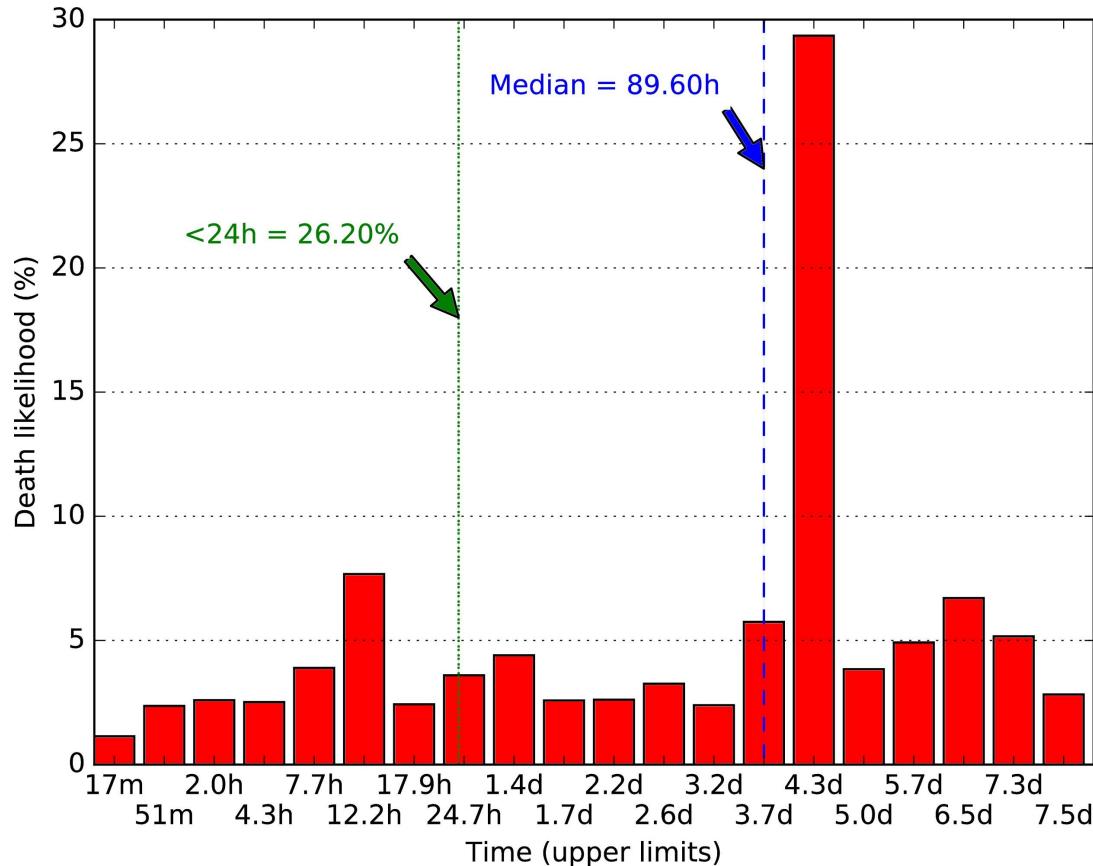
- Skoki ~1h, ~1.5d, ~4d
- automatyczne procedury?
- TLD są wolniejsze niż DNSBL:
medianą to ~76h (>3d)
- Tylko 22% usunięte w <24h



Poziom ISP

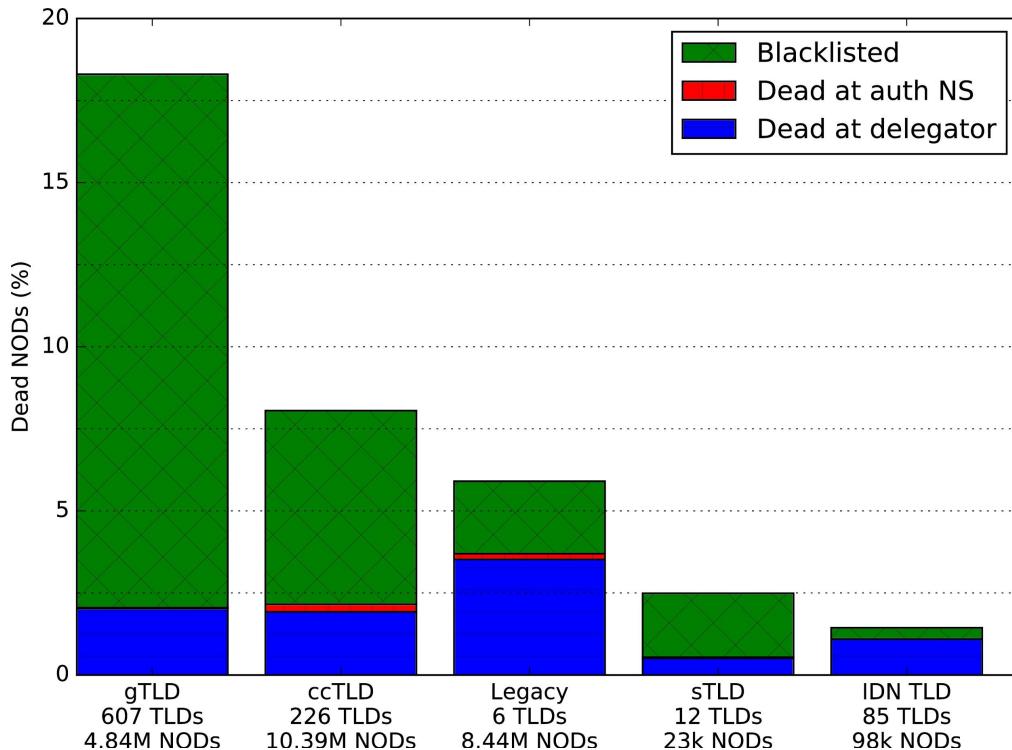
(0.2% NODs)

