

# Information Gathering as a Researcher: a use case

---

 [silentpush.com/blog/information-gathering-as-a-researcher-use-case](https://silentpush.com/blog/information-gathering-as-a-researcher-use-case)

April 29, 2021



## Threat Hunting Reconnaissance

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 :

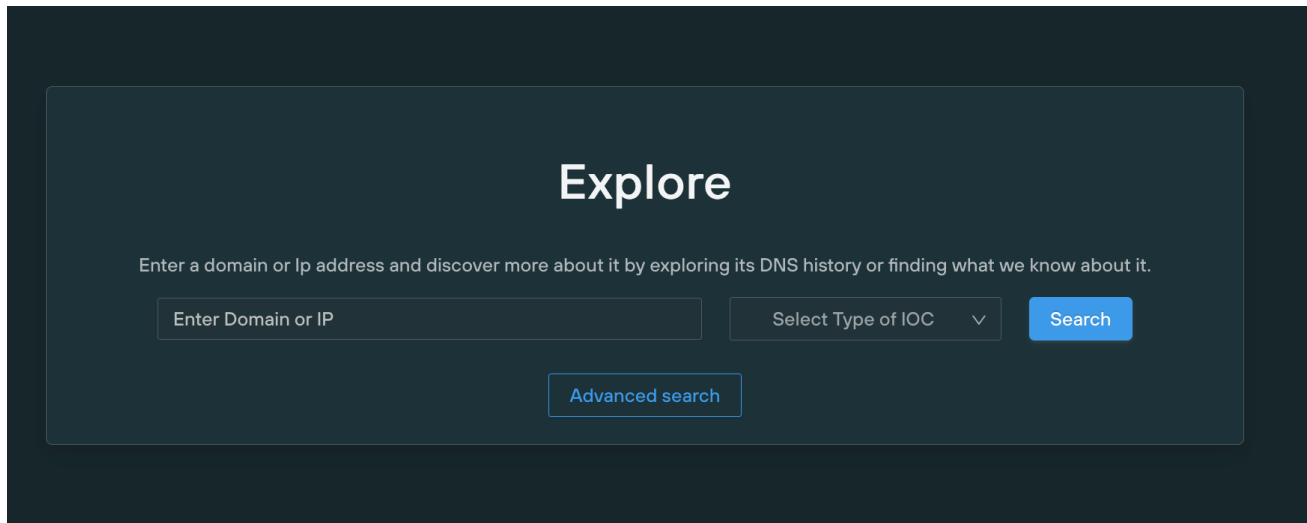
Domain : magicbricks.com

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.

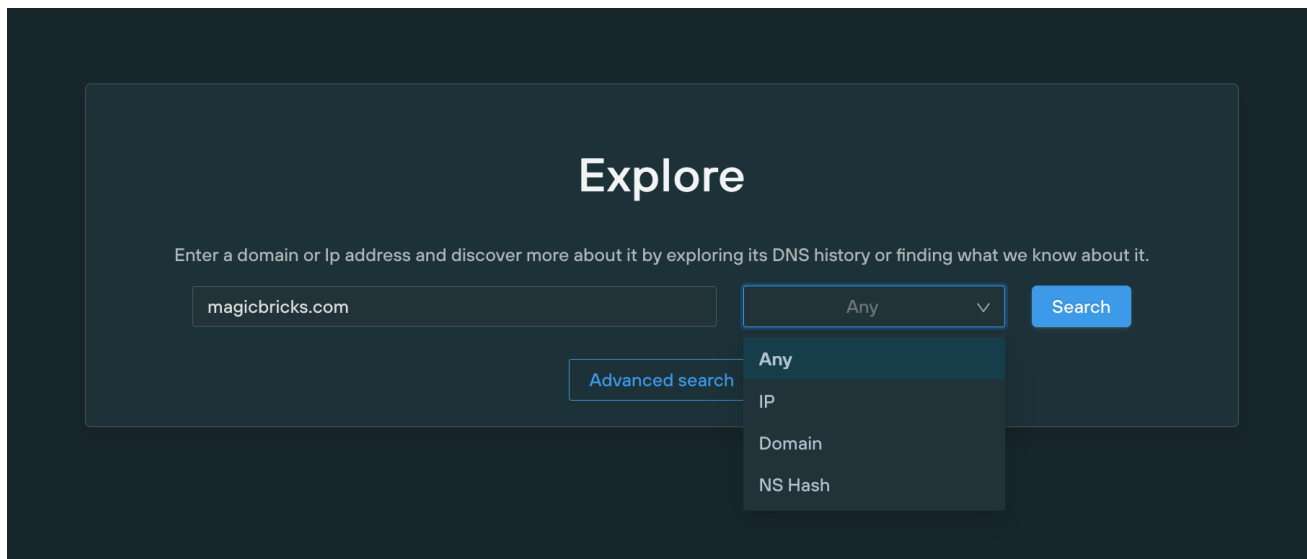
I have worked on the application mentioned above a couple of months back and was not able to collect more information. Then I gave it a try with Silent Push and the information gathered was just done in a few minutes, normally it will take me a few days to get that information from different sources.

