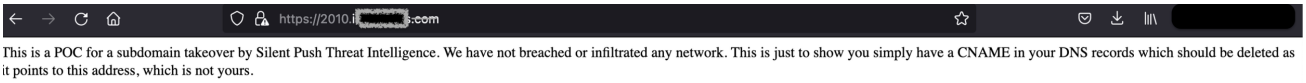
Subdomain Takeovers and 1.1 million “dangling” risks

silentpush.com/blog/subdomain-takeovers-and-other-dangling-risks

May 3, 2022

May 3
Written By The Team



Subdomain takeover proof of concept by Silent Push on an Azureedge.net target.

There have been an incredible number of very large scale data breaches lately that seemed to have unexplained entry points. Combining social engineering with “token” collection or stealing seems to be a more efficient way to gain access to customers who are heavy users of cloud based applications.

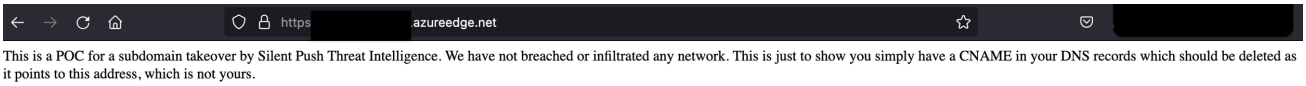
Let me begin with the most simple explanation of a subdomain takeover. Your organization owns a domain, lets say for example, it is `israwords.com.`

One day someone sets up a service using a third party, it could be anything, a wordpress site, a CDN, heroku, github. The thing is it needs you to point a subdomain at the service so it appears to be under your domain. In this case it is the Microsoft CDN which uses customername.azureedge.net .

So for this example the company put in place a CNAME record

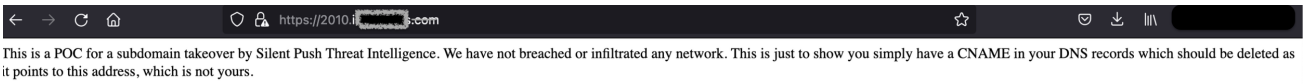
```
2010.israwords.com. 800 IN CNAME 2010israwords.azureedge.net.
```

So far so good. The organization is using this service from Microsoft Azure and any traffic for 2010.israwords.com gets redirected to the Content Delivery Network provided by Azure. However, at some point the organization changes provider or gives up on the service. At some point Microsoft will deem 2010israwords to be an unused subdomain in Azureedge.net and someone else can use it. So we did this as a Proof Of Concept.



Target dangling domain on Azure

Then, we looked up the original subdomain to see if it had worked.



Full subdomain takeover.

We would like to emphasize that we did not really take over anything for this to happen. We didn't need to. The dangling CNAME just points at something we control. However, what are the potential consequences of that?

Potential Damage

We have found 1.1 million CNAME's that are potentially vulnerable to a takeover.

We didn't want to take the Proof Of Concept any further than that but the possibilities are large. A number of them are called out on Hacker One here https://www.hackerone.com/application-security/guide-subdomain-takeovers

Loss of control over the content of the subdomain - The party controlling the endpoint could post any content they wanted there. This could be insulting to the original domain owner or malicious.

- **Session Cookie Harvesting and OAuth Tokens**- Becoming a valuable resource and one of the main vectors in modern hacking and access brokerage cookies and OAuth tokens are worth money immediately in hacker forums and can quickly escalate the access that they have.

