Infra-Tagging -a new tool in Cyber Threat Intelligence

silentpush.com/blog/infra-tagging-a-new-tool-in-cyber-threat-intelligence

June 15, 2021

Jun 15

Written By Ken Bagnall

Working with Intelligence Analysts as well as SOC teams over many years has led us to identify pain points that just seemed solvable with a little thought. A couple of these can be helped enormously by “Infra-Tagging”. It’s a new term so just go with it for now while I explain.

The problem: I’m looking at a bunch of domains and want to see how they are related. There are many different ways to do this and each involves numerous look-ups and then saving the results to compare them.

This is where Infra Tagging steps in. We just do one API call for each domain to generate an Infra-tag. The tag will be of the form {mx.ns.as.reg} where MX= the domain portion of the first mail exchange record in DNS, NS= the domain portion of the top last seen Name Server, AS= the AS name of the assigned IP address of the A record, Reg- the registrar mentioned in Whois if available. If any field is unavailable it is replaced with a _.

This results in something like the below

Example 1

API

https://api.silentpush.com/api/v1/merge-api/explore/domain/infratag/zicanotes[.]com

Result

"tag": "_:dns.com:cnservers:key-systemsgmbh"

Example 2

So lets try this for a particular bunch of domains from a related campaign.

"domain": "dimetriadit[.]top", "tag": "**_:cloudflare.com:hz:porkbunllc**"

"domain": "glooverdoover[.]top", "tag": "**porkbun.com:cloudflare.com:hz:porkbunllc**"

"domain": "sillkolo[.]space", "tag": "**porkbun.com:cloudflare.com:hz:_**"

"domain": "woodabeg[.]fun", "tag": "**porkbun.com:cloudflare.com:hz:porkbunllc**"

These domains are related to IcedID infrastructure

Having this tag alongside each domain in your security tools is very useful as any analyst has a chance of being able to spot trends with a glance.

However there are even greater advantages such as being able to search for tags in data. That means we can do this in a couple of places.

1. Search for similar tags in threat feeds and see which items may be related.
2. Search in Passive/Active DNS to see what else is out there with the same Infra-Tag and similar

Would you like to use our Infra-Tags API? Would you like to help us make tools like this for you.

Please contact us to join our Beta program.

Name *
Thank you!

Ken Bagnall