Authoritative DNS centralization

The effects on threat hunting and domain/DNS reputation

SPAMHAUS

(No horses were harmed for this presentation)

01 Setting the stage

Let's make sure we're all talking about the same thing

'Big Auth'

For this exploration we're looking at two categories:

Registrar authoritative DNS - Free or paid-for ('premium') authoritative NS provided by the registrar where a domain is bought.

Cloud authoritative DNS - Free or paid-for authoritative NS operated by a number of cloud service providers - some of which only do auth DNS.

Malicious or fraudulent domain registrations

Domains registered by miscreants for the sole purpose of supporting malicious activities, such as:

- Phishing
- Malware distribution (including ransomware)
- Spam
- Botnet C2

DNS Centralization

We know that an increasing number of end users are using a couple of very large resolvers, for various reasons.

This centralization effect is also clearly visible on the authoritative side.

02 Authoritative centralization

Is this happening for bad domains as well?

'Big Auth'

For this exploration we're looking at two categories:

Registrar authoritative DNS - Free or paid-for ('premium') authoritative NS provided by the registrar where a domain is bought.

Cloud authoritative DNS - Free or paid-for authoritative NS operated by a number of cloud service providers - some of which only do auth DNS.

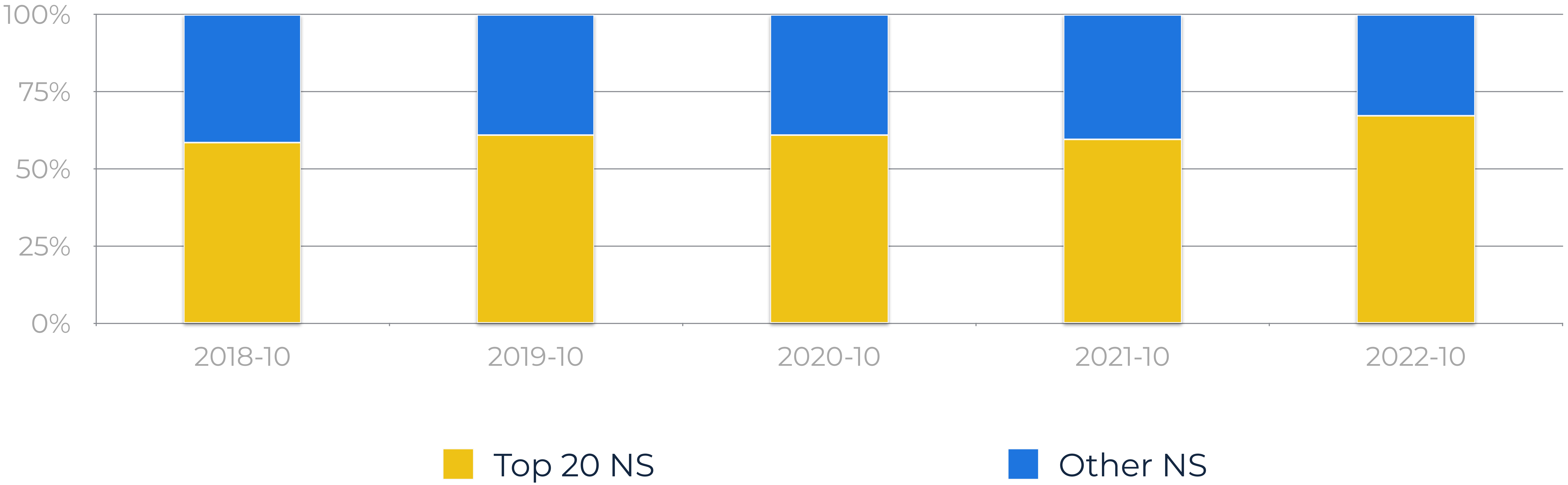
Malicious authoritative NS

An Authoritative nameserver fully operated and controlled by miscreants.

