Shodan Query Guide - How To Track Amadey Bot Infrastructure With TLS Certificates and Russian Profanity

By Matthew

Published: 2023-05-19 · Archived: 2026-04-05 23:00:56 UTC

Analysing a suspicious IP address found in our previous post on Amadey Bot Malware. Utilising Shodan and Censys to pivot to additional Amadey infrastructure.

Here you'll see how to use a known c2 to craft additional queries based on html content and certificate information. In total, 12 unique servers will be identified.

Original sample can be found here and original post here.

(If you're just here for the c2 list, it's at the bottom of this post)

Analysis

In the original post on Amadey bot, conditional breakpoints were used to extract decrypted strings and obtain the address of a command and control (C2) server.

A partial output of this can be seen below. Observing that the ip `77.91.124[.]207` has been extracted alongside a partial URL.

By utilising Shodan and Censys, we wanted to try and identify any additional C2 servers or related infrastructure.

Special thanks to Michael Koczwara for the initial inspiration for this post. Also thanks to Chris Duggan and 0xburgers for their inspiring and helpful posts.

Analysis of the IP with Shodan

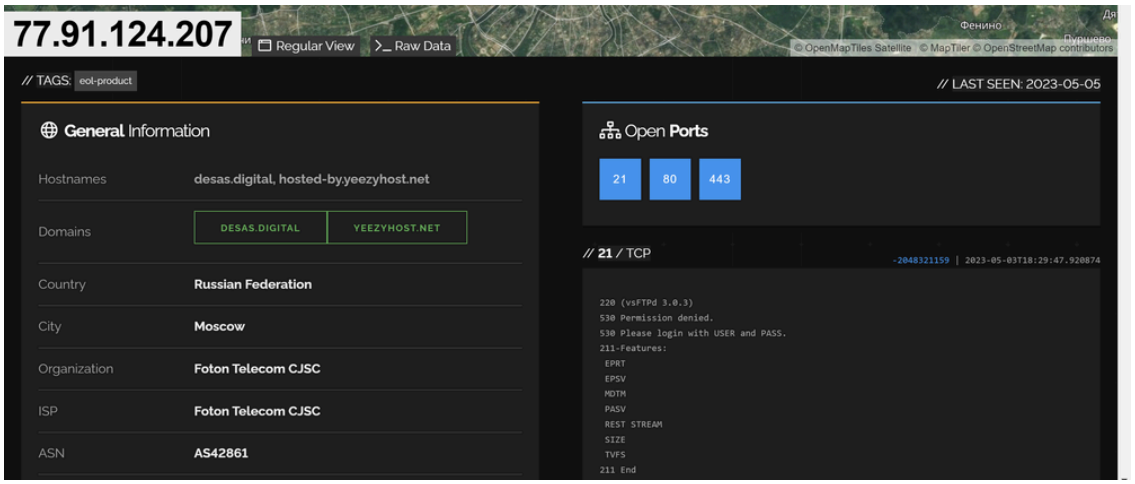
We initially analyzed the IP of `77.91.124[.]207` by inputting it directly into Shodan. Our goal here was to identify any unique pieces of information that could potentially be used to pivot to additional servers.

The kinds of information we were mainly looking for were..

- Unique headers and header values

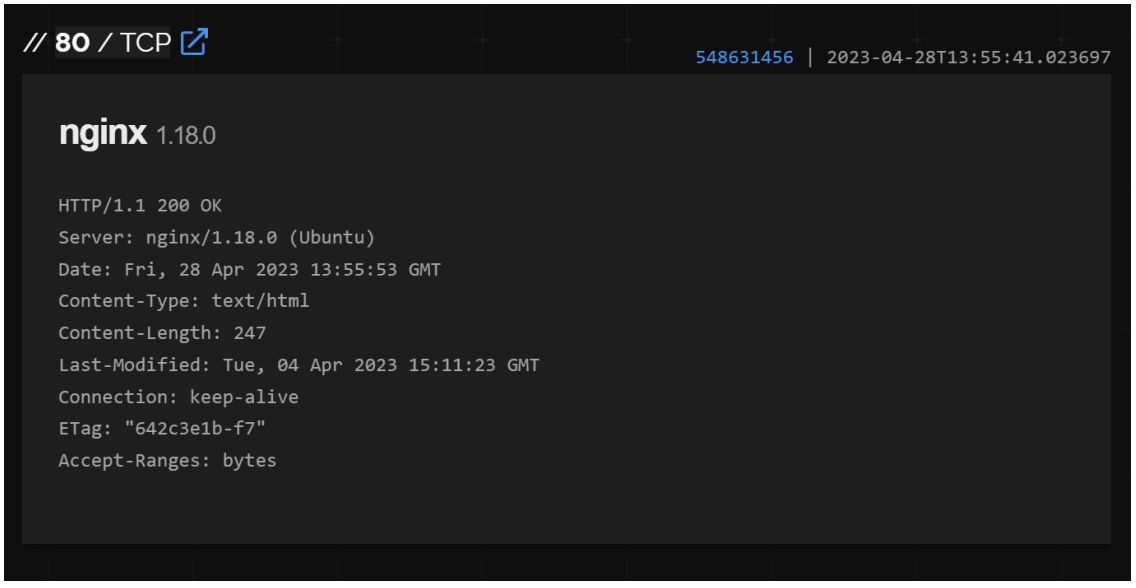
- SSL Certificates with unique information (issuer and subject in particular)
- SSL Fingerprints (JARM and JA3)
- Unique titles in HTTP Responses
- Unique content returned in HTTP bodies.