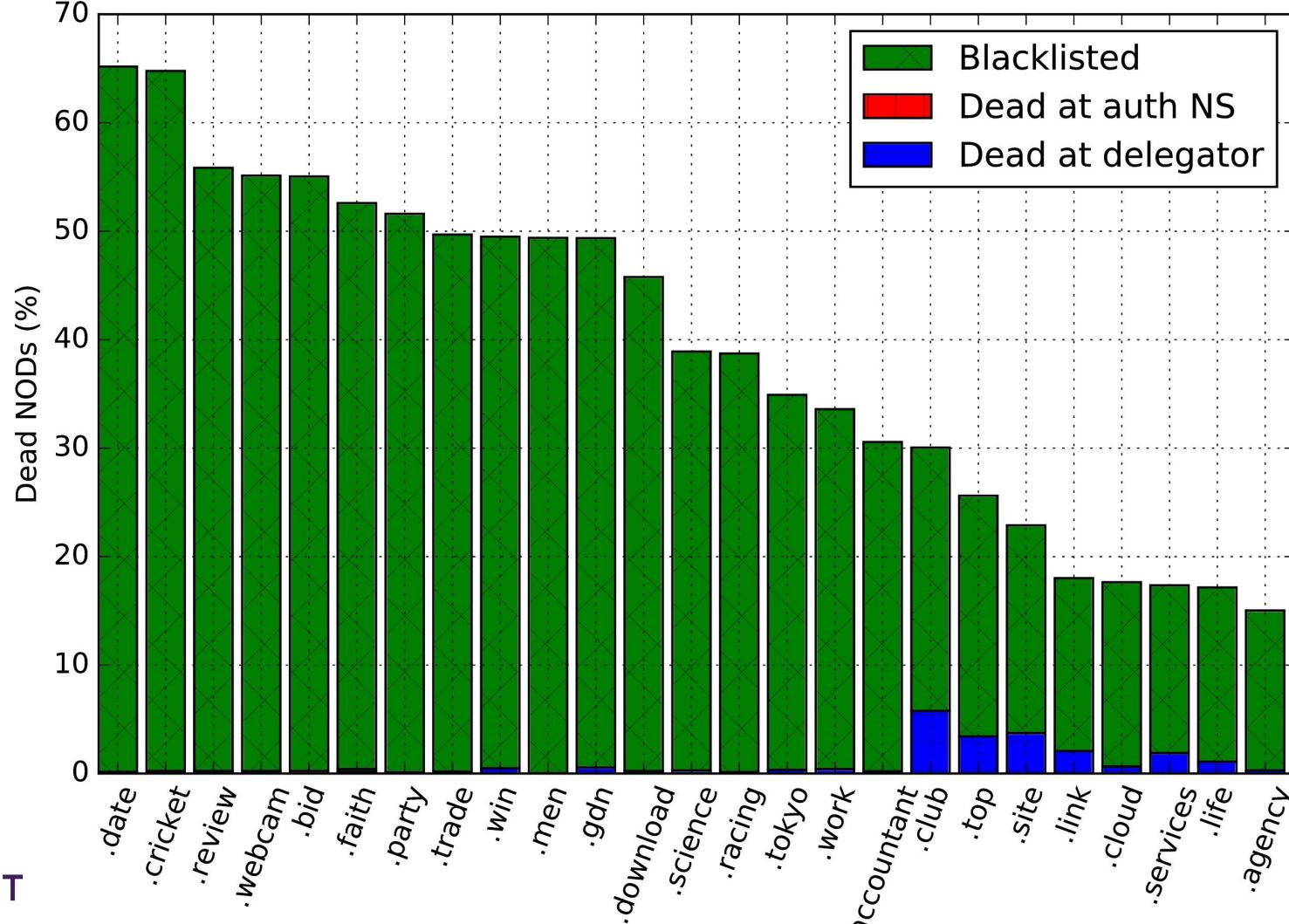
- Skok ~4d (.to), mniejszy ~12h
- Nowe domeny bardzo rzadko i powoli “giną” u ISP: odpowiednio 0.2% i ~90h (3 dni i 18h)
- Poziom stosunkowo łatwy w kontroli (własny serwer)