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.



Query	Answer	Count	First Seen	Last Seen	Type
magicbricks.com	104.88.90.209	1	2021-04-25 12:27:20	2021-04-25 12:27:20	A
magicbricks.com	104.117.219.126	2	2021-04-16 15:31:30	2021-04-22 16:12:50	A
magicbricks.com	95.101.46.160	32	2021-01-11 14:55:30	2021-04-21 19:32:39	A
magicbricks.com	2.19.36.50	6	2021-04-04 15:35:42	2021-04-15 19:07:49	A
magicbricks.com	104.108.51.195	3	2021-04-09 16:16:35	2021-04-14 12:28:07	A
magicbricks.com	184.30.218.32	21	2020-12-30 14:22:24	2021-04-02 16:12:30	A
magicbricks.com	23.79.136.145	14	2021-03-13 05:41:48	2021-03-31 21:36:17	A
magicbricks.com	104.111.234.27	1	2021-03-26 16:10:39	2021-03-26 16:10:39	A
magicbricks.com	104.111.243.132	41	2021-01-07 03:09:13	2021-02-28 12:27:43	A
magicbricks.com	104.86.92.109	1	2021-02-13 13:59:28	2021-02-13 13:59:28	A

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.

Query	Answer	Count	First Seen	Last Seen	Type
rating.magicbricks.com	rating.magicbricks.com.edgekey.net	23	2021-01-16 17:22:14	2021-04-27 05:04:31	CNAME
demoauctions.magicbricks.com	demoauctions.magicbricks.com.edgekey.net	18	2021-01-16 03:02:04	2021-04-27 05:04:31	CNAME
pgi.magicbricks.com	pgi.magicbricks.com.edgekey.net	9	2021-01-16 07:56:39	2021-04-23 13:43:32	CNAME
talent-217111.magicbricks.com	talent-217111-magicbricks-com.go.akamai-access.com	15	2021-01-16 12:36:42	2021-03-30 07:42:55	CNAME
talent-217110.magicbricks.com	talent-217110-magicbricks-com.go.akamai-access.com	10	2021-01-16 05:14:23	2021-03-30 07:42:54	CNAME
gohf.magicbricks.com	gohf.magicbricks.com.cdn.cloudflare.net	13	2021-01-16 04:07:10	2021-03-29 21:37:59	CNAME
agent.magicbricks.com	agent.magicbricks.com.edgekey.net	13	2021-01-16 03:27:01	2021-03-29 20:06:13	CNAME
m.magicbricks.com	m.magicbricks.com-v1.edgekey.net	12	2021-01-16 05:27:46	2021-03-28 14:12:02	CNAME
immail2.magicbricks.com	immail2.magicbricks.com-v1.edgekey.net	13	2021-01-16 13:25:00	2021-03-28 07:04:41	CNAME
gurutalk.magicbricks.com	gurutalk.magicbricks.com.edgekey.net	6	2021-02-12 10:19:26	2021-03-28 06:23:43	CNAME

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.