Our first search was a plain search for the original Amadey C2 of `77.91.124[.]207` (without the [.]), this identified a running server with three open ports. `21,80,443`



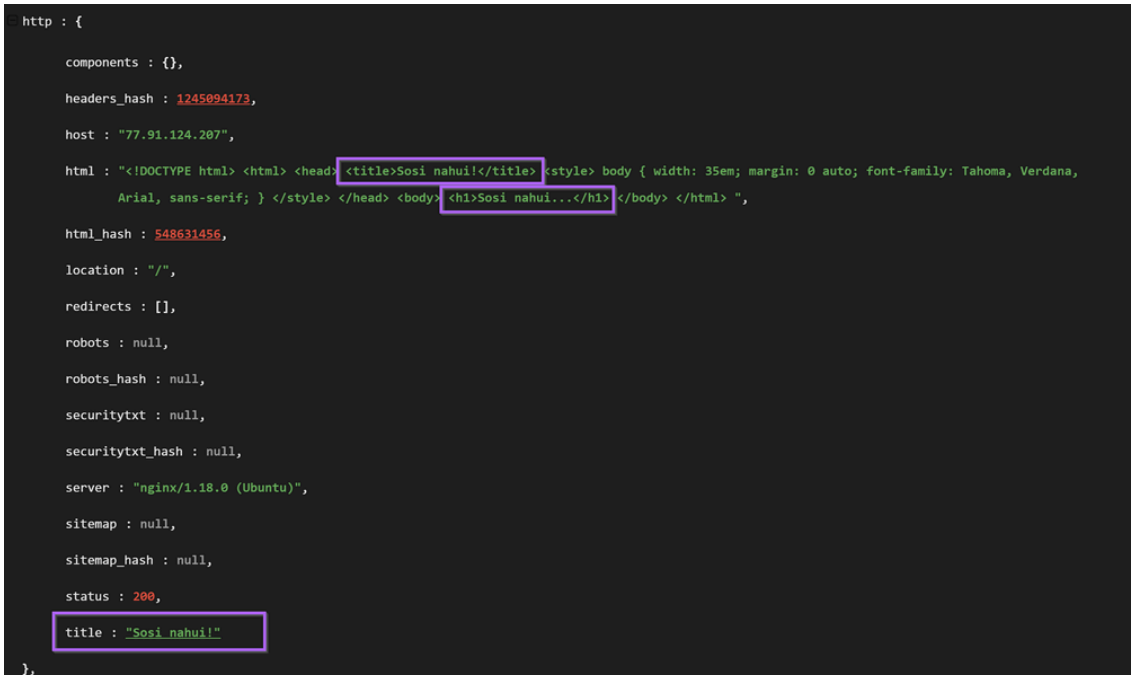
The first port available was port `21` , this appeared to be a plain FTP server without any unique information to pivot from.

The second available port was port `80` , nothing stood out within the headers but we decided to look further by inspecting the http response.



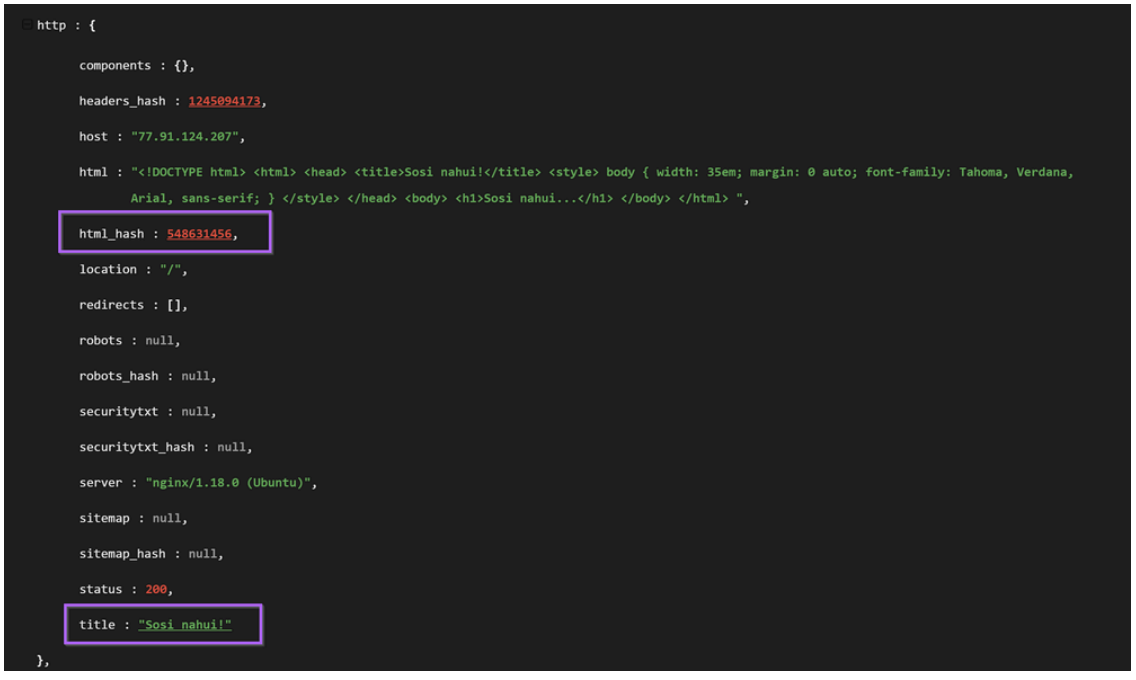
The html response was obtained from within the "raw data" Shodan tab and contained multiple references to "*Sosi nahui!*". (Essentially a f*ck off in Russian)

This was a reasonably unique value that could serve as a pivot point.



This polite message was present in both the html body and html title. These two fields provided two values that could be used for pivoting.

