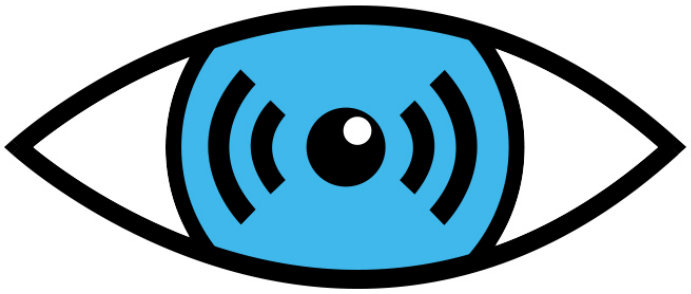
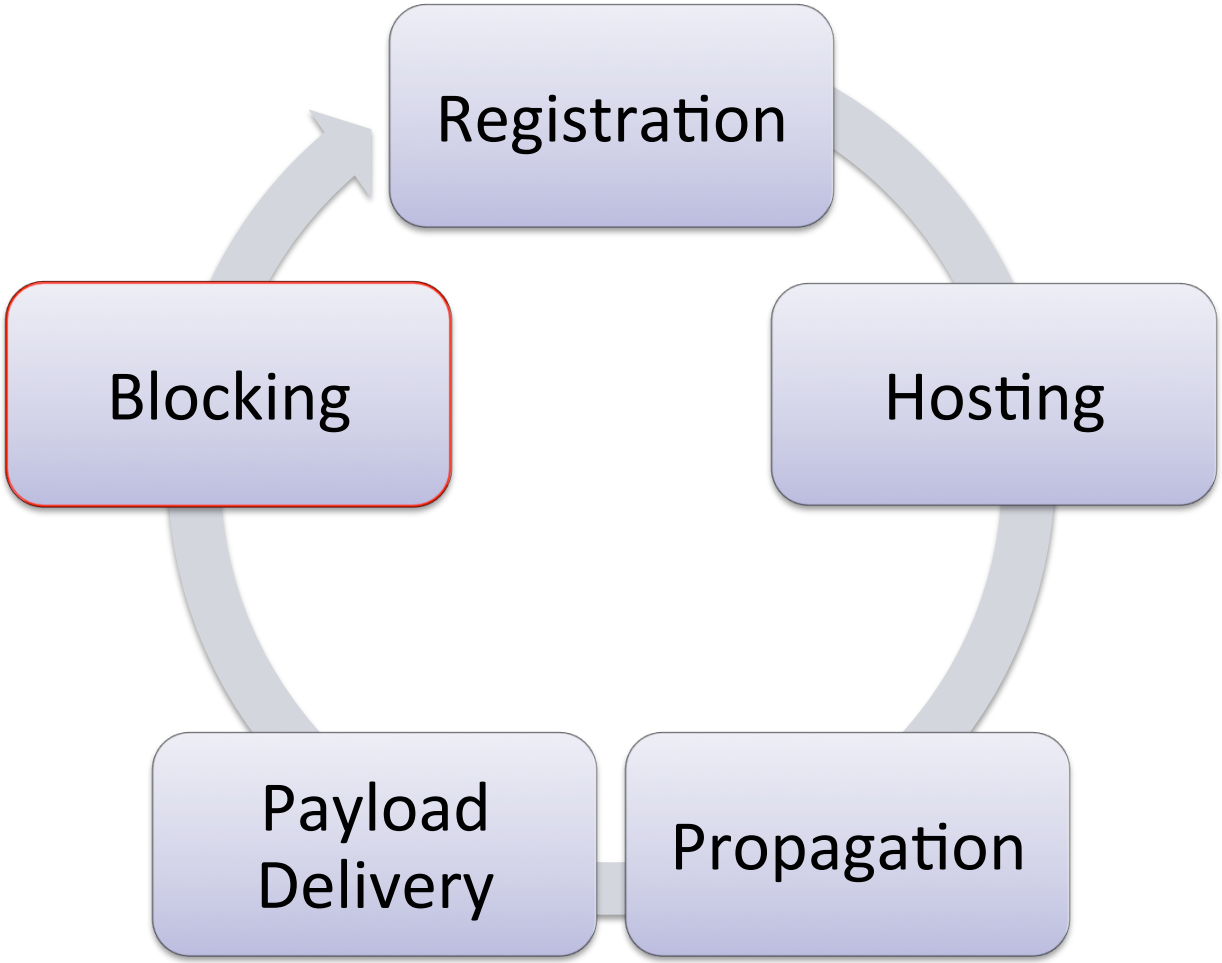