Typ TLD a śmiertelność

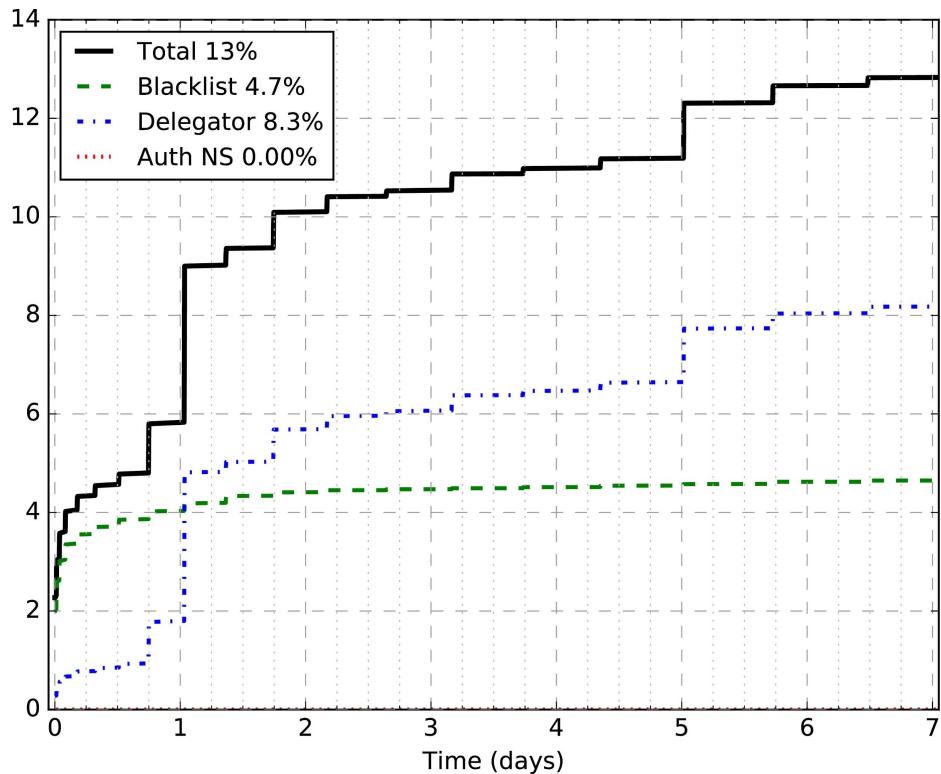
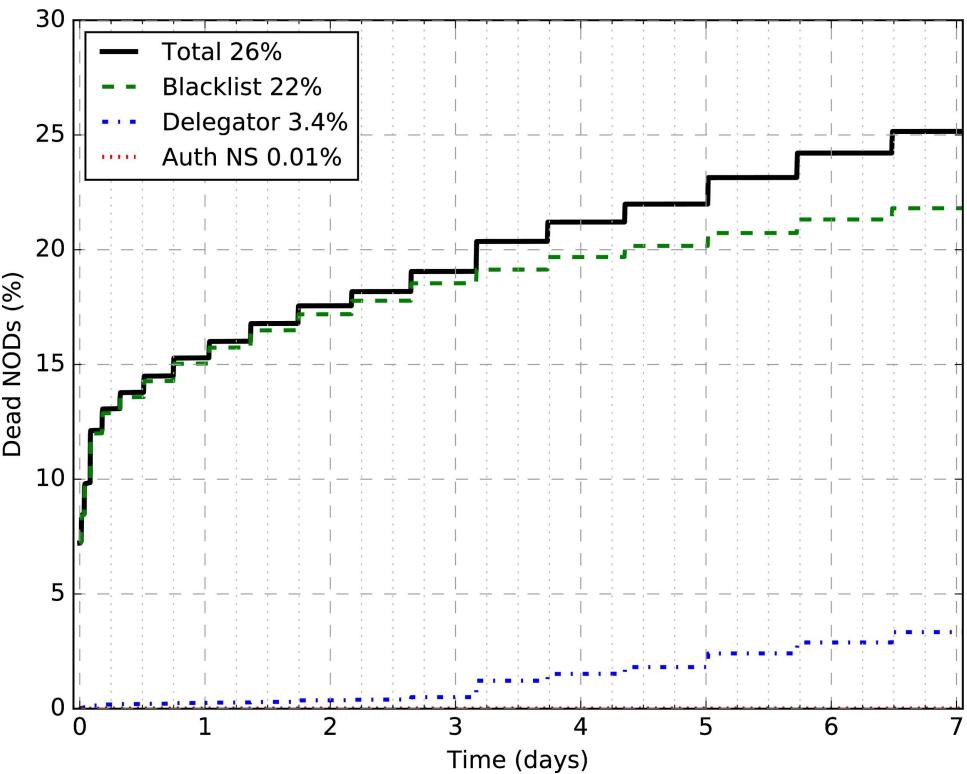
- Niemal co 5 nowa domena gTLD zniką w 7 dni (blacklisty)
- Domeny “tradycyjne” (.com itp.) zwykle “umierają” na poziomie TLD
- Domeny kraju (ccTLD) wypadają nieco gorzej niż tradycyjne, ale należą do nich .tk, .gq, itp.
- Nowe domeny w TLD typu IDN i sponsorowanych są kasowane dość rzadko (czemu?)