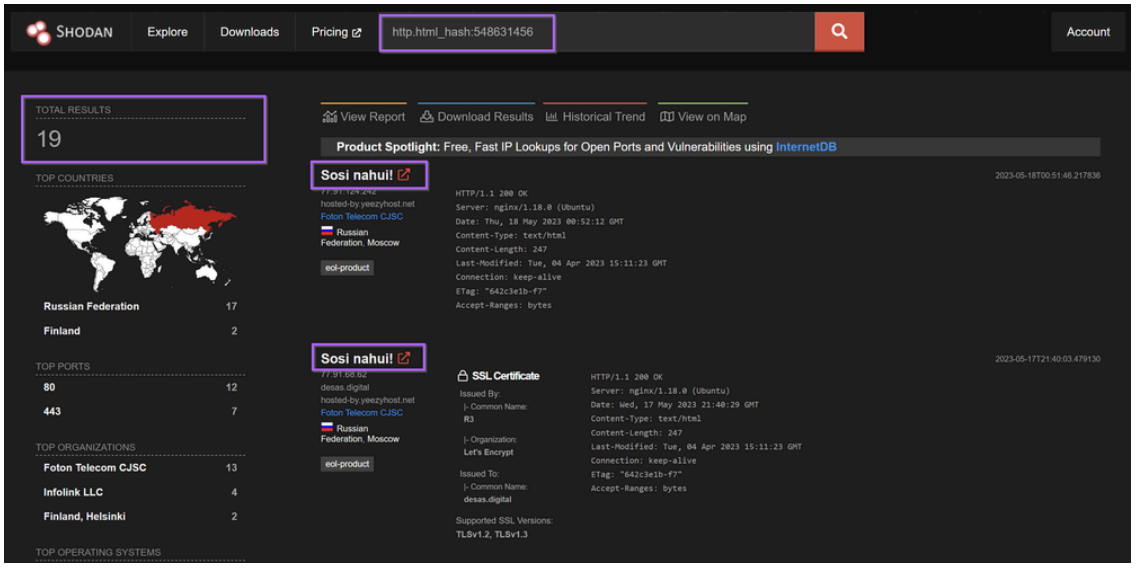
Option one was the hash of the html response. Option two was the html title. Both are dependent on the "unique" content of "*Sosi Nahui!*"



Option 1 - Shodan Pivoting with the html hash

Pivoting with the html_hash produced 19 results for similar servers. Each server had an identical html title of "*Sosi Nahui!*" and were all based in either Russia Finland. For me, this was enough similarity to begin assuming similar origin.

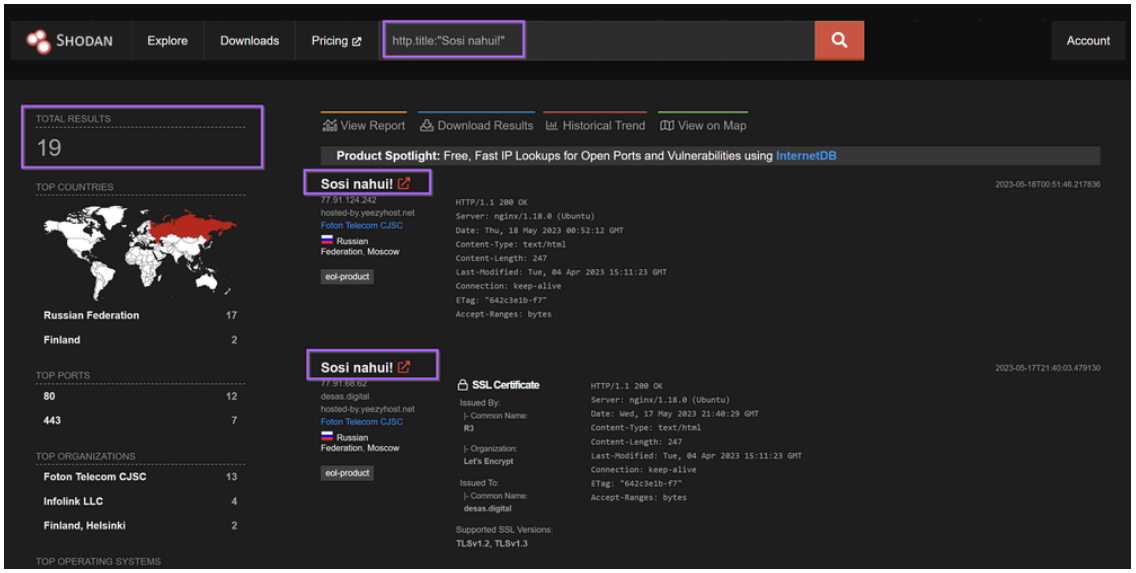
> Note that of these 19 results there were only 12 unique IP addresses. Some IP's were counted twice if the same hash appeared on multiple ports. (Eg same response on port `80` and `443`)



The results of this scan have all been exported and added to the end of this post.

Option 2 - Shodan Pivoting With the HTML Title

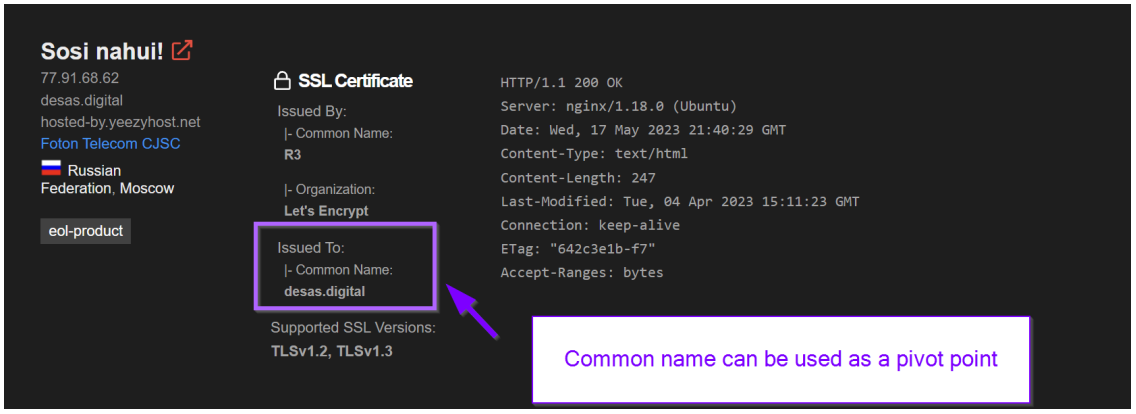
Pivoting based on the html title produces the same 19 results. Again noting that some of these are duplicates.



Shodan Pivoting With the Subject Common Name

Both Shodan searches contained references to `desas.digital` inside the subject common name of the ssl certificate.

This was another unique and interesting value that could be used as a pivot point.

