Information Gathering as a Researcher: a use case

silentpush.com/blog/information-gathering-as-a-researcher-use-case

April 29, 2021

Threat HuntingReconaissance
Apr 29
Written By Ken Bagnall

Author: Mahesh Tata First Published 29th April 2021

Mahesh Tata works as a penetration tester. We asked him to try the Silent Push service to see how it could help him and his team to get their work done quicker. This is written in Mahesh's own words and only uses one of our features, DNS Explore.

Reconnaissance

Reconnaissance is performed to gain as much information on the target before beginning the penetration testing. 'Recon' is an essential element of any penetration testing. Recon on a target can be done in two ways: passive and active reconnaissance.

During the recon process researchers try to collect information about the subdomains associated with the target and their respective IP address. Most of today's applications are protected using WAFs and CDNs and it is often challenging to identify the real IP address associated with an application. That is where the subdomains associated with the application help researchers get more information about the main application and expand the attack surface.

The Silent Push application can be used for passive reconnaissance quickly.

Case Study :

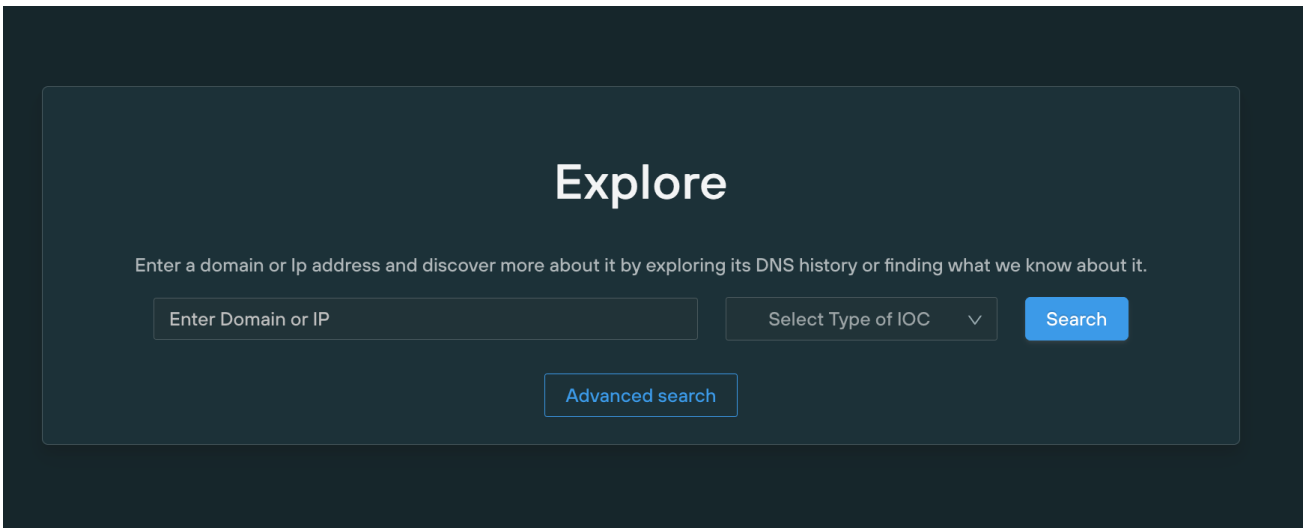
Domain : magicbricks.com

For the past few years I have been testing web applications and spend around 2 to 5 days on collecting the information about each target. The information that I collect includes all the domains that are associated with the company and their respective subdomains and IP addresses and information about the OS.

There are different search engines available for collections of the above information but there is no single place where we can find more information at a time.