The image shows two screenshots of a network analysis tool interface. The top screenshot displays a table of DNS records for the domain \*.magicbricks.com. The bottom screenshot shows the results of an enrichment query for the IP address 23.79.136.145, listing other domains that point to this IP.

Query	Answer	Count	First Seen	Last Seen	Type
staging.magicbricks.com	172.29.104.208	3	2021-01-16 18:45:48	2021-03-30 07:23:34	A
post.magicbricks.com	184.25.115.188	2	2021-03-30 05:51:41	2021-03-30 05:51:41	A
ownerdashboard.magicbricks.com	103.18.143.136	6	2021-01-16 16:35:11	2021-03-30 05:18:45	A
blog.magicbricks.com	23.79.136.145	4	2021-03-12 08:58:48	2021-03-30 04:32:23	A
imt2.magicbricks.com	23.79.136.145	31		2021-03-29 23:18:53	A
imt12.magicbricks.com	Enrich	47		2021-03-29 23:18:48	A
ig.magicbricks.com	14.140.109.65	7	2021-01-16 12:00:18	2021-03-29 22:33:06	A
cplapp.magicbricks.com	23.79.130.193	4	2021-03-12 15:25:59	2021-03-29 19:55:25	A
chat.magicbricks.com	23.79.136.145	4	2021-03-15 03:42:45	2021-03-29 18:55:45	A
stgluxury.magicbricks.com	192.168.207.180	5	2021-01-16 18:56:49	2021-03-29 11:36:51	A

Query	Answer	Count	First Seen	Last Seen	Type
a23-79-136-145.deploy.static.akamaitechnologies.com	23.79.136.145	52	2020-12-28 18:19:12	2021-04-09 10:10:46	A
e14423.dscj.akamaiedge.net	23.79.136.145	22	2021-03-13 09:23:19	2021-04-01 01:32:37	A
magicbricks.com	23.79.136.145	14	2021-03-13 05:41:48	2021-03-31 21:36:17	A
immail2.magicbricks.com-v1.edgekey.net	23.79.136.145	2	2021-03-16 05:34:54	2021-03-31 21:23:25	A
nps.magicbricks.com.edgekey.net	23.79.136.145	1	2021-03-31 17:44:39	2021-03-31 17:44:39	A
etimes.in	23.79.136.145	2	2021-03-16 05:20:26	2021-03-31 17:26:58	A
Enrich	23.79.136.145	2	2021-03-13 04:56:32	2021-03-31 10:27:10	A
kmslive-a.slike.in.edgekey.net	23.79.136.145	4	2021-03-13 04:02:00	2021-03-31 10:19:03	A
tvid.in	23.79.136.145	2	2021-03-22 20:03:05	2021-03-31 09:02:39	A
cn.cmbtech.com	23.79.136.145	4	2021-03-14 01:26:11	2021-03-31 08:34:02	A

*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.

**etimes.in**  
domain

**8**  
Total Score

Secondary (Enriched) Indicators

NS Entropy	NS Reputation	NS Average TTL	Associated SSL Certificates
0	0	0	0

Is New	Age	Dynamic Domain	Algorithm Generated Domain	URL Shortener	Alexa Top 10k
n/a	n/a	false	0	false	0

Custom Indicators

Customer Domain Score	Top Brands Score	Supplier Domain Score
15	n/a	0

Whois

Creation Date	Country	City	Address	Zip Code	Registrar	Email	Name Server
2015-03-03 ...	CA	n/a	n/a	n/a	Tucows Inc.	n/a	pdns1.ultradns.net

*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