Analysis of Amadey Bot Infrastructure Using Shodan

embee-research.ghost.io/amadey-bot-infrastructure/

Matthew

May 19, 2023

intel

Identifying Amadey Bot Servers Using Shodan.

Analysing a suspicious ip address found in my 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.

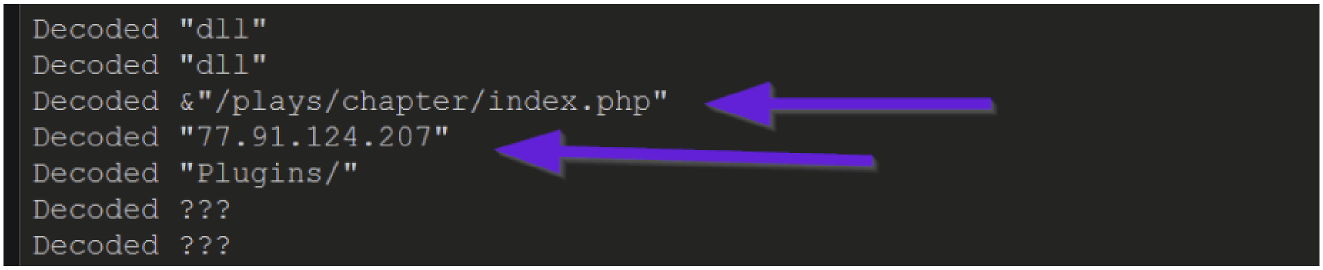
Original sample can be found here and original post here.

(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.



```
Decoded "dll"
Decoded "dll"
Decoded &"/plays/chapter/index.php"
Decoded "77.91.124.207"
Decoded "Plugins/"
Decoded ???
Decoded ???
```

By utilising Shodan and Censys, I 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.

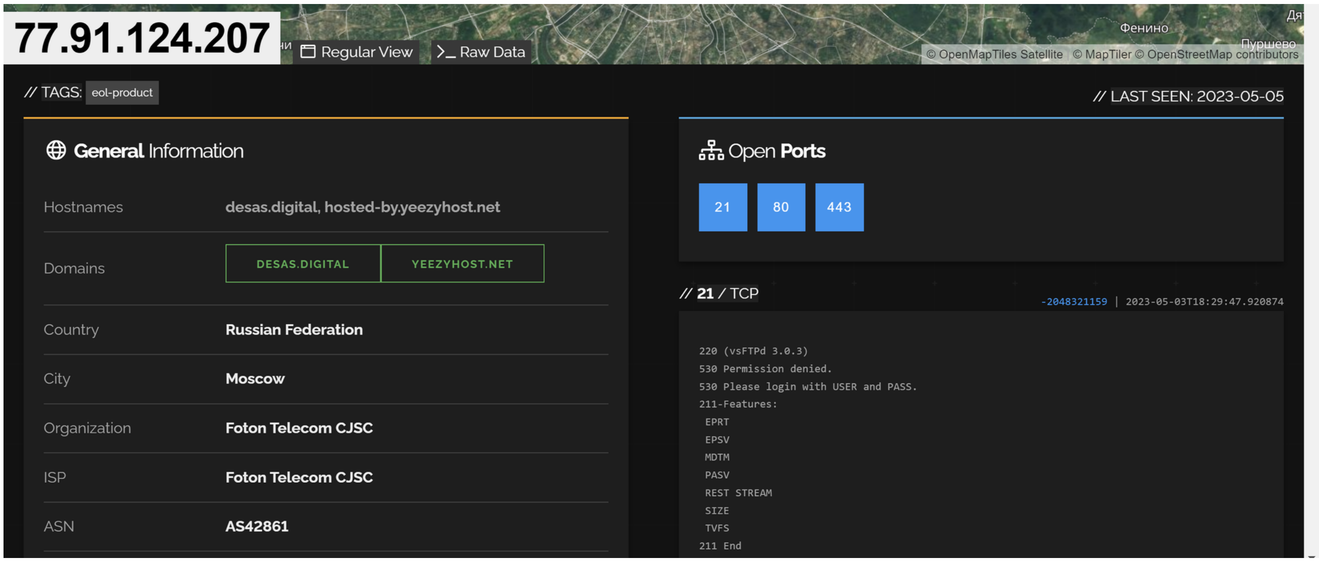
Analysis of the IP with Shodan

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

I'm still new to Shodan and this type of analysis, but the kinds of information I was 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.