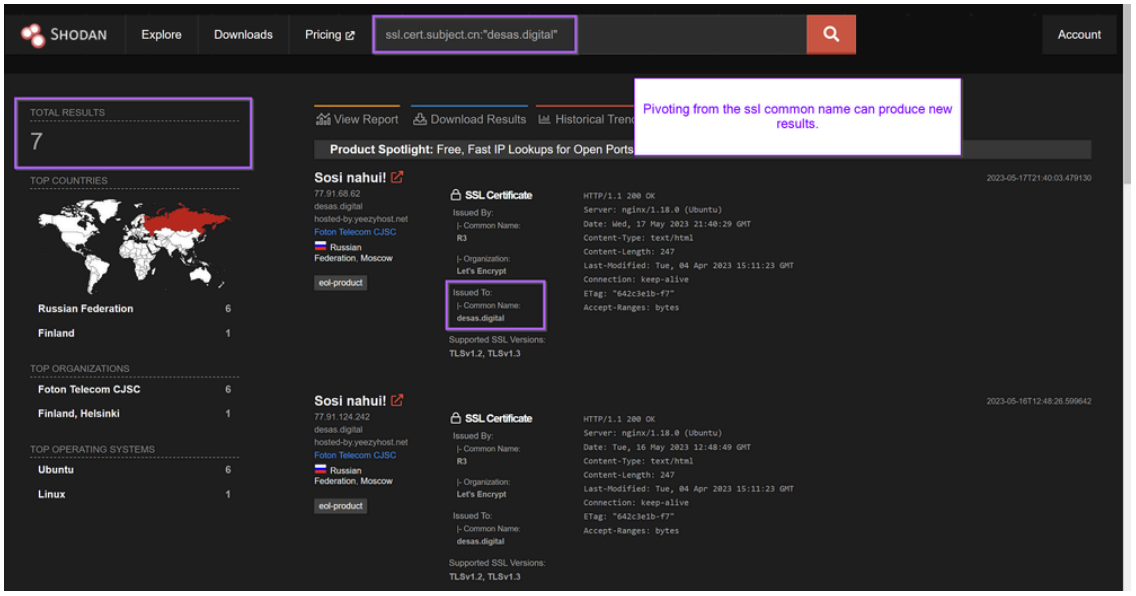


Seven results could be found by modifying the Shodan query to `ssl.cert.subject.cn:"desas.digital"`.

This query was able to be crafted by referencing the Shodan Filter list.

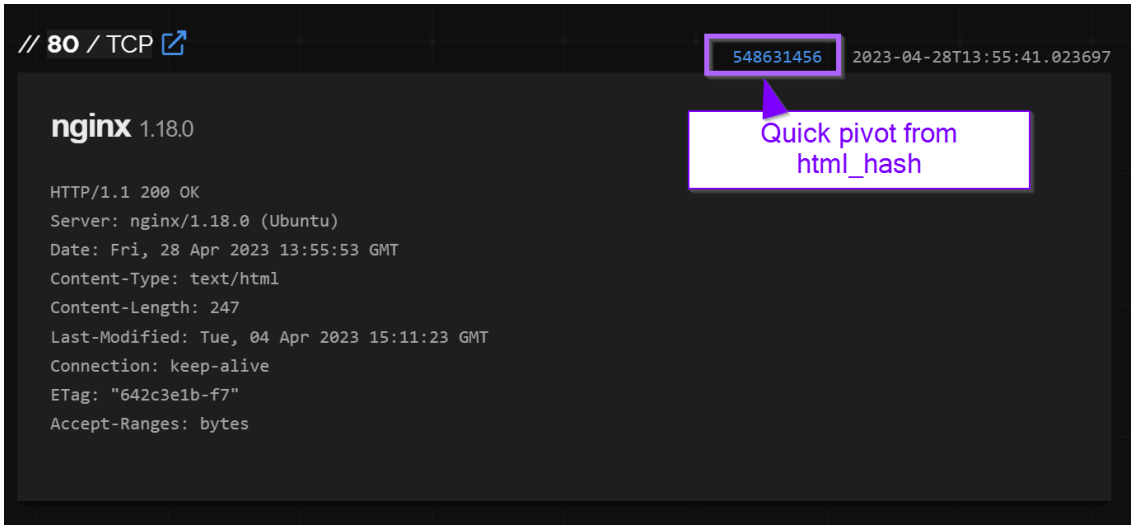
Pivoting with the subject common name *can* produce new results and additional servers. In this case, no new servers were found.

The returned results were all contained within the initial results for "*sosi nahui!*" and the html_hash.



At this point we were satisfied with our analysis of port `80` and decided not to pursue it further. There may be other avenues that could have resulted in more servers.

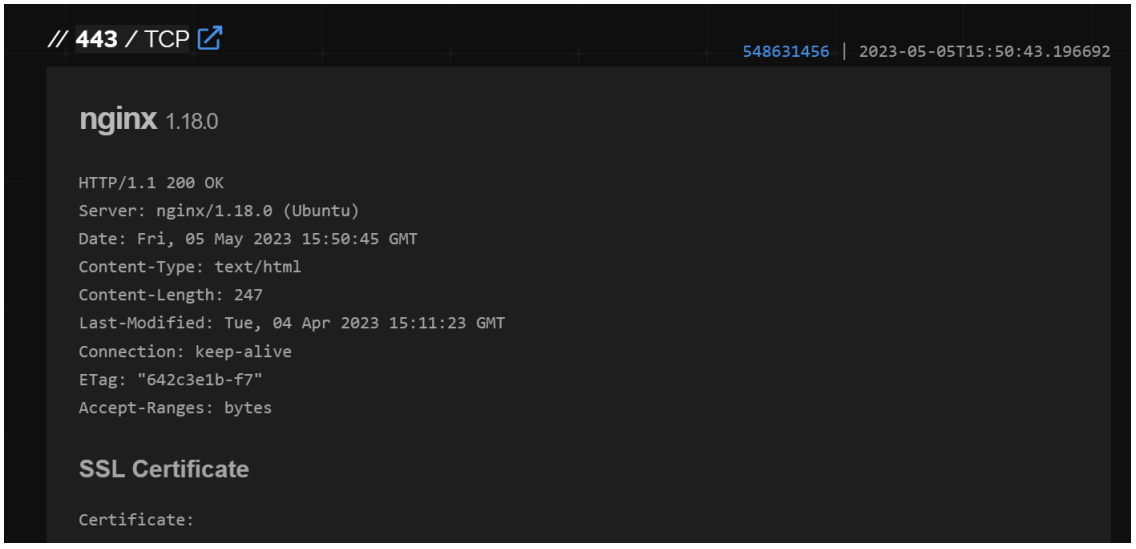
> These same results could also have been obtained by clicking directly on the html_hash from the original page. This is a good option if you don't have the paid version of Shodan.



