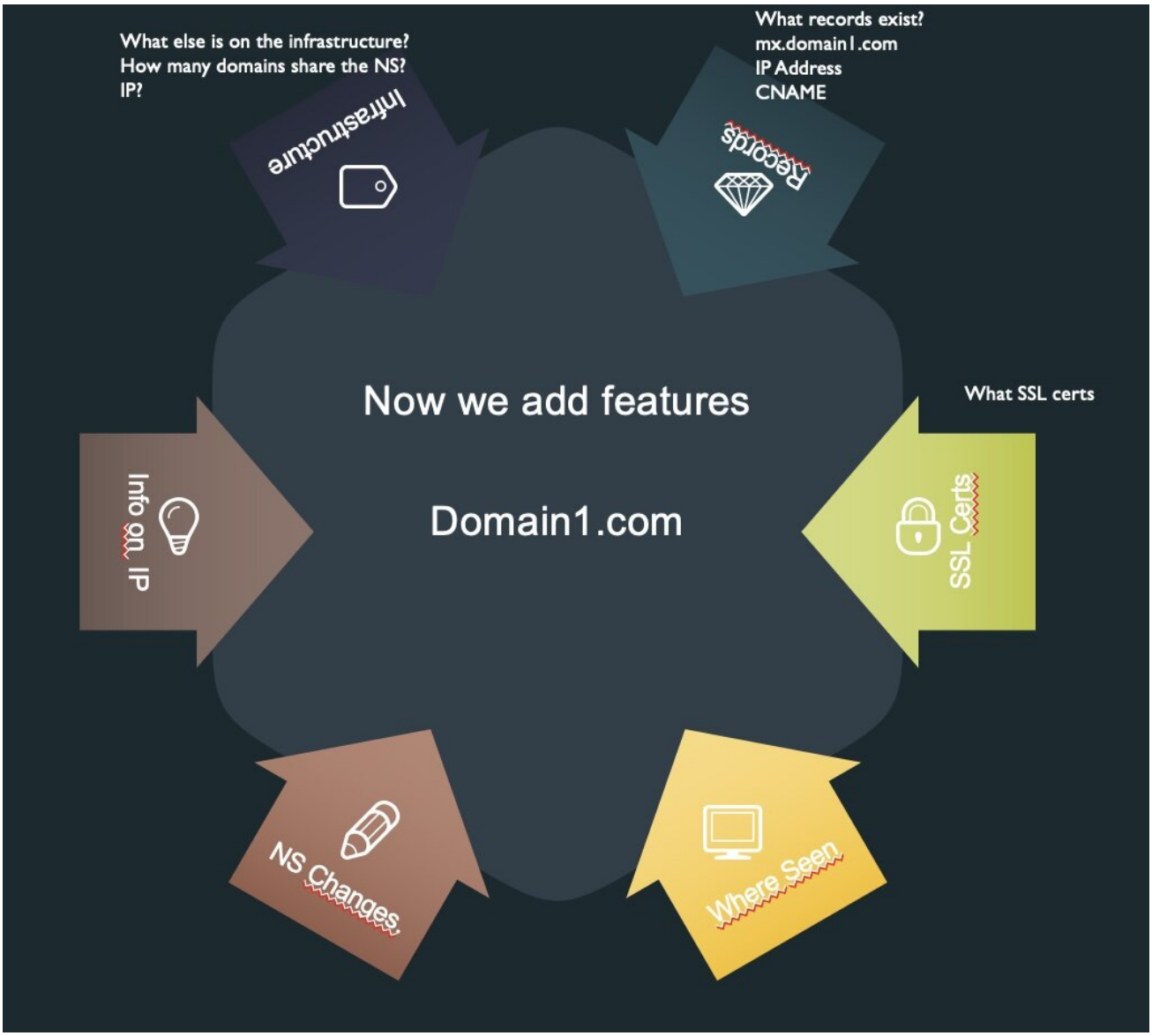
Behavior Clustering just got easier using new characteristics.

silentpush.com/blog/behavior-clustering-just-got-easier-using-new-characteristics

April 25, 2021

Threat HuntingThreat Intelligence
Apr 25
Written By Ken Bagnall

First Published February 5th 2021 by Ken



Intelligence Analysts as well as Security Analysts lost a lot of information when GDPR changed the content of WHOIS information by obscuring claimed registrant details.

In order to expand some characteristics to help build attacker TTP profiles and do threat hunting and behavior clustering, some new elements need to be added to the actor profile whether it is around their infrastructure or assets.

We have started to expand these characteristics in order to make the threat hunters and Intelligence Analysts job easier to build a profile and we will briefly explain some of the new attributes and characteristics below.

This explanation is also useful to our users as our concept of a large composite indicator includes these data points.

The characteristics are:
Domain/Name Server Entropy- Combining information about number of changes, time of changes and types of changes across Name-Servers for a domain. This is quite a complex construction and each of the underlying elements is also available separately in our API. Certain types of changes take on a higher weighting than others when constructing the final risk score.

Name Server Density- This is simply the number of domains we see hosted on this nameserver. The nameserver density can be an important factor in tracking particular types of campaigns. Some examples of that are mentioned in this post about single domain name servers towards the end of the page.

Name Server Reputation(listed domains in last 30 days/number of domains on name server) This is a characteristic of recent known malicious activity on a given Name-Server relative to the number of domains on the Name-Server.

IP Reputation can be divided into contributing factors of:

AS Rank- various forms of this have been available over the years in OSINT this is just our own variant

to rank the AS numbers by malicious activity.

AS Reputation- simple calculation of recent malicious activity relative to size of the IP block

AS Takedown Reputation- a complex algorithm to give an impression of how long malicious items

survive in an IP block

AS Assignment Age- how long this IP has been assigned to this AS Number

AS Size- how many IP addresses in this block

Subnet Reputation- also number of malicious times associated with the IP subnet in recent time.

IP Density (Number of A records we see on that IP address)

IP History- (Number of listings associated with that IP address in x days)

MX Density

Number of SSL Certs on an IP

Number of reuses of each SSL Cert

Number of WHOIS changes
These can be combined in different ways to conduct research. There are also a number of starting points for this. For example if you look in the threat feeds available and pick a worrying indicator that is relevant to your organization, then build a profile based on the above characteristics plus the more regular characteristics also included in the data. You can then conduct a search over our non-threat data to see what matches come up that maybe should be added to a cluster and further investigated or blocked by network defenders.

IP Diversity

The number of A records associated with a domain over time and how they rotate through them is trace evidence of attacker process. It can also help distinguish quickly through different types of Content Delivery Networks.

Name *
Thank you!

Ken Bagnall