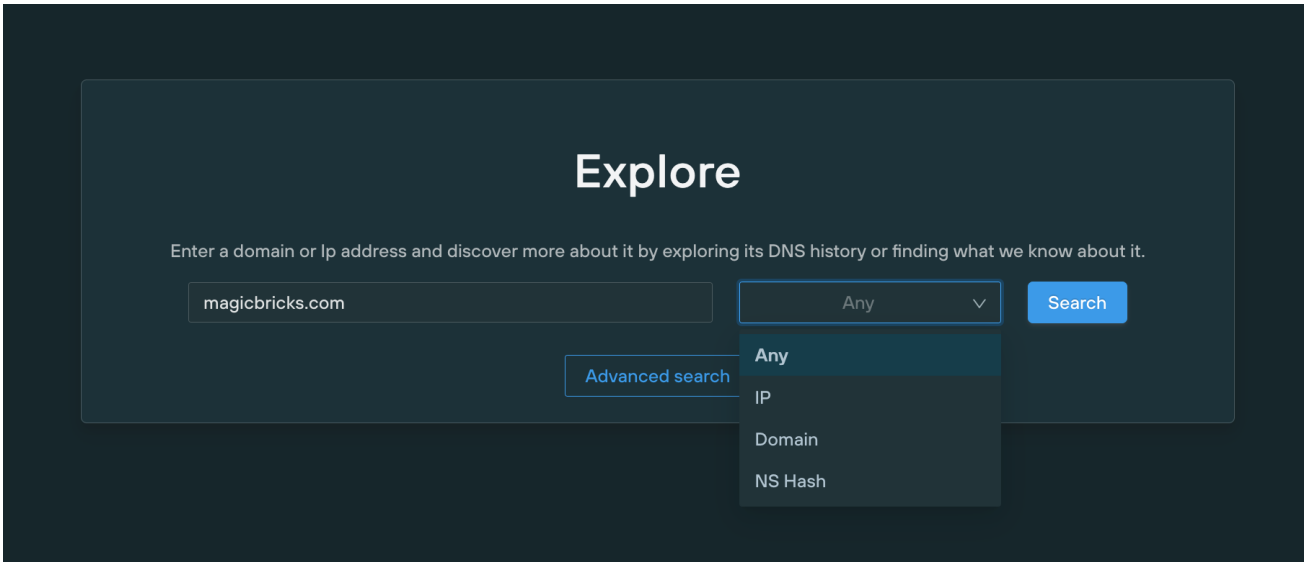
I have worked on the application mentioned above a couple of months back and was not able to collect more information. Then I gave it a try with Silent Push and the information i gathered was just done in a few minutes, normally it will take me a few days to get that information from different sources.

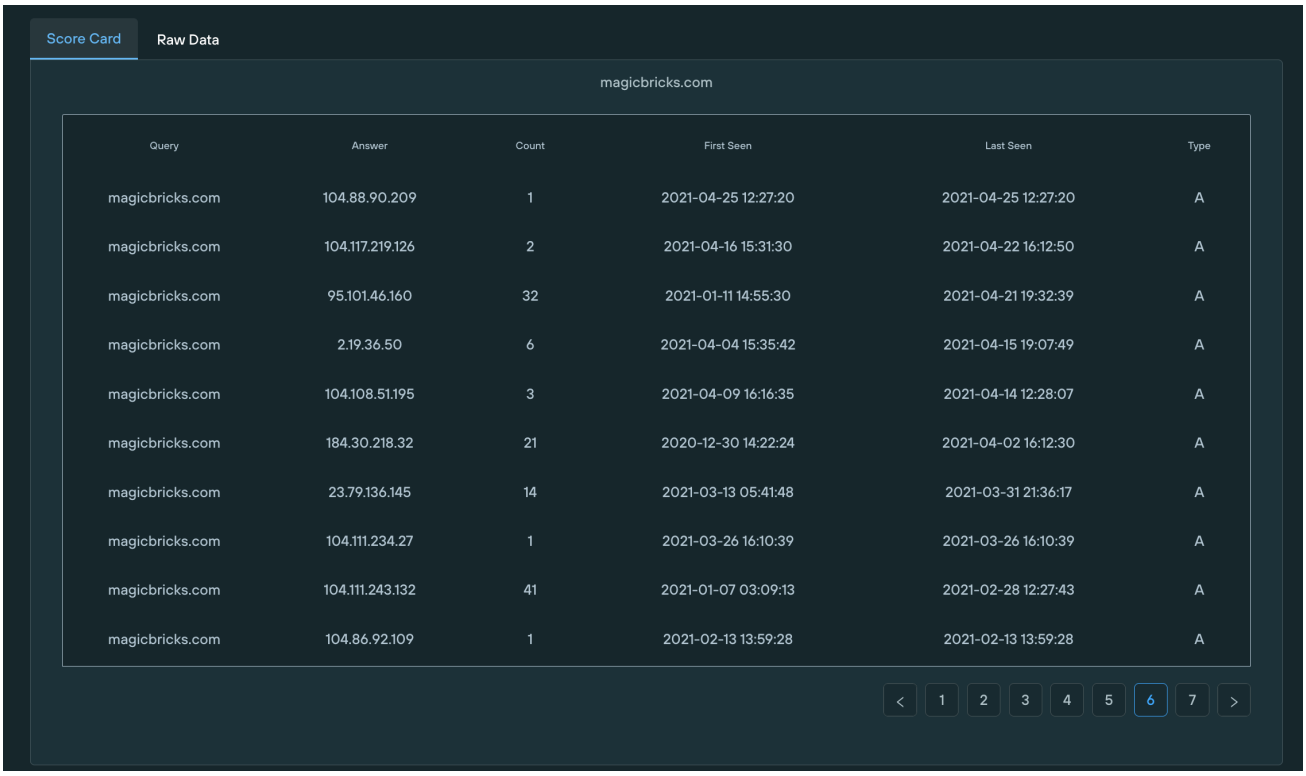
I started by using their Explore DNS feature which accepts wildcards.