Shodan Analysis of Port 443

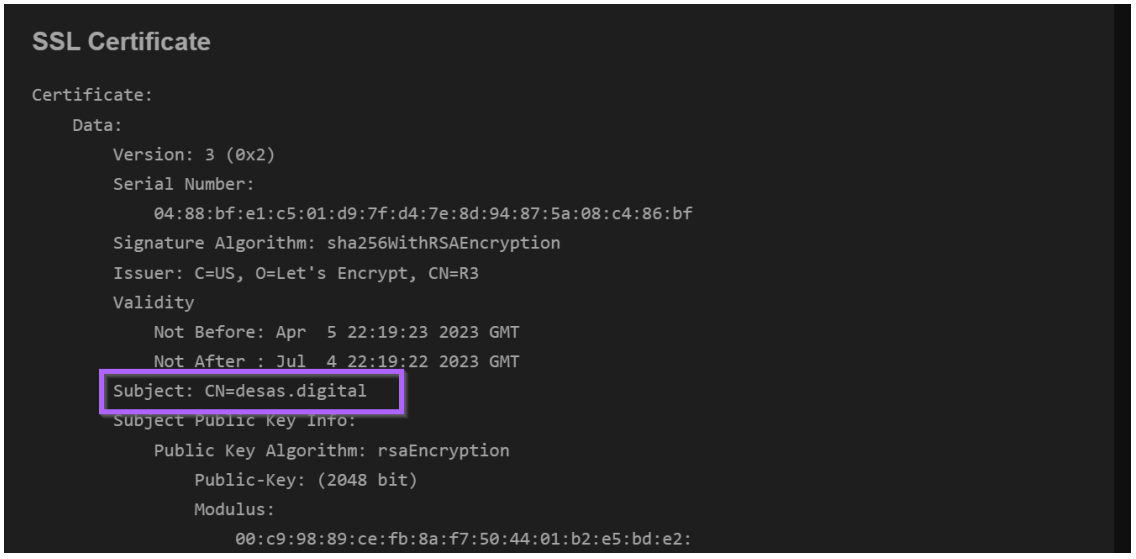
Moving back to the original search for `77.91.124[.]207`, there still remained port `443` to be analyzed.

This revealed another reverse proxy running with nginx.



The html responses on this port were identical to those on port `80` and would produce the same results when searched.

Port `443` also contained references to the same `desas.digital` certificate that was previously identified.



The rest of the certificate did not contain anything that we could pivot from.

The remaining certificate values were not interesting outside of additional references to `desas.digital` which had already been identified. The next task was to try to pivot further using the ssl ja3 and ssl jarm hashes.

> The ja3 and jarm are ssl/tls fingerprints that can be used to identify separate servers containing certificates with similar origins. They are often used as pivot points in blogs utilising Shodan.

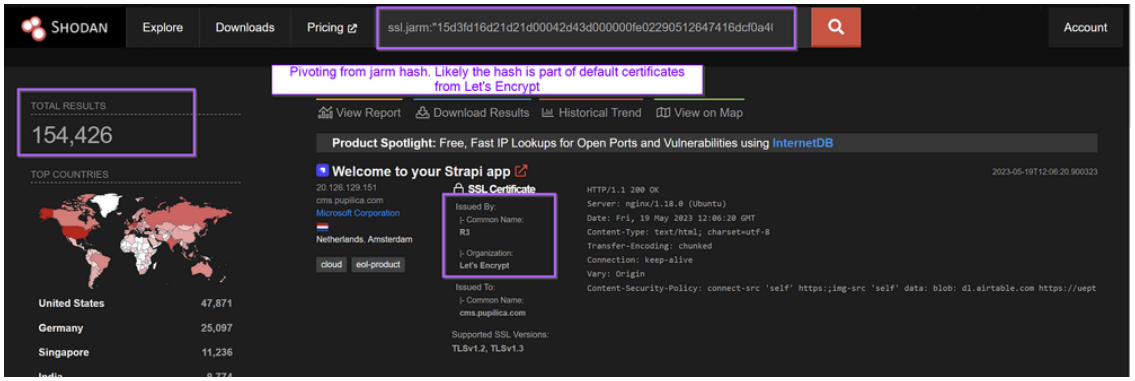
These two fingerprint values were present in the `raw_data` tab of Shodan. (Expand All and CTRL+F if your raw data tab gets too wild)

```
],
ja3s : "574866101f64002c6421cc329e4d5458",
jarm : "15d3fd16d21d21d00042d43d000000fe02290512647416dcf0a400ccbc0b6b",
ocsp : {},
tlsext : [
```

Pivoting from the Jarm hash produced `154,426` results.

