The Modality of Mortality in Domain Names

An In-depth Study of Domain Lifetimes

Dr. Paul Vixie, CEO
Farsight Security, Inc.

Copyright 2019 Farsight Security, Inc.
Agenda

1. Introduction & study details
2. What % of new domains survive a week?
3. How fast new domains die?
4. Causes of death
5. Impact of new gTLDs, ccTLDs, etc.
6. Summary & takeaways
Introduction: BIG data

- Passive DNS sensors deployed world-wide
- Data volume: 2TB of streaming data per day
- DNSDB: historical pDNS database since 2010
- Newly Observed Domains (NOD): real-time notifications of newly observed effective second-level domains
Introduction: BIG questions

• Are popular assertions correct?
  • “95% of new domains are junky and malicious”
  • “they live nasty, cruel, and short lives”
  • “they are quickly destroyed by the registrars”
  • “it is all because of the new gTLDs!”

• Why should I care?
Study details: measuring NOD lifecycle

- **Idea**: measure all NODs during their first 7 days of life
  - data cleanup: drop wildcard TLDs (e.g. .pw) and incomplete measurements
- For each NOD (e.g. `domain.com`), repeatedly query:
  - **delegator**: usually the TLD name server (e.g. `a.gtld-servers.net`)
  - **authoritative NS**: the server delegated for the zone (e.g. `ns.domain.com`)
  - **DNSBLs**: Spamhaus, SURBL, Swinog URI BL
- Make **20 repetitions** per NOD in **increasing** time intervals
  - 0 sec., +1024s (~17 min), +2048s (~34 min), +4096s (~68 min), ..., 7 days
- Consider **only the first** cause of domain death
Background: Effective Second-Level Domains

e.g. for FQDN = lb5.azure-app.cloudapp.net

• Theory:
  -- Top-Level Domain (TLD): .net
  -- Second-Level Domain (SLD): cloudapp.net

• Practice:
  -- effective TLD: .cloudapp.net
  -- effective SLD: azure-app.cloudapp.net

More info: see https://publicsuffix.org/
Background: NOD vs. NOH

- **NOD**: Newly Observed Domains
  - effective SLDs, e.g. example.com
  - use case: protecting brands
  - March 2018 avg: >2 NODs / sec, or >150K NODs / day

- **NOH**: Newly Observed Hosts
  - FQDNs (hostnames), e.g. printer4.example.com
  - use case: detecting domain shadowing
  - March 2018 avg: >150 NOHs / sec, or >12,000K NOHs / day
What % survives?

- Evaluating 23.8M NODs (after cleanup – slide 5)
- Time span: 11/2017 - 05/2018
- 21.6M survived (90.7% of all NODs)
- 2.2M “dead” in under a week (9.3% of all NODs)
How fast do they die?
(drill-down into 2.2M NODs)

• “The newer the domain, the more likely to die really fast
• Majority will die in under 5 hours
• >60% will die in under 24 hours
• Three “modes” in mortality rates:
  0-2h  1-1.5d  4-4.5d
Causes of death
(only the first one)

- **Blacklisting is the major cause** (6.7% of NODs)
- **Delegators (TLDs) are the second largest cause** (2.5% of NODs)
- **NODs are rarely “killed” at the authoritative NS level** (0.2% NODs)
- **Each cause has different time characteristics**

![New Domains: causes of death](image-url)
Intersections
(ignoring which was the first)
Blacklisting kills fast
(drill-down into 147,400 NODs)

- In most cases, DNSBL will effectively kill a NOD in <1h
- >79% of NOD blacklisting happens in the first 24 hours
- No peaks, simple distribution
Deaths at delegators
(drill-down into 55K NODs)

• Huge peaks at \(\sim 1\text{h}, \sim 1.5\text{d}, \sim 4\text{d}\)
  - impact of automated procedures?
• Delegators are much slower than DNSBLs: median \(\sim 2.2\text{ days}\)
• Only <22% deleted in <24h
Authoritative NS
(drill-down into 4,400 NODs)

- Huge peak around 4 days, smaller around 12h
- Deaths at authoritative NS rare & slow: median ~3.7 days
- <27% of deaths at auth NS happen in <24h
Impact of TLD Type

- **Almost 1/5 of new gTLD domains** die fast, usually due to blacklists
- **Domains under Legacy TLDs** usually die at the delegator
- **6.2% of domains in ccTLDs die fast**, but these include .tk, .gq, etc.
- **Domains in IDN and sponsored TLDs** least likely to die fast (<2.5%)
New Domains: top 25 gTLDs by death rate

Avg. registration price: <$1

Dead NODs (%)

Blacklisted
Dead at auth NS
Dead at delegator

Copyright 2019 Farsight Security, Inc.
New Domains under .top: causes of death

- Total 26%
- Blacklist 22%
- Delegator 3.4%
- Auth NS 0.01%

New Domains under .xyz: causes of death

- Total 13%
- Blacklist 4.7%
- Delegator 8.3%
- Auth NS 0.00%
New Domains: top 25 Legacy TLDs by death rate

[Chart showing the breakdown of dead domains across different TLDs.]
New Domains: top 25 ccTLDs by death rate

Avg. registration price: >$5
Summary & Takeaways

- NOD death rate varies among TLDs, **8.4% on average**
  - ...but some TLDs have >50% death rate
- Majority of NOD deaths **happen in <5h** on average
  - ...but blacklists kill in <2h
- **Blacklisting** is the main cause of NODs becoming effectively dead
  - delegators seem to use automated procedures (>1h, >1d, >4d)
  - NODs are rarely killed at their authoritative NS (0.2% avg.)
- Domains **under the new gTLDs** are much more likely to die fast (~1/5)

Copyright 2019 Farsight Security, Inc.