Explore DNS history using wildcards proved very powerful

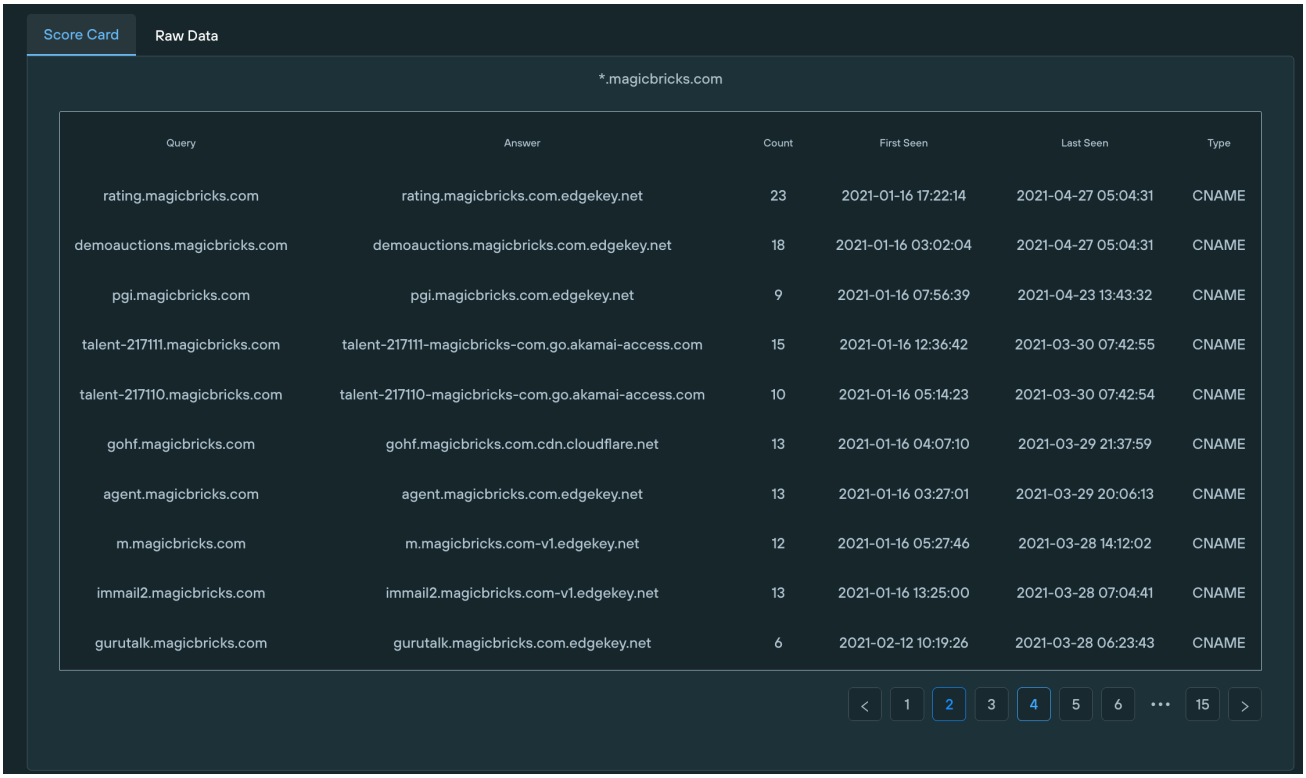
I first searched for Any records associated with the test domain.