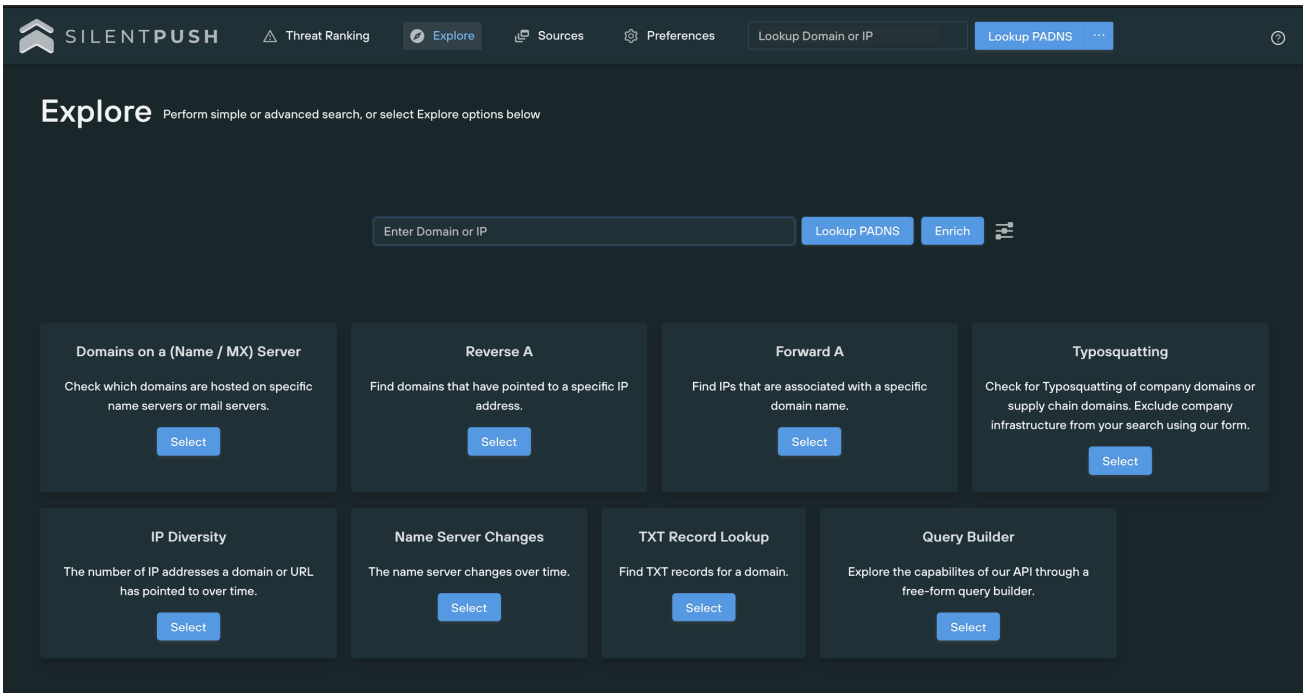
- **Phishing campaigns** - One of the main concerns resulting from subdomain take overs is Phishing campaigns targeting your staff or customers. Your staff will be very vulnerable to campaigns appearing to be on your own domain and at high risk of entering valid credentials in any forms. The reputational damage to customers would be very large if they are targeted as they will take some convincing that you didn't have a breached network when they enter their details on a site that appears on your domain.

- **Further risks** - Malicious sites might be used to escalate into other classic attacks such as XSS, CSRF, CORS bypass, and more.

How Can I Protect My Organization From Sub-Domain Takeover?