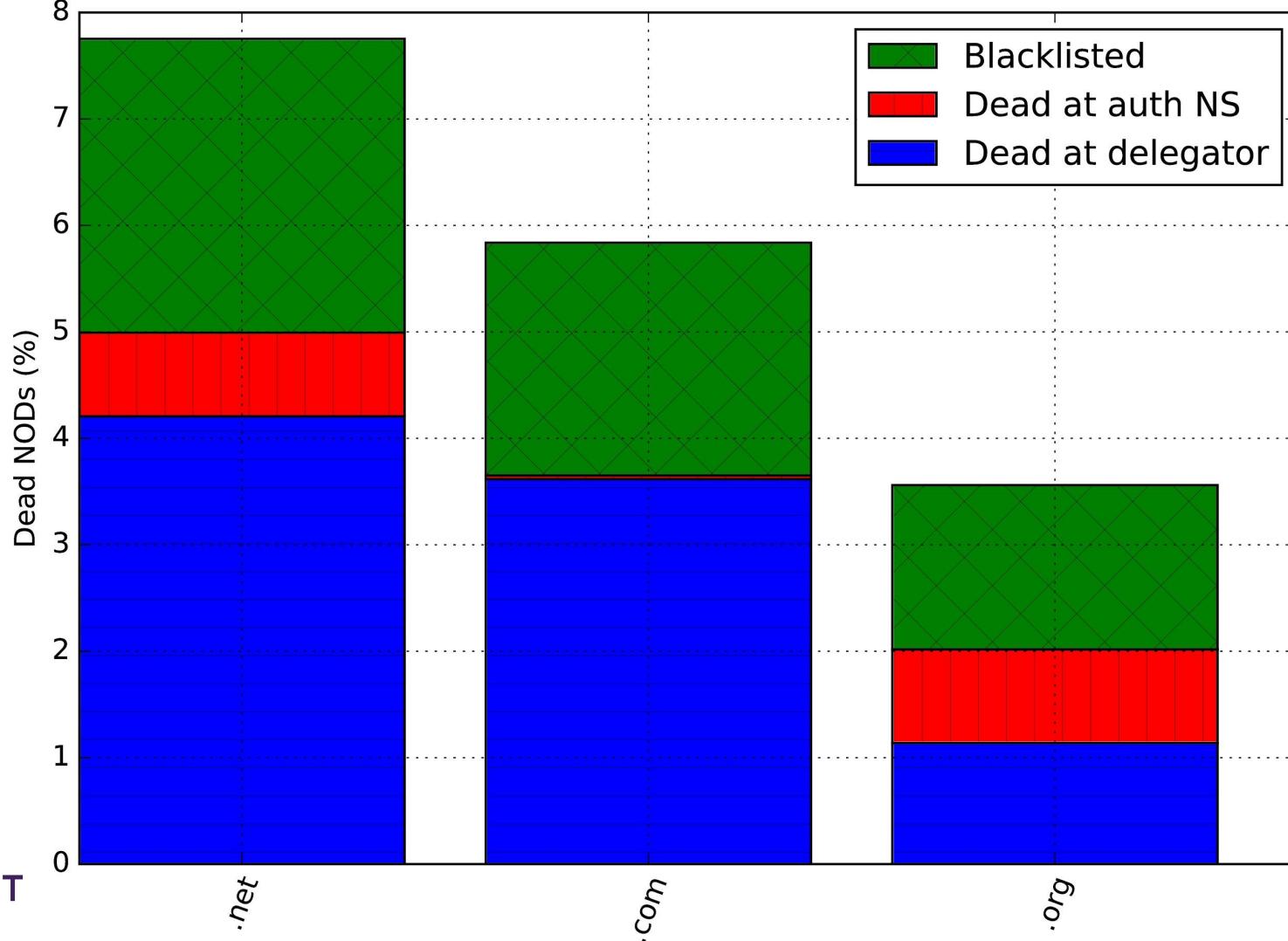


.top

.xyz