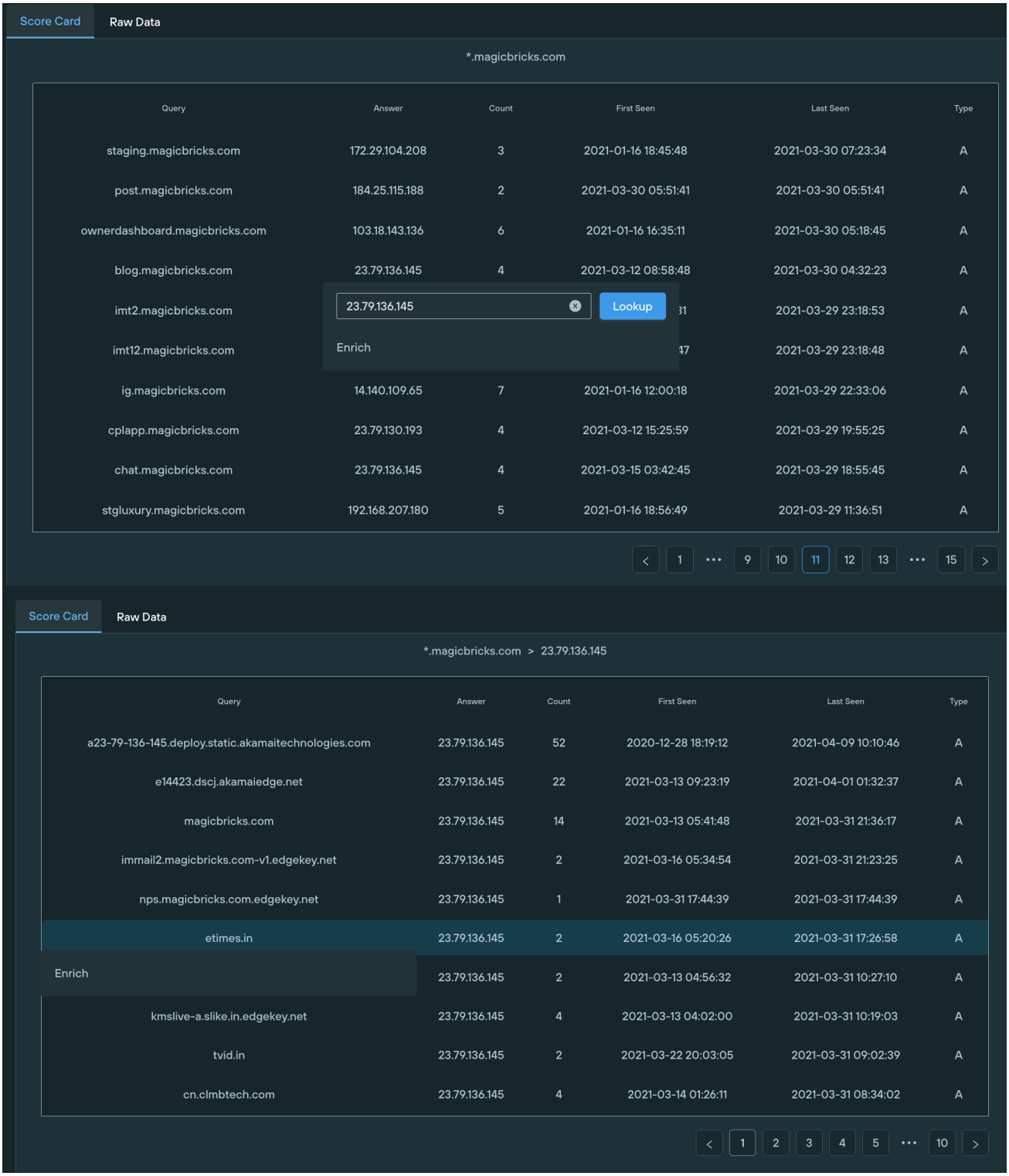
Gathering all the DNS information in one place using Silent Push's explore feature

I then realized I could use a wildcard and gather subdomains and see what CNAME records were gathered and what IPs subdomains were using.