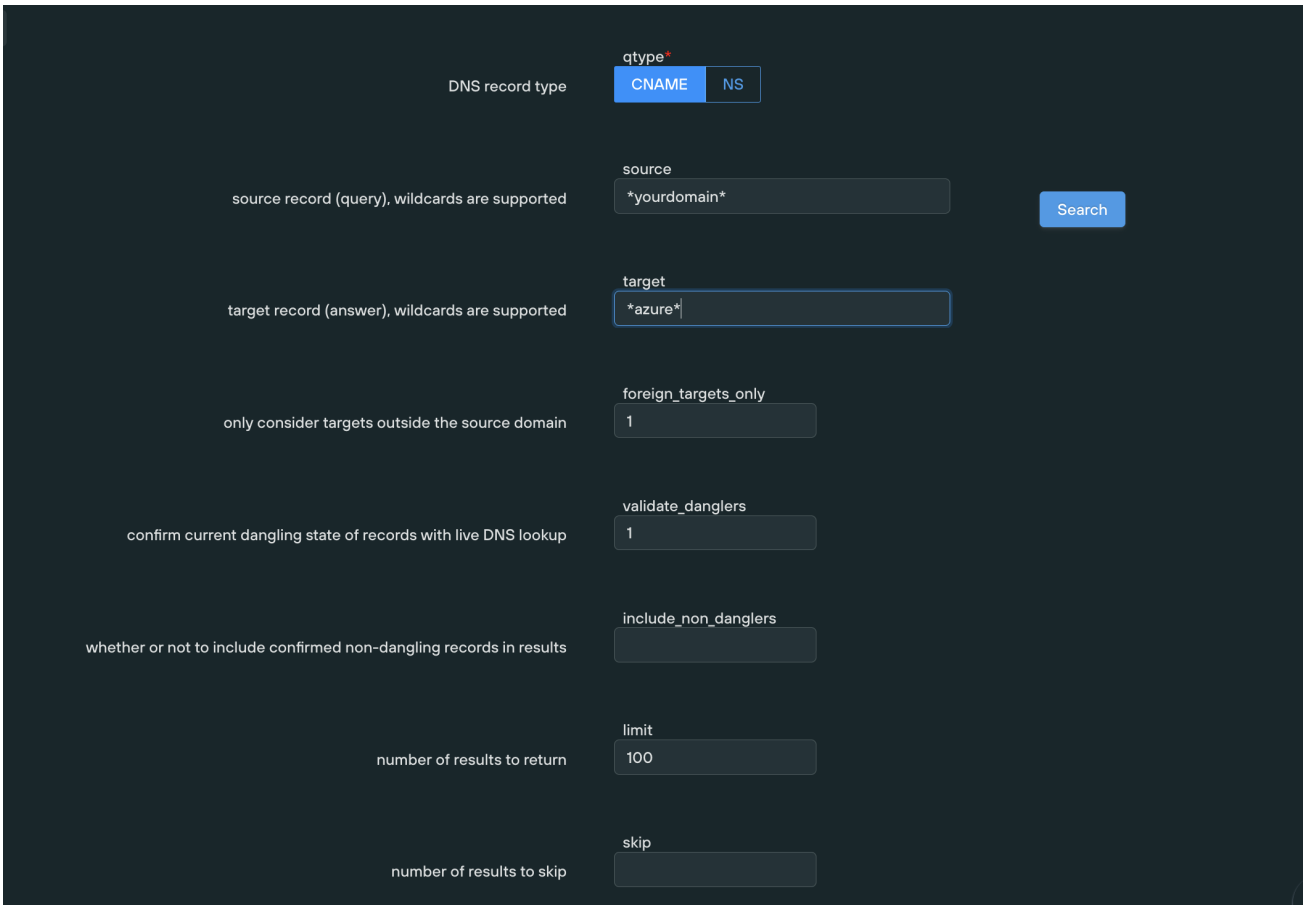
Fortunately, this is an easy answer.

We provide a free lookup tool in our Community Edition. From our Explore page, choose Query Builder.