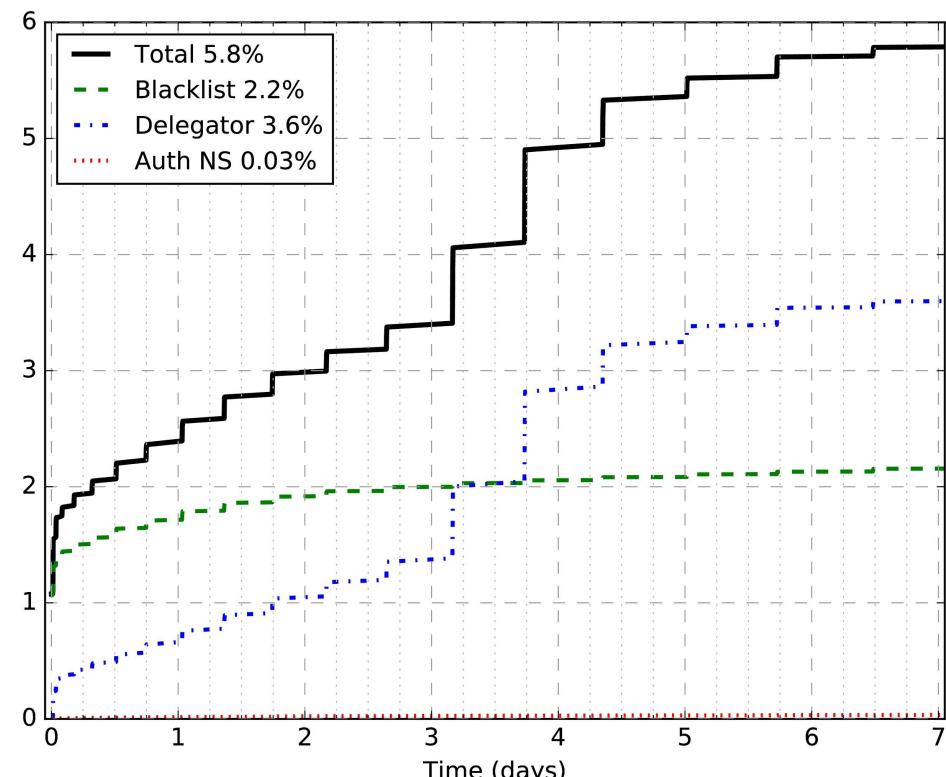
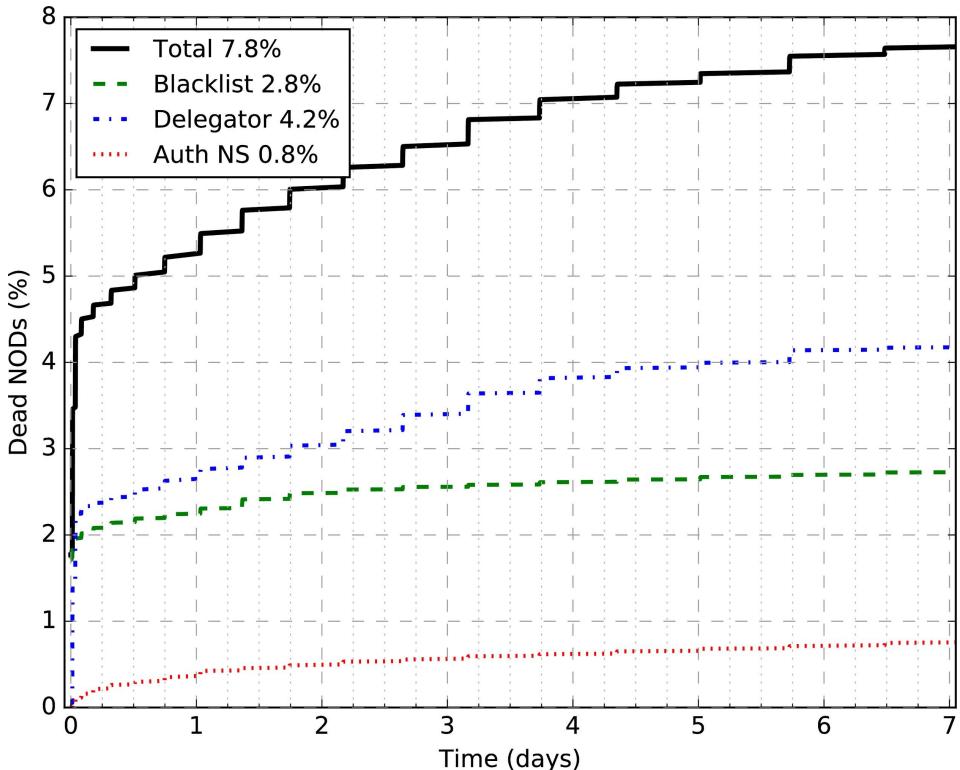