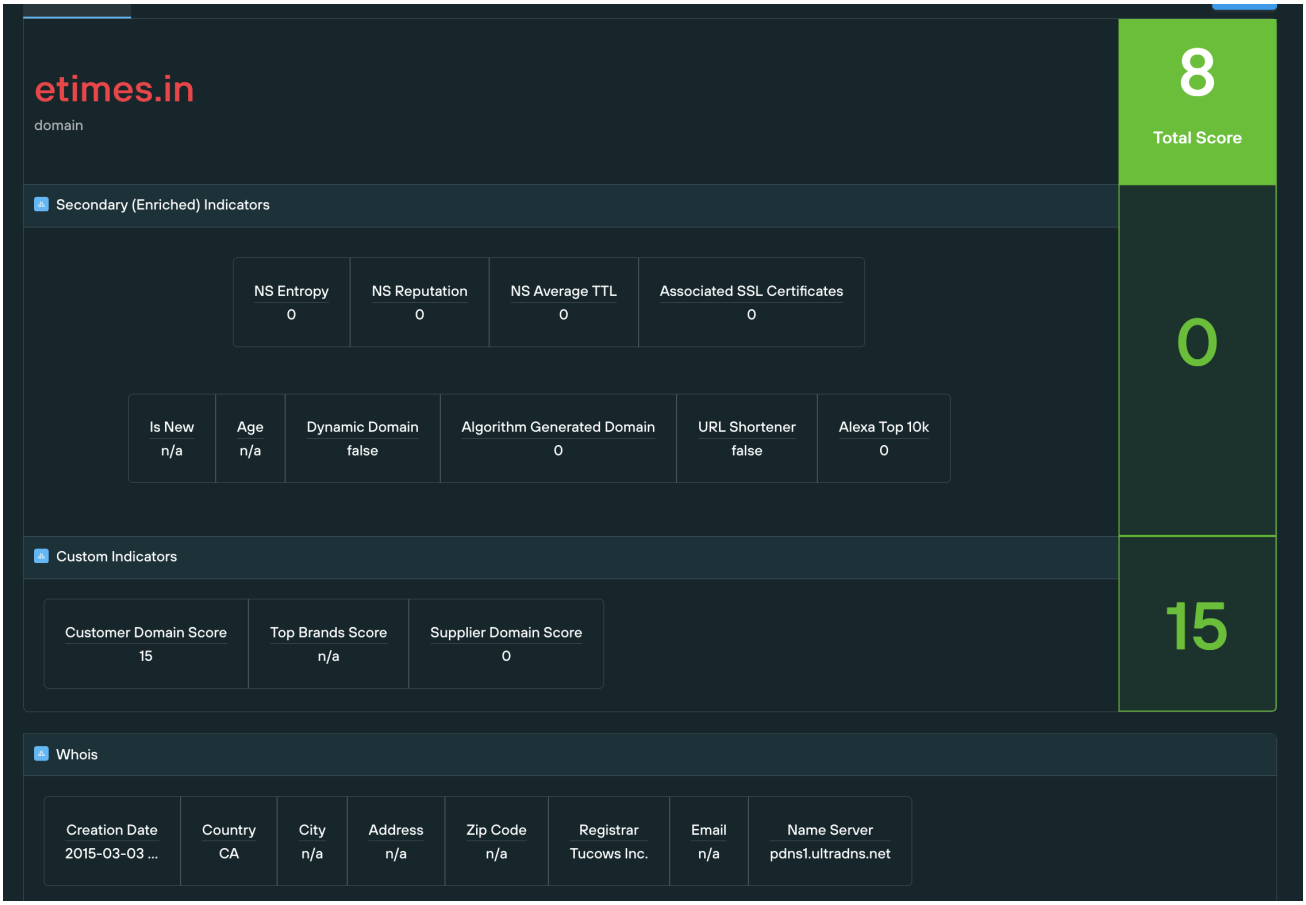
Gathering all subdomain info using a wildcard

This allowed me to pivot off this information and see what else was pointed to the same infrastructure.



I could see all A records pointing to the same IP straight away

I could enrich that information to find out more about 'the neighbours' and see what sort of reputation was associated with them.



This looked like a clean domain

So in conclusion, even though I am not on a threat intelligence team, the simple data gathering capabilities of this part of the Silent Push application saved me enormous amounts of time. Quite literally this saves me days per job. The use cases across entire security teams is tremendous.

Subscribe

Sign up with your email address to receive news and updates.

We respect your privacy.

Thank you!

Ken Bagnall