We suspect this was because the Jarm was related to `Let's Encrypt` and not specifically to this malware. (Let's Encrypt is a popular free service for producing TLS certificates, so it makes sense that there are a lot of "similar" certificates)

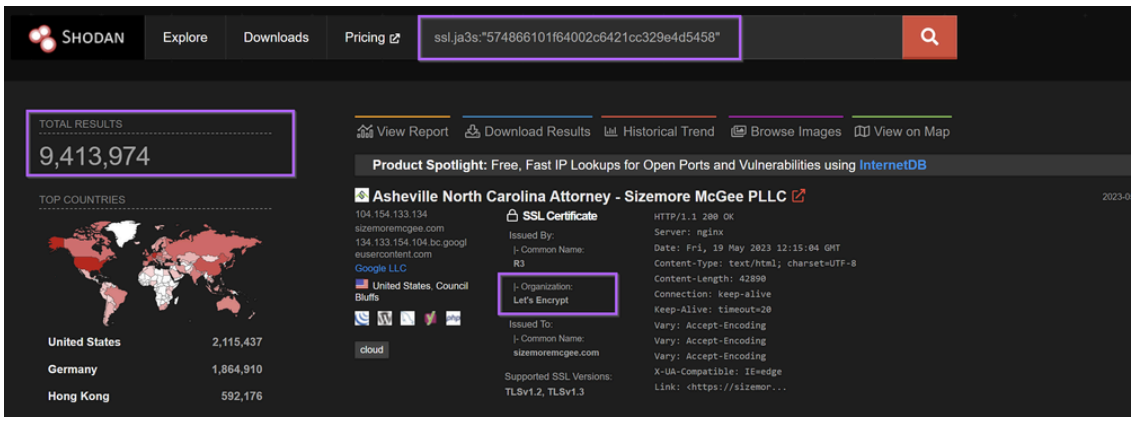
Essentially, this meant that the Jarm (on its own) was not useful as a pivot point as the properties that produce the Jarm fingerprint are shared with a huge number of other Let's Encrypt certificates.



Pivoting from the ja3 came to a similar conclusion with over nine million results returned.

As with the Jarm, the Ja3 fingerprint was not useful as a pivot point.

It's possible that the Jarm/ja3 fingerprints could be combined with other fields to produce a better result, but we decided not to pursue this route when 9 Million results were returned.



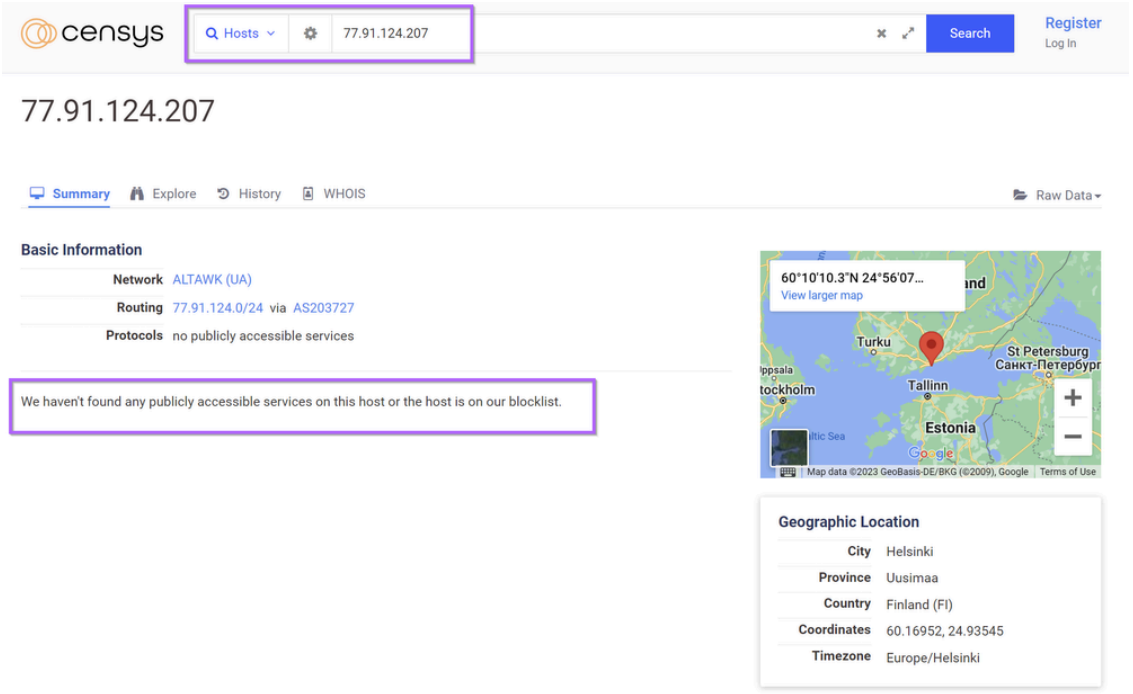
We then moved on to Censys to continue analysis.

Analysing Infrastructure With Censys

Continuing analysis using Censys, we decided to input the initial ip in order to compare results.

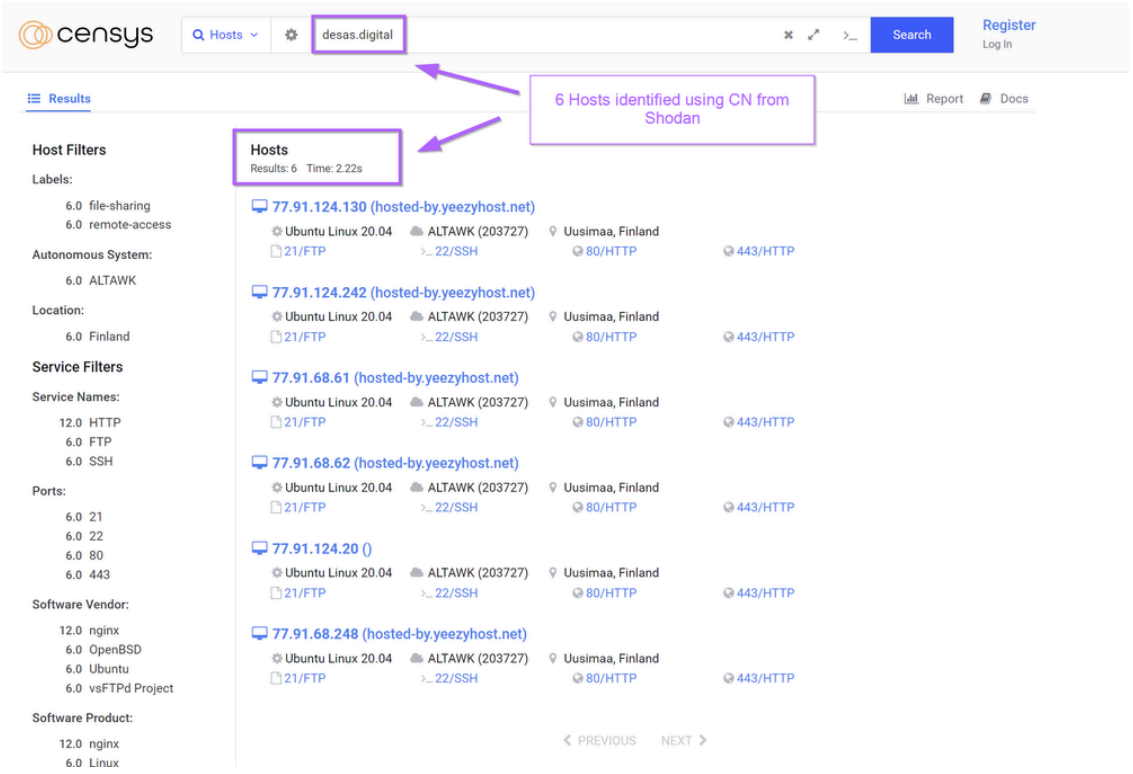
A Censys search for the ip `77.91.124.207` returned the ip with no running services. Censys has likely performed a scan whilst the server was down or not responding to Censys headers.