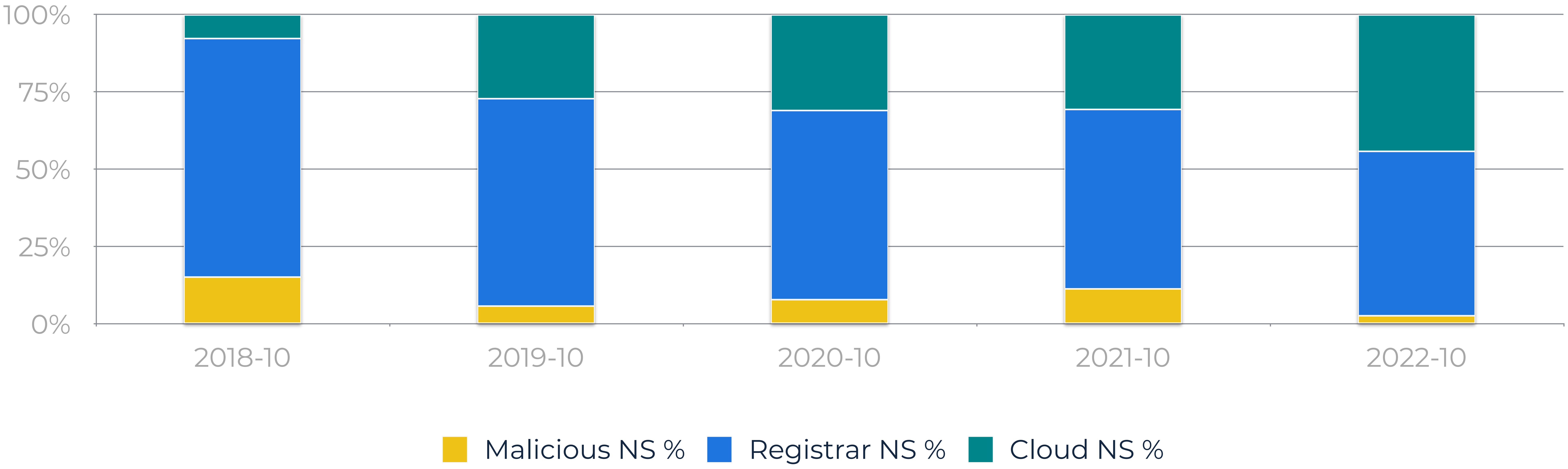
Every domain using this authoritative NS is bad.

Comes in many shapes and sizes. Can be hosted on good or bad networks.

% Of bad reputation domains served by top 20 NS



Classifying the top 20 NS for bad reputation domains



Some observations (1)

A lot of the gain in the cloud category is amongst providers that offer a free tier.

Popular registrar authoritative NS'es for bad domains are found at the lower end of the market.

Almost all large domain volume abuse has moved to shared infrastructure.

Some observations (2)

Bad reputation domain names seem to do even more centralization than good ones.

We have seen the reputation of the most used registrar and cloud authoritative NS'es drift towards bad due to the amount of low and bad reputation domains.

03 Malicious NS

The what and why

Fast flux & double fast flux

Fast flux NS is used to rapidly cycle through possible A-record answers. Often multiple are provided with very short (<60s) TTLs.

Double fast flux: the authoritative NS rotates as well!

Many self-serve NS'es on 1 IP address

```
badthings.horse          IN NS       ns1.badthings.horse
```

ns1.badthings.horse	192.0.2.1
ns1.worsethings.horse	192.0.2.1
ns1.theworstofthings.horse	192.0.2.1
ns1. ... .horse	192.0.2.1

Multiple miscreant domains on one NS

badthings.horse	IN NS	ns1.noapple.horse
worsethings.horse	IN NS	ns1.noapple.horse
theworstofthings.horse	IN NS	ns1.noapple.horse
… .horse	IN NS	ns1.noapple.horse

