The Modality of Mortality in Domain Names

Pawel Foremski, Paul Vixie

Farsight Security, Inc.

{pjf,vixie}@fsi.io

Objectives

1. What fraction of new domains survive a week?
2. How fast new domains die?
3. What are the causes of death?
4. How the above differs among TLDs?

Full report at bit.ly/dns-mortality

Contributions

New Measurement Methodology

1. Newly Observed Domains (NOD), a data feed that notifies us in real-time about second-level domains used for the first time on the Internet,
2. A scheduler that listens to NOD, looks up the name servers responsible for each new domain, and schedules periodic measurements,
3. A distributed pool of resolvers that run DNS lookups, and
4. A database that collects and aggregates the results.

The general method is to repeatedly check for 7 days:

- *Does it still exist in the DNS?*
- *Is it still not listed in domain block lists?*

Quantification of Malicious DNS Usage

The methodology allowed us to quantify the prevalence and longevity of new suspicious domains on the public Internet, including understanding the mechanisms that actually neutralize abused names.

Identification of Struggling gTLDs

The new gTLDs program brought the community some exciting TLDs, but it also gave the Internet some TLDs that are disproportionately abused. Our work pinpoints the gTLDs that may need remedial attention — at least if those specific new gTLDs are to remain welcome at most sites.

New Domains Need Assessment

9.3% of NODs ended up "dead" within a week, which underscores the importance of intentionally temporarily ignoring new domains for a certain period of time, until they can be vetted by domain reputation organizations.

Collected Data

- Evaluated 23.8 million NODs seen by Farsight during the six months from December 2017 through May 2018.
- Each NOD tracked via a series of active probes made to (a) the delegator, (b) the authoritative name server, and (c) three DNS block lists (Spamhaus, SURBL, Swinog).
- Sent a total of 20 probes over roughly 7 days to each NOD. First immediately upon discovery, then after 1,024s, 2,048s, 4,096s, and at intervals that increased by 4096s. The final probe made at 7d 6h 56m (629,760s). Each probe was repeated 3 times in case of no reply.
- A NOD considered "dead" when the delegator or the authoritative name server starts returning NXDOMAIN, or when the domain is listed on a domain block list.

Selected Results

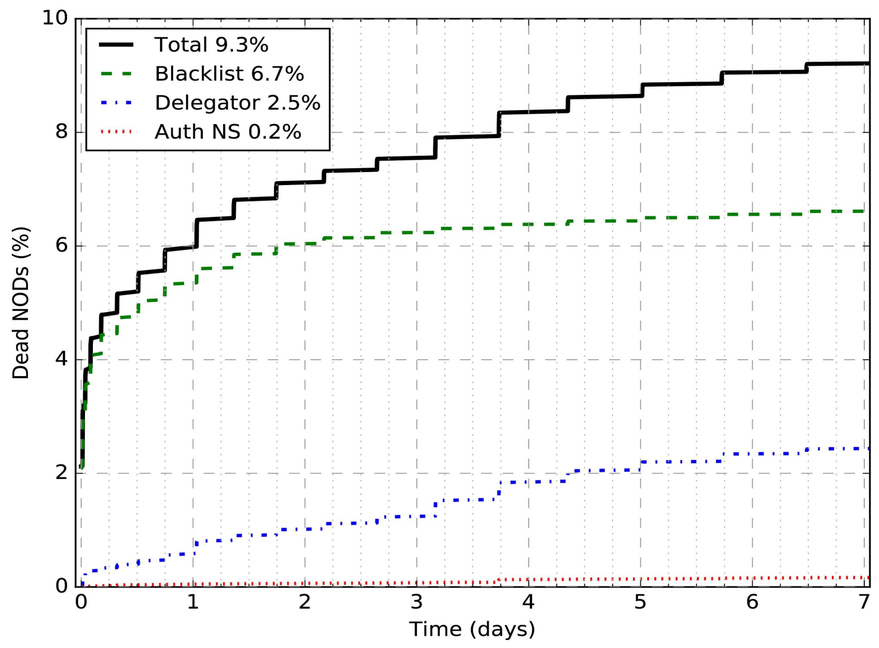

Fig. 1: Why NODs die? CDF of death probability for 3 causes.