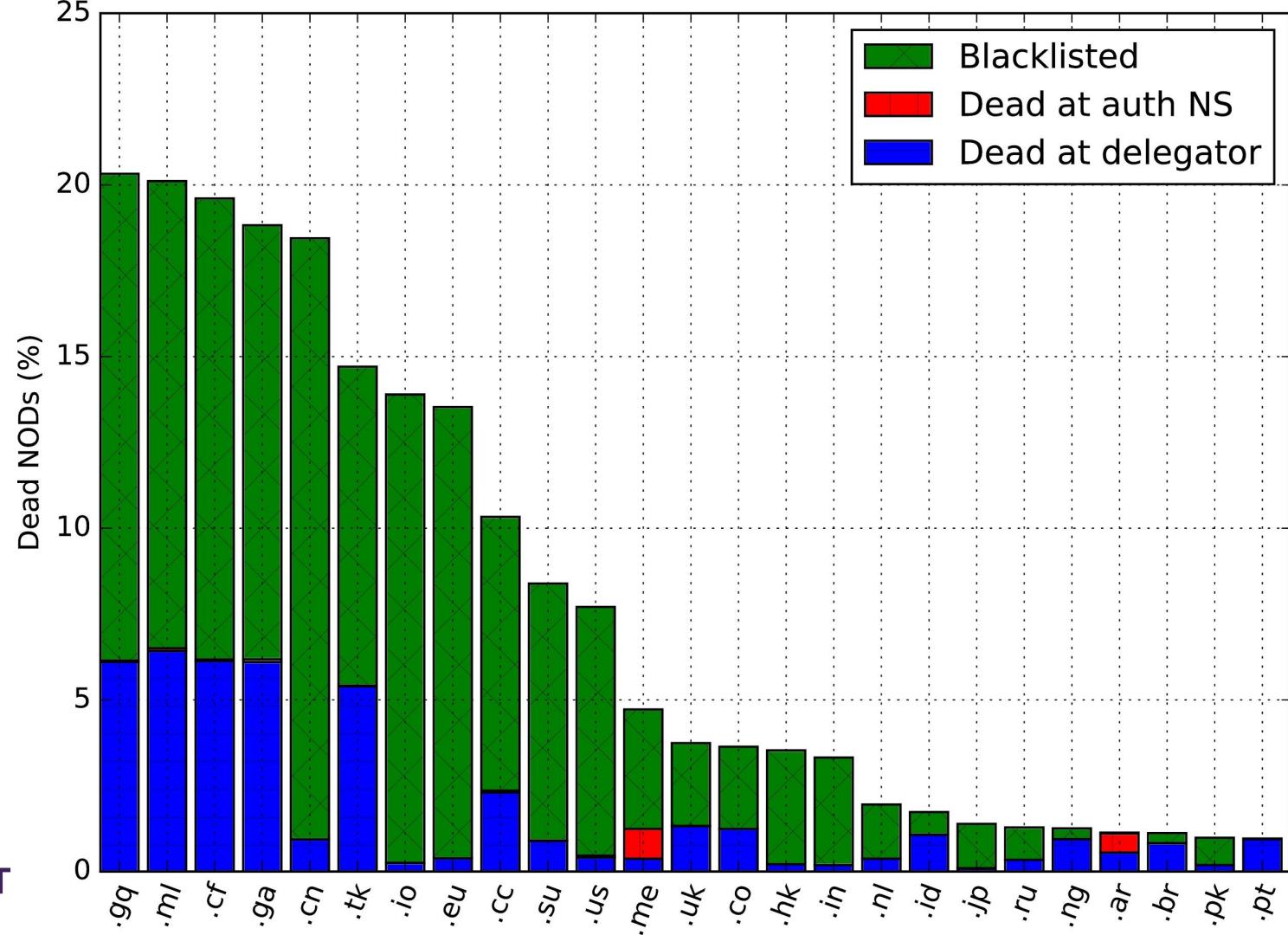
Legacy



.net