My 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`


Фенино
Пуршево
Дя
© OpenMapTiles Satellite © MapTiler © OpenStreetMap contributors
Regular View
>_ Raw Data

77.91.124.207

// TAGS: eol-product

// LAST SEEN: 2023-05-05

General Information

Hostnames	desas.digital, hosted-by.yeezyhost.net
Domains	DESAS.DIGITAL YEEZYHOST.NET
Country	Russian Federation
City	Moscow
Organization	Foton Telecom CJSC
ISP	Foton Telecom CJSC
ASN	AS42861

Open **Ports**

21 80 443

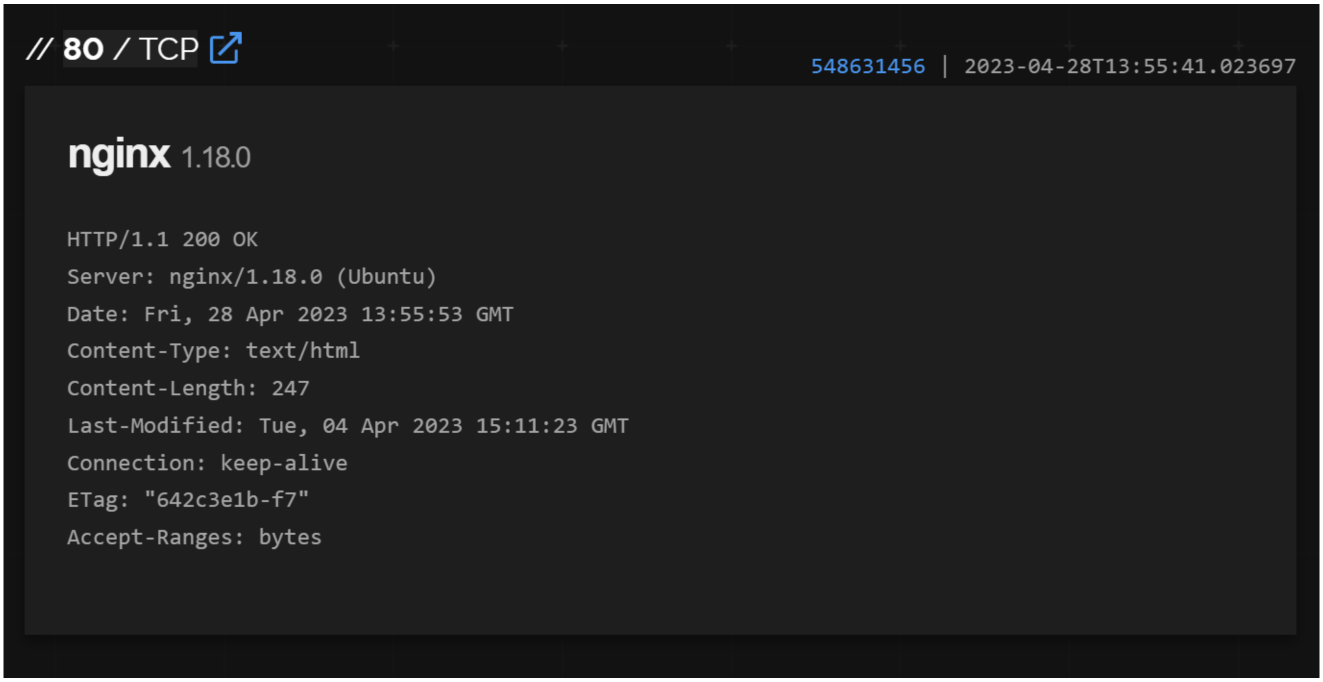
// **21** / TCP

-2048321159 | 2023-05-03T18:29:47.920874

```
220 (vsFTPd 3.0.3)
530 Permission denied.
530 Please login with USER and PASS.
211-Features:
 EPRT
 EPSV
 MDTM
 PASV
 REST STREAM
 SIZE
 TVFS
211 End
```

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 I decided to look further by inspecting the http response.



// 80 / TCP