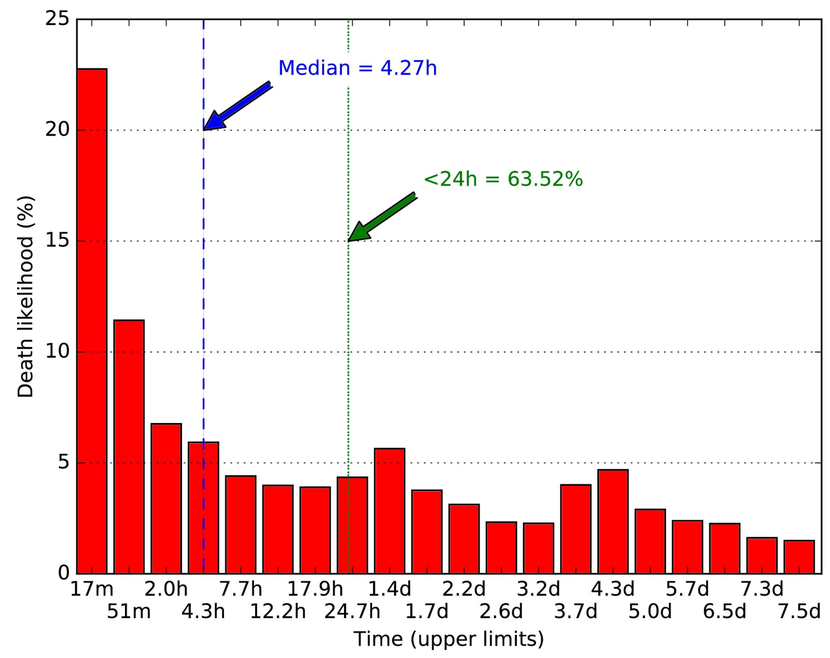

Fig. 2: How fast NODs die? Death likelihood vs. domain age.

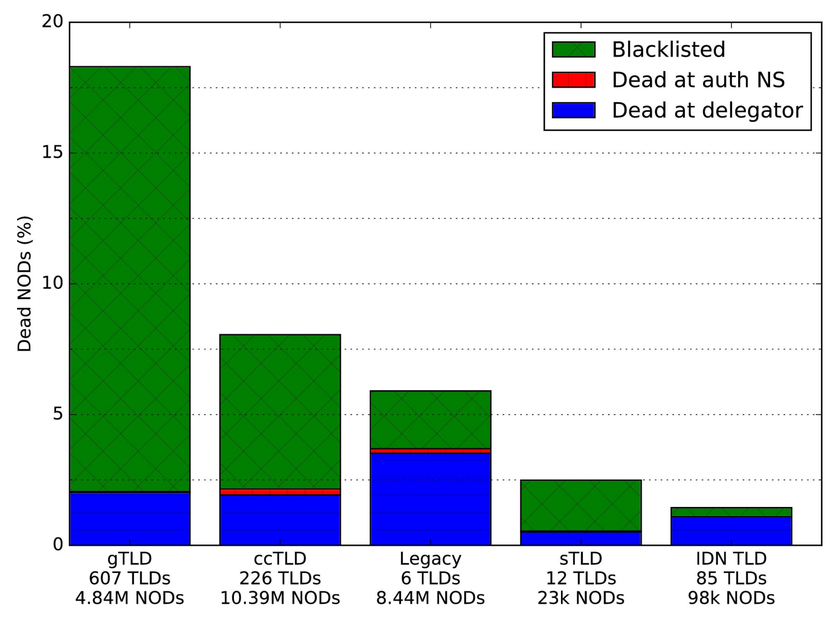

Fig. 3: How the TLD type impacts NOD death ratio?

Fig. 4: How bad a TLD can be? Top 25 significant gTLDs.

FARSIGHT SECURITY

ACM Internet Measurement Conference 2018

Oct 31 - Nov 2, 2018, Boston, MA, USA