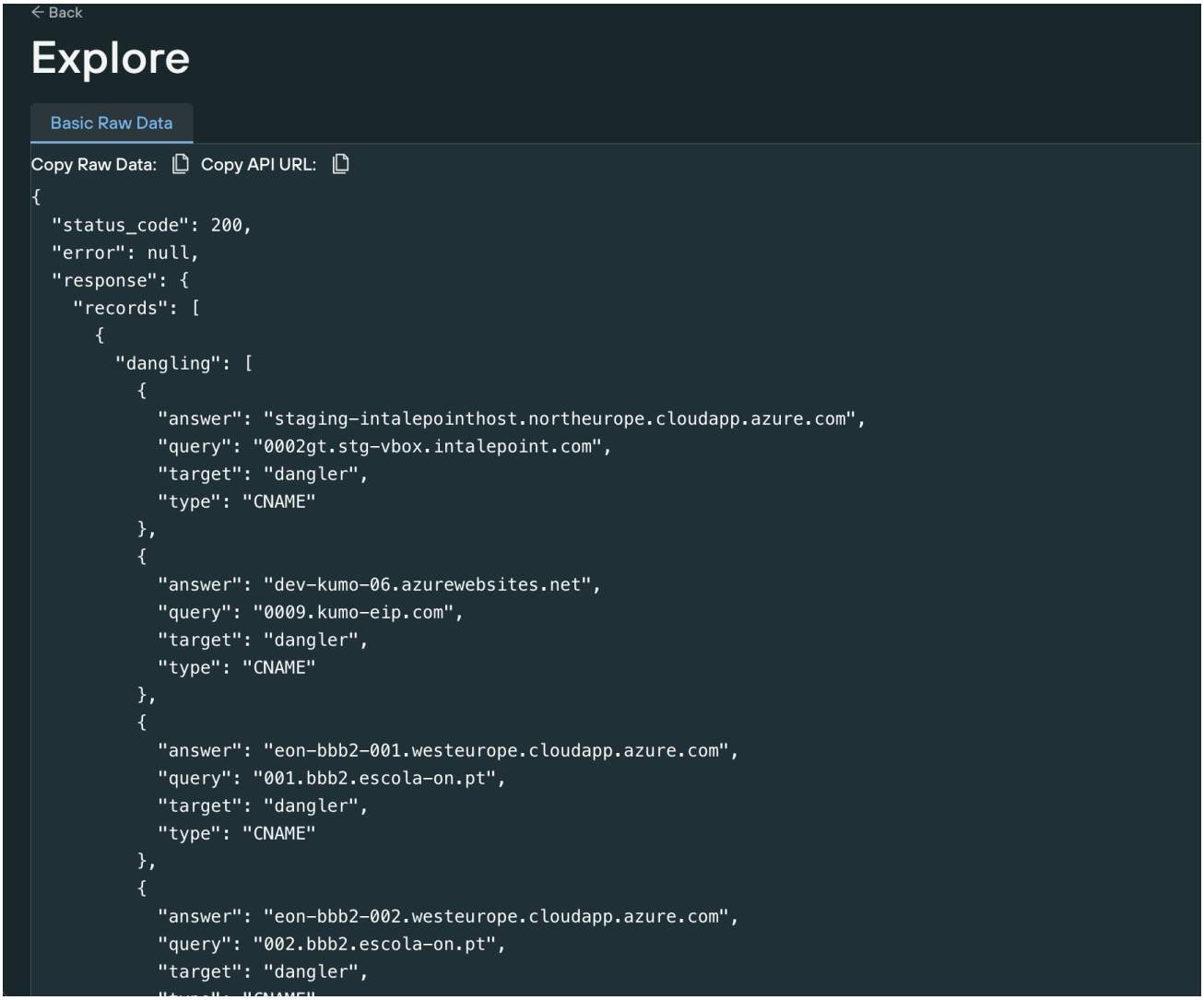


Then from the bottom left in our Experimental section choose -PADNS search dangling records

Enter your domain, wildcards are accepted. If you wish you can also enter the target service. For example, if you are concerned about having a dangling domain pointed at some Azure service you can enter



This will give you the results you need. In the example below, I have just entered the target. This could be used by security researchers to look for soft targets.



We have achieved this by marking all CNAME records where the target has no destination as a dangling record. We do the same for Name Servers.

Next Steps

Now you need to delete all of these dangling DNS entries so they no longer leave you exposed.

Access

You can apply for access to the community edition of our service here

Name *
Thank you!
Or for a trial of the main service with all its real time monitoring and threat feeds,

Name *
Thank you!

The Team