This highlights why it is useful to use multiple tools.

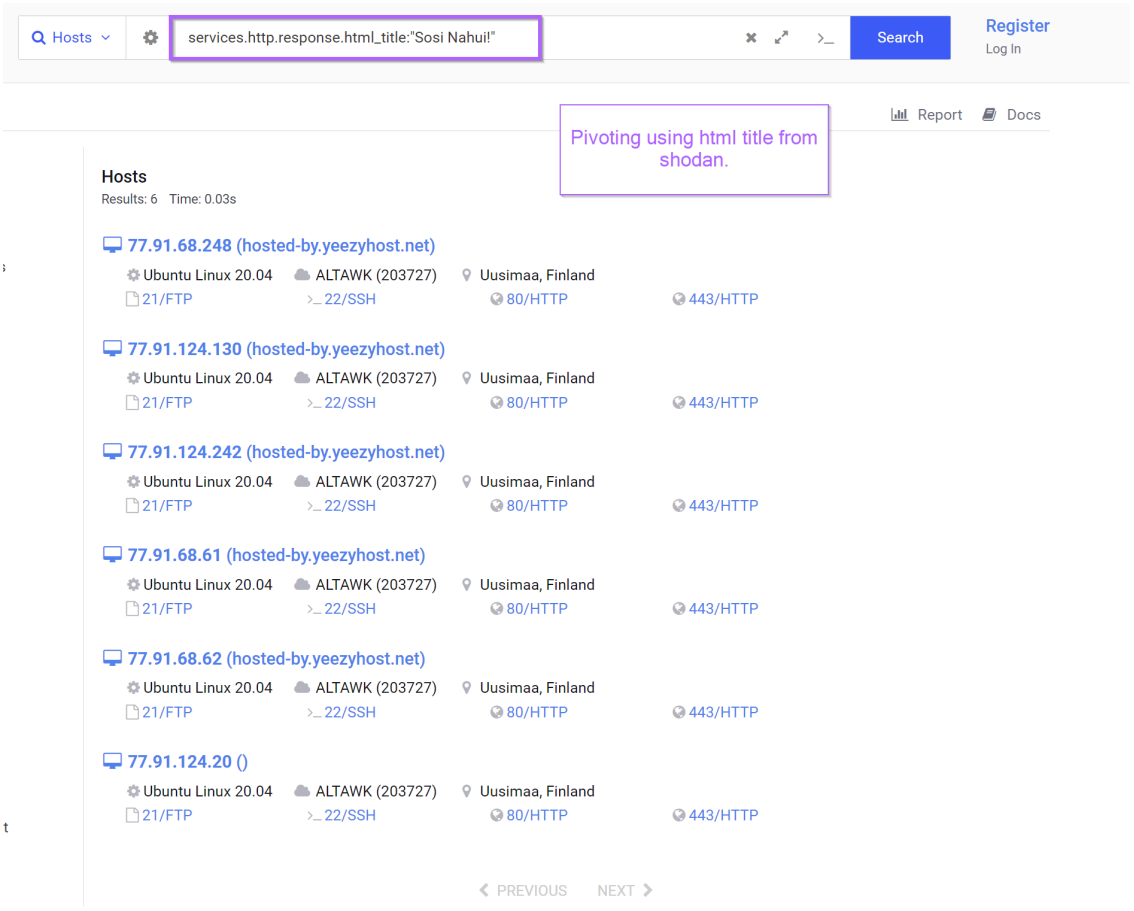


Utilising the previously obtained `desas.digital`, 6 results are found.

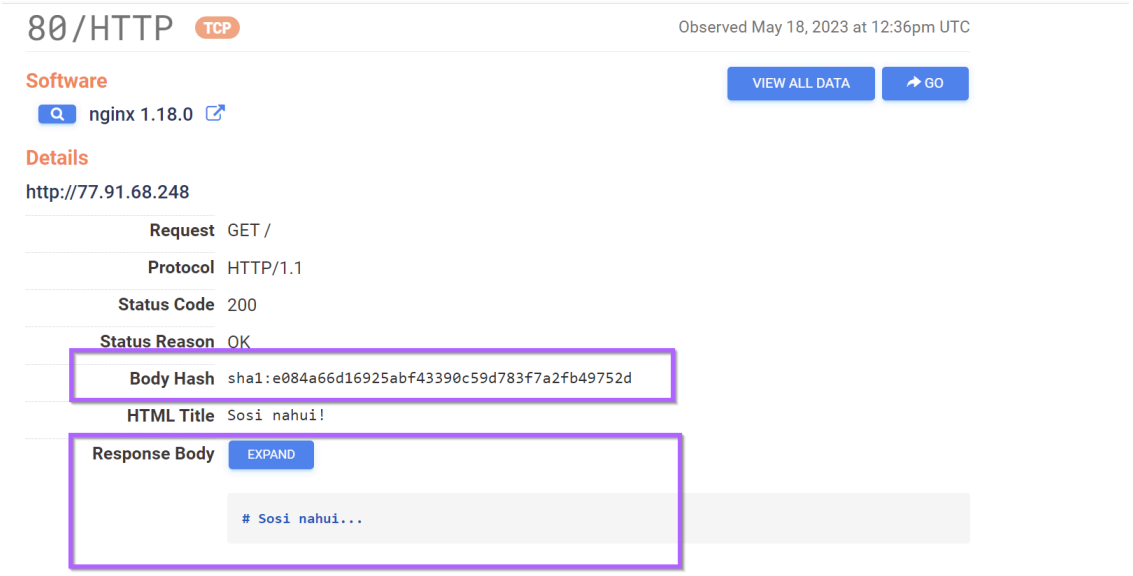
These results were all contained within the 19 results from Shodan. No new results were found.