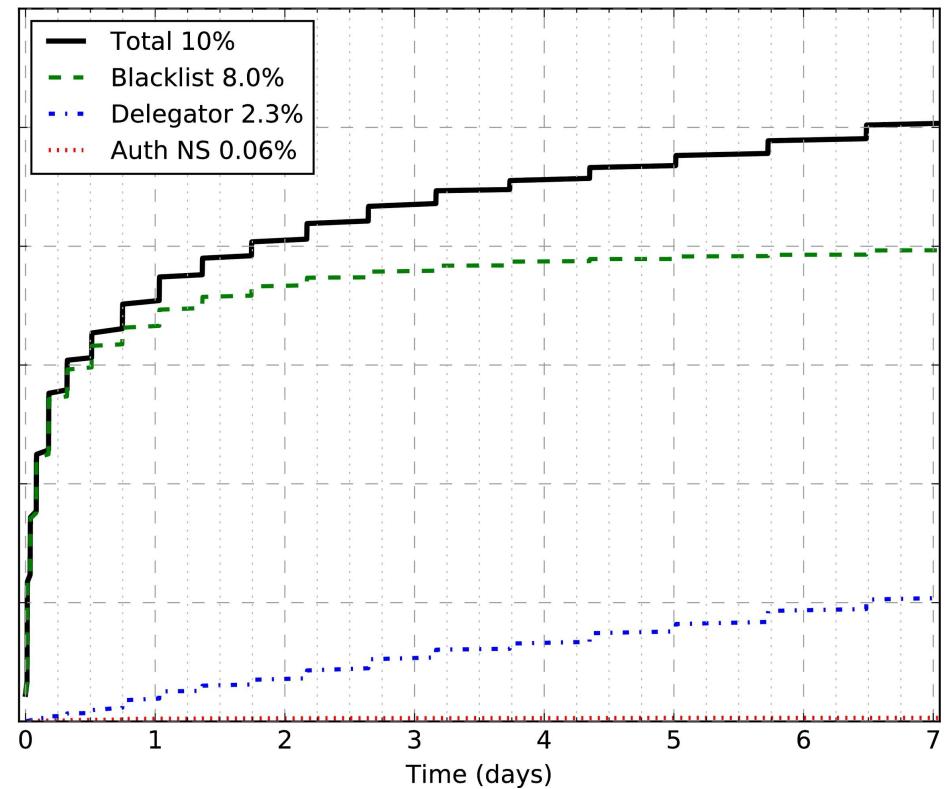
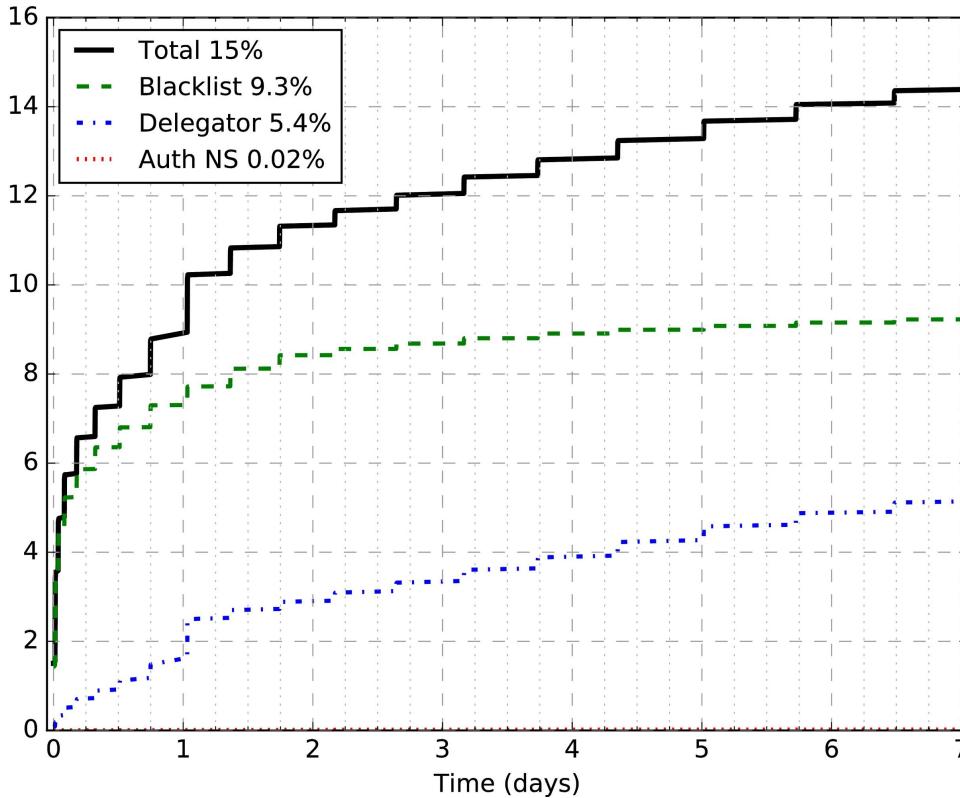
.com