FARSIGHT SECURITY

Using Passive DNS to Mitigate Abusive Domain Registration

Henry Stern <stern@fsi.io>
Senior Distributed Systems Engineer
Farsight Security, Inc.

Malicious Domain Name Life Cycle



Fresh Domains in Spam

LifePfizer Media

To: ek@nymo.us

Virtual shop with real discounts

Stunning online offer! Up to 75% off!
http://ek.doctorbyqg.ru/?398F16

RRset results for ***.doctorbyqg.ru/ANY**

Returned 199 RRsets in 0.32 seconds.

bailiwick	**doctorbyqg.ru.**
count	16
first seen	2014-05-31 06:52:02 -0000
last seen	2014-06-01 06:13:42 -0000

doctorbyqg.ru.	A	189.197.62.149

NS **ns2.dedicruey.su.**

doctorbyqg.ru.	NS	ns2.dedicruey.su.
doctorbyqg.ru.	NS	ns1.serverybsx.com.

bailiwick	**doctorbyqg.ru.**
count	1
first seen	2014-05-31 07:18:25 -0000
last seen	2014-05-31 07:18:25 -0000

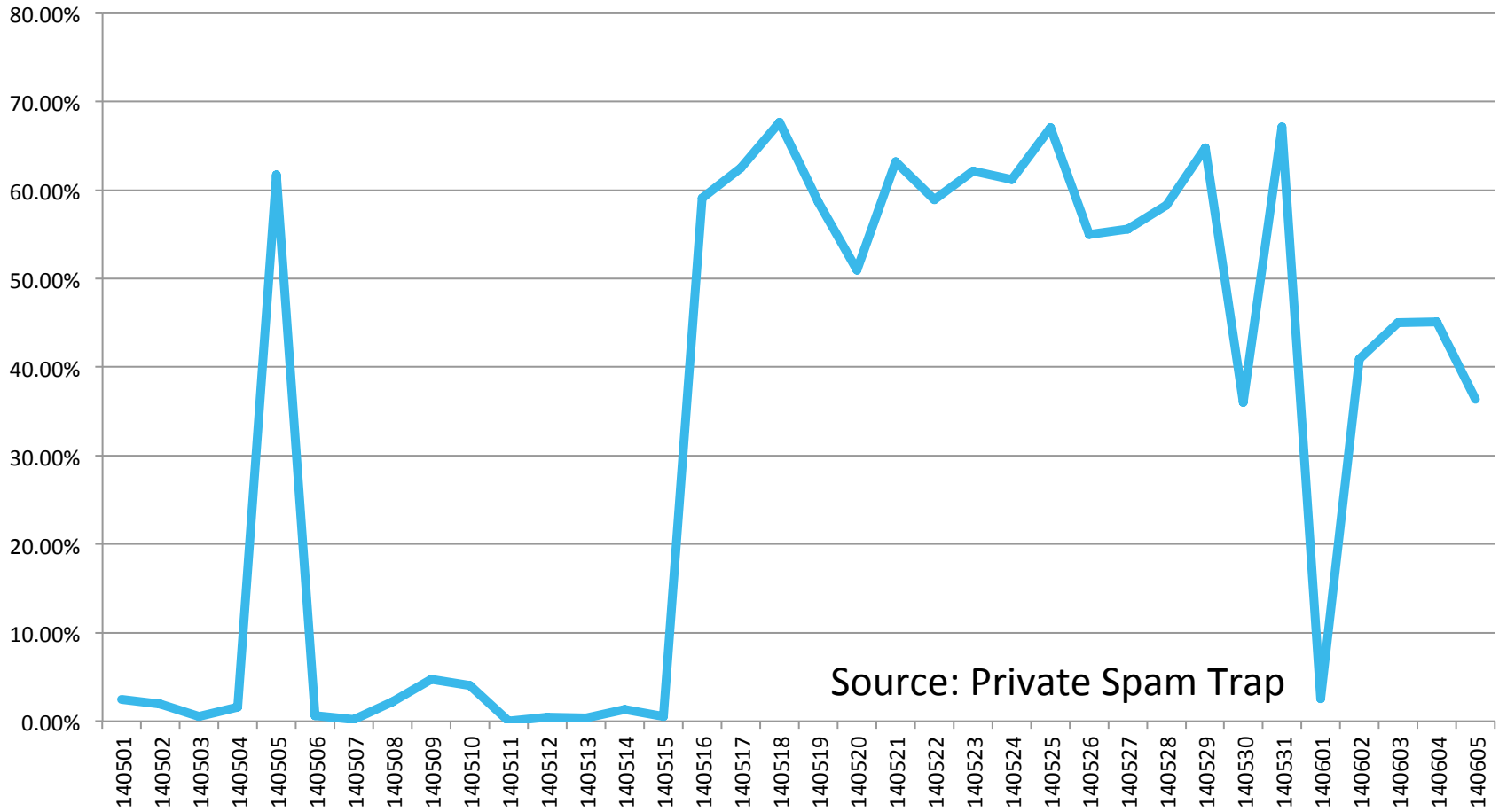
b5.doctorbyqg.ru.	A	189.197.62.149

Rdata results for **ANY/ns2.dedicruey.su.**

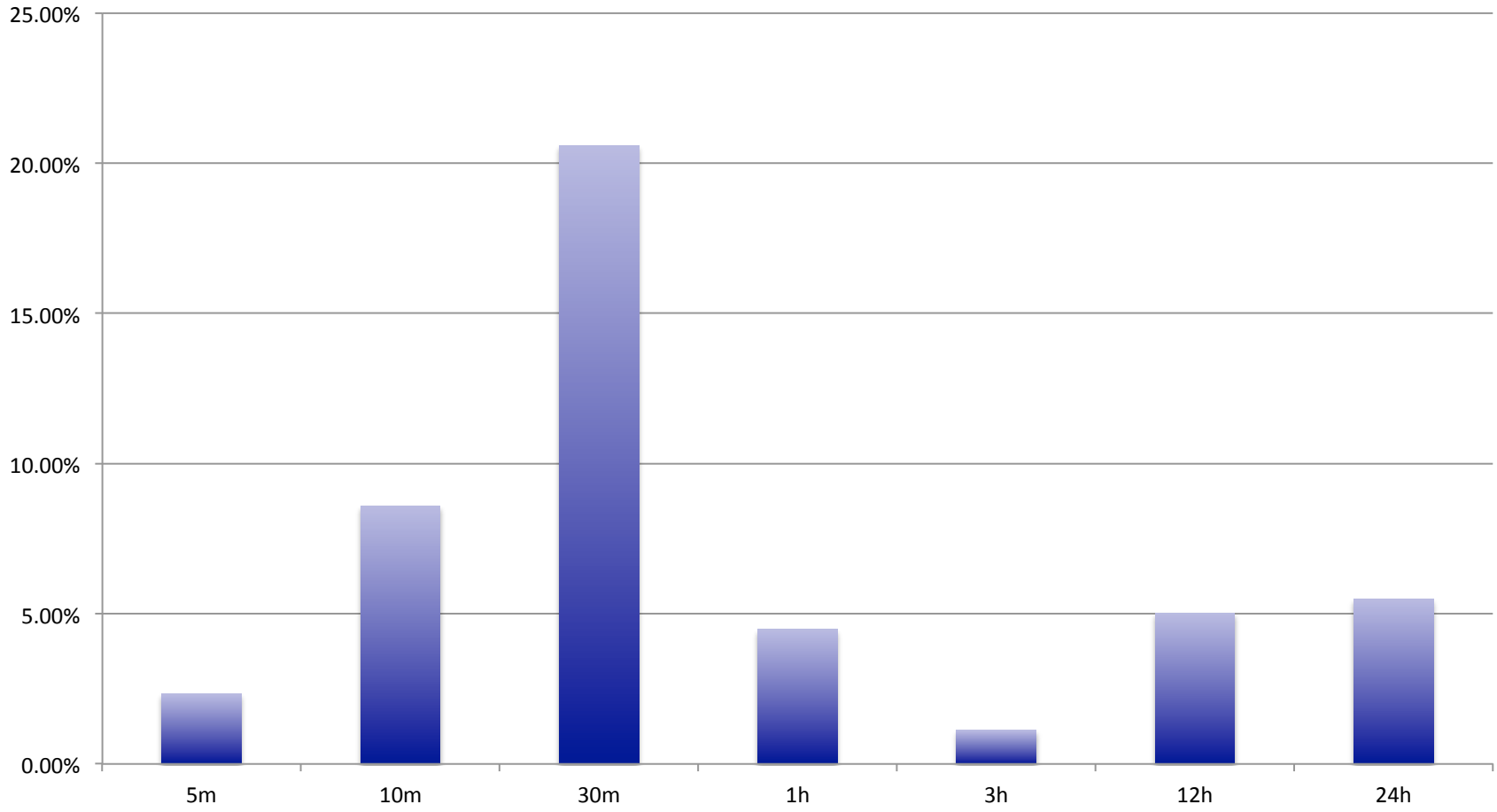
Returned 91 RRs in 0.57 seconds.

doctoraqcr.ru.	NS	ns2.dedicruey.su.
doctoratld.ru.	NS	ns2.dedicruey.su.
doctorazag.ru.	NS	ns2.dedicruey.su.
doctorbdpb.ru.	NS	ns2.dedicruey.su.
doctorbgmx.ru.	NS	ns2.dedicruey.su.
doctorblrt.ru.	NS	ns2.dedicruey.su.
doctorbqym.ru.	NS	ns2.dedicruey.su.
doctorbxhn.ru.	NS	ns2.dedicruey.su.
doctorbyqg.ru.	NS	ns2.dedicruey.su.
doctorcewl.ru.	NS	ns2.dedicruey.su.
doctorcfga.ru.	NS	ns2.dedicruey.su.
doctorcmdd.ru.	NS	ns2.dedicruey.su.
doctorcwnb.ru.	NS	ns2.dedicruey.su.
doctorcxat.ru.	NS	ns2.dedicruey.su.
doctordbxv.ru.	NS	ns2.dedicruey.su.
doctorddsp.ru.	NS	ns2.dedicruey.su.
doctordeuv.ru.	NS	ns2.dedicruey.su.

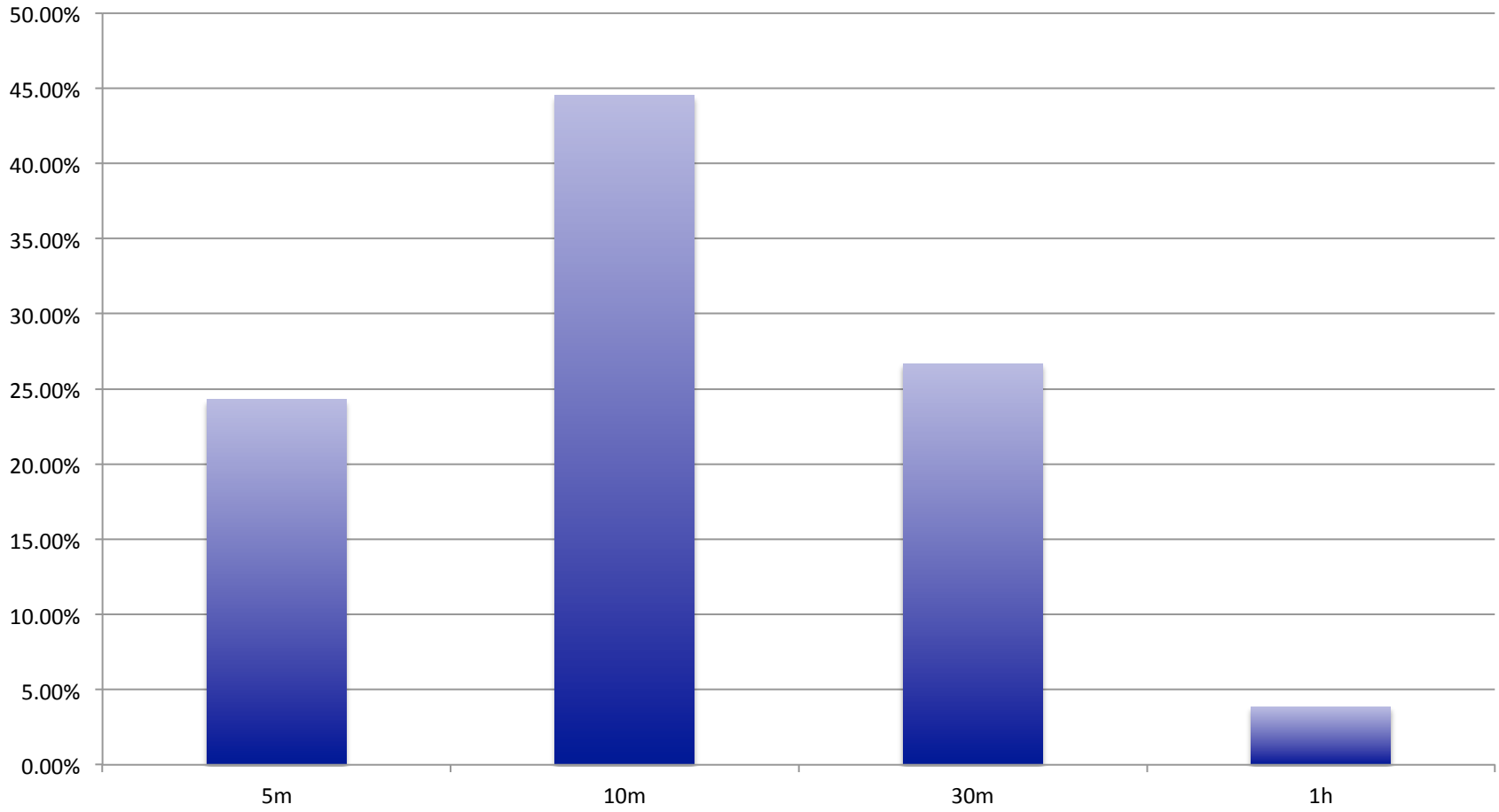
Percentage of Spam with Domains Less than 24h Old, by Date



Age of Domain Names in Spam



Distribution of Domain Age



Anti-Abuse Pain Point

- 10% of spam messages use domain names less than 10 minutes old.
- Boosts spam catch rate on domain names <5 minutes old by 20%.

What About Zone File Access?

- Snapshot in time from the zone's authoritative name server.
- Only tells of new delegation points.
- Not available for most CCTLDs.
- Only available to public every 24 hours.

Using Passive DNS Instead

- Farsight DNSDB.

  `https://www.dnsdb.info/`
- Historical database of 350 million known domain names, 7 billion hostnames.
- Detecting 50k new domain names per day.

What Farsight is Doing About It

- Publishing a DNSBL, several DNS RPZs of domain names first observed less than 24 hours ago.

  domain`.v1.bl.dns-nod.net`

- ZFA-like dumps from passive DNS.
  - Resource records from authoritative name servers for the zone.

Why This is (Part of) the Wrong Approach

- All domains, even legitimate ones, will be penalized by NOD's subscribers.
- Up-front accountability would prevent this junk at lower total cost.
- The need and demand for NOD should embarrass the whole DNS industry.

What's the Right Approach for Registries?

- Improve accountability for new domains.
  - Credit cards, whois, identity.
- Offer ZFA, including deltas, for all TLD's.
  - Even CCTLD's.
- Improve takedown procedures.
  - Consider APWG's API/process for this.
- Consider putting new domains in "pause."
- Limit NS changes to one per day.
  - Exceptions only by phone.

https://www.farsightsecurity.com/
https://www.dnsdb.info/