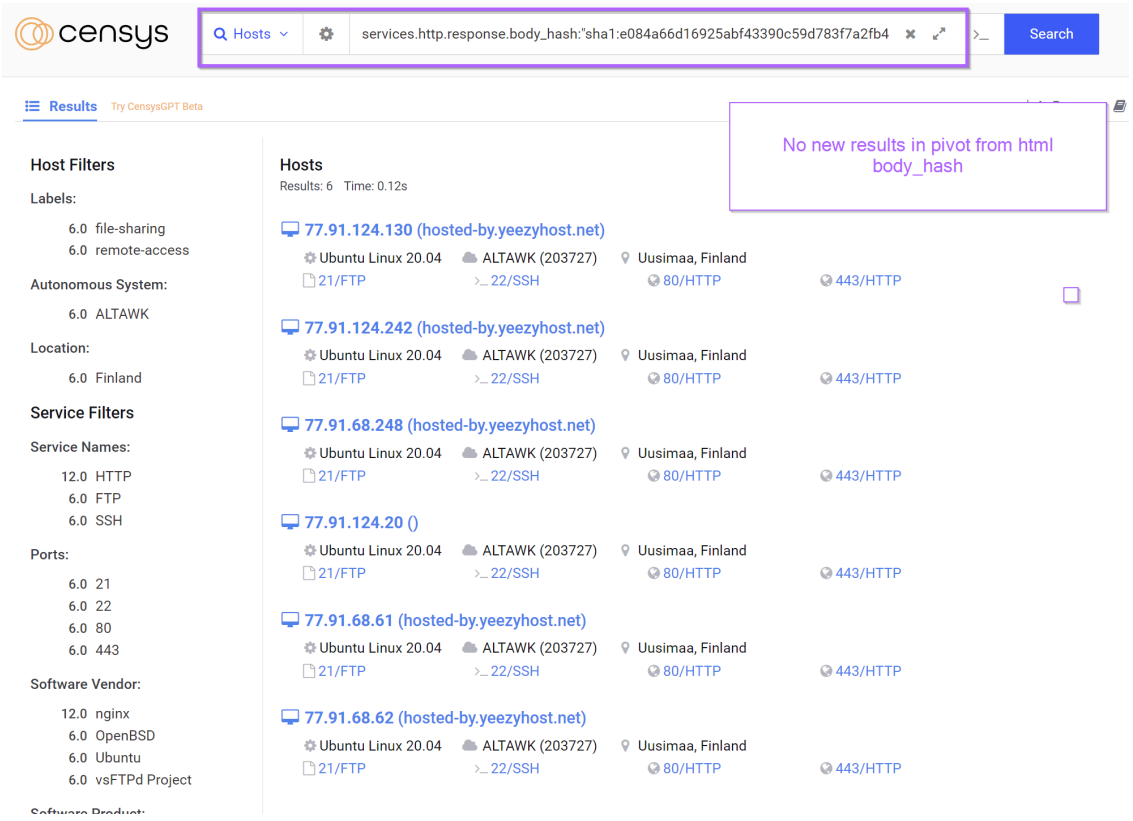
Attempts to pivot using the html title produced the same 6 results as the search for `desas.digital`.



The Censys page for `77.91.68[.]248` contained references to a body hash which could be useful for additional pivoting.



However, attempts to pivot from this html hash produced no new results.



Continuing analysis, we were unable to identify any additional servers with Shodan or Censys.

We exported our results from Shodan and they have been included at the end of this post.

Conclusion

At this point we were happy with the 12 unique servers initially identified by Shodan and we decided to call it a day. These 12 servers all shared extremely similar html content, location and certificate information so we had high confidence that they were related.

If you wish to read the original analysis that produced the initial IP address, you can find that here.

> Redline Stealer/Amadey Bot - Static Analysis and C2 Extraction
>
> Deep dive analysis of a redline stealer sample. I will use manual analysis to extract C2 information using a combination of Ghidra and x32dbg

Embee ResearchMatthew

One Last Thing

If you enjoyed this post and would like to see more. Consider becoming a member of the site.

Members will receive early access to blogs and threat intel, exclusive posts, as well as access to a discord server where you can ask questions and get help with analysis.

Sign up here

Final Results

Shodan

- `http.html_hash:548631456`
- `ssl.cert.subject.cn:"desas.digital"`
- `http.title:"sosi nahui!"`

Censys

- `services.tls.certificates.leaf_data.subject.common_name:"desas.digital"`
- `services.http.response.body_hash:"sha1:e084a66d16925abf43390c59d783f7a2fb49752d"`

List Of Identified Servers

```
 77.91.68.61
77.91.68.62
77.91.68.248
77.91.124.20
77.91.124.130
77.91.124.203
77.91.124.207
77.91.124.242
193.201.9.43
193.201.9.44
193.201.9.67
193.201.9.241
```

VirusTotal CrossCheck (2023-05-17)

```
 77.91.68.61 - 1/87
77.91.68.62 - 11/87
77.91.68.248 - 3/87
77.91.124.20 - 1/87
77.91.124.130 - 3/87
77.91.124.203 - 10/87
77.91.124.207 - 1/87
77.91.124.242 - 1/87
193.201.9.43 - 1/87
193.201.9.44 - 0/86
193.201.9.67 - 11/87
193.201.9.241 - 2/87
```