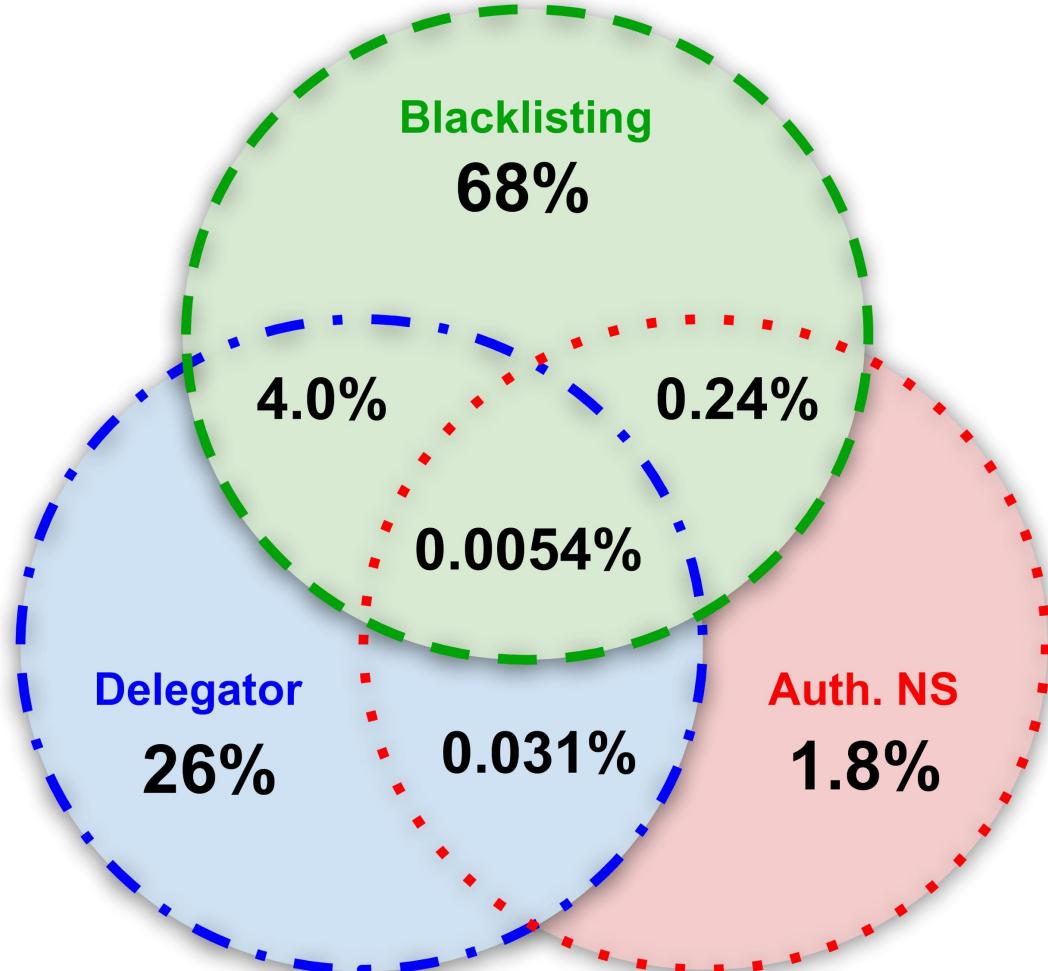
.tk

.cc



Zależności

Gdyby nie rozważyć wyłącznie chronologicznie *pierwszej* przyczyny śmierci domeny, to jak te wszystkie 3 przyczyny zależą od siebie?



Podsumowanie

- Passive DNS to prosta metoda zbierania **faktów** nt. bezpieczeństwa
- Farsight Security to światowy **lider** passive DNS, otwarty na współpracę
- Jest **free trial** do DNSDB ;-)
- Codziennie wchodzi do użycia **150 tysięcy** nowych domen (i tyle samo **hostów** w ciągu sekundy)
- Spośród nowych domen, **ok. 10%** nie przetrwa tygodnia (mediana 4h)
- Główną przyczyną **blacklisty** (1h), chociaż działania TLD również
- Średnio prawie **co 5 domena gTLD** ginie dość szybko po użyciu
- **Nie** wystarczy zablokować wszystkich domen gTLD :)
- Różne mechanizmy bezpieczeństwa DNS **uzupełniają się wzajemnie**

Pytania?

*DNS intelligence:
czas życia nowych domen*

PLNOG 21
Kraków, 1-2 X 2018



Paweł Foremski

pif@fsi.io, [@pforemski](https://twitter.com/pforemski), www.foremski.pl

Senior Distributed Systems Engineer
Farsight Security, Inc.

www.farsightsecurity.com

FARSIGHT
SECURITY