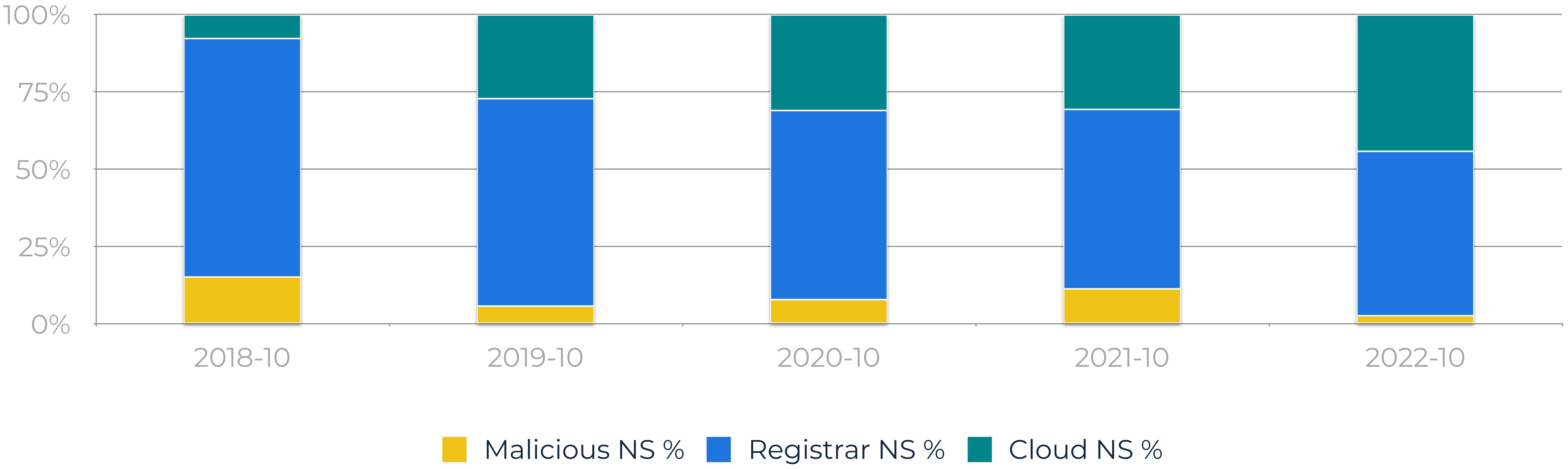
Running your own NS brings flexibility

Easy (and/or automated) zone management to quickly adapt in case of changing circumstances.

Easy domain management: newly bought domains added with tooling.

Compare: web interface @ registrar!

But Malicious NS % is in decline!



BigAuth in 2022…

All big players (registrar and cloud) offer APIs for zone and domain management. This can easily replace any homegrown solution for bulk domain management.

Added bonuses for malicious operators (1)

Human shields: Now your bad domains are mixed with good ones.

Added bonuses for malicious operators (2)

Some level of anonymity.

Added bonuses for malicious operators (3)

It's someone else's computer.

Which is sometimes even free to use!

04 Hunting & Investigations

Here be dragons?

When you come across a domain name…

Does it uniquely belong to the adversary?

If so, are there more?

When you come across a domain name...

Does it uniquely belong to the adversary?

If so, are there more?

vichavoliken.horse	← Used Nov. 8
chaffrontain.horse	← Used Nov. 10
carbonapart.horse	← Not used yet!

DNS can be a time machine

Due to the fact that domains need to be registered before they can be used, there is an opportunity for defenders to find out future miscreant infrastructure.

DNS can be a time machine

Due to the fact that domains need to be registered before they can be used, there is an **opportunity for defenders to find out future miscreant infrastructure**.

DNS can be a time machine

Due to the fact that domains need to be registered before they can be used, there is an **opportunity for defenders to find out future miscreant infrastructure**.

vichavoliken.horse	← Used Nov. 8
chaffrontain.horse	← Used Nov. 10
carbonapart.horse	← Not used yet!

Remember the dead...

The data that used to be abundant in domain registration records (aka WHOIS) has largely gone dark. Correlation became harder.

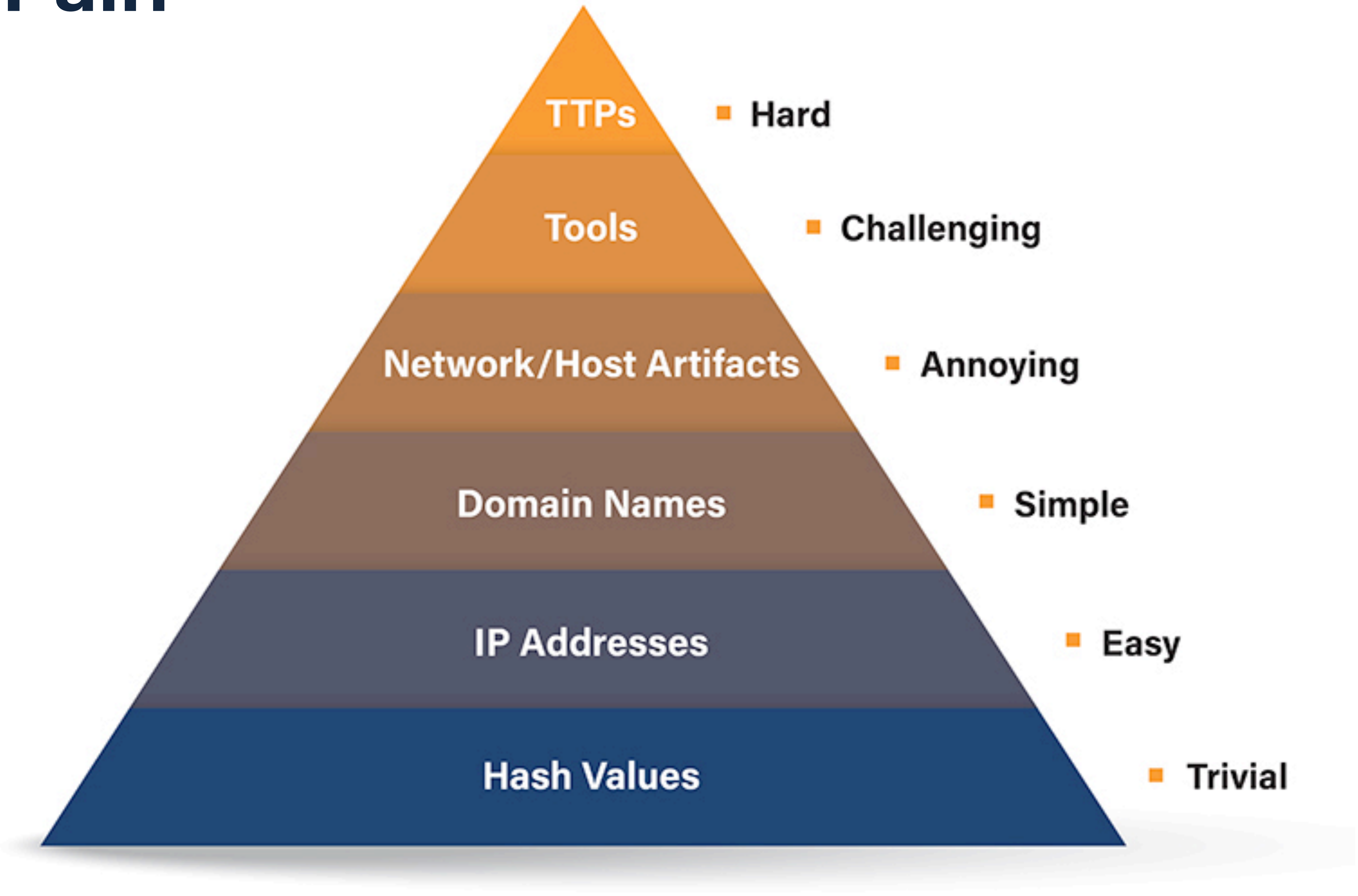
(Expedited Policy Development Process anyone?)

Auth DNS Centralization makes clustering even harder

Passive DNS dumps of shared registrar/cloud infrastructure can be massive.

That needle now becomes a lot harder to find.

Pyramid of Pain



Something good?

Centralization lowers the amount of responsible parties, which may make takedowns easier.

However, if you're not carrying a gun and a badge, this remains to be seen.

Thank you!

carel@spamhaus.org

www.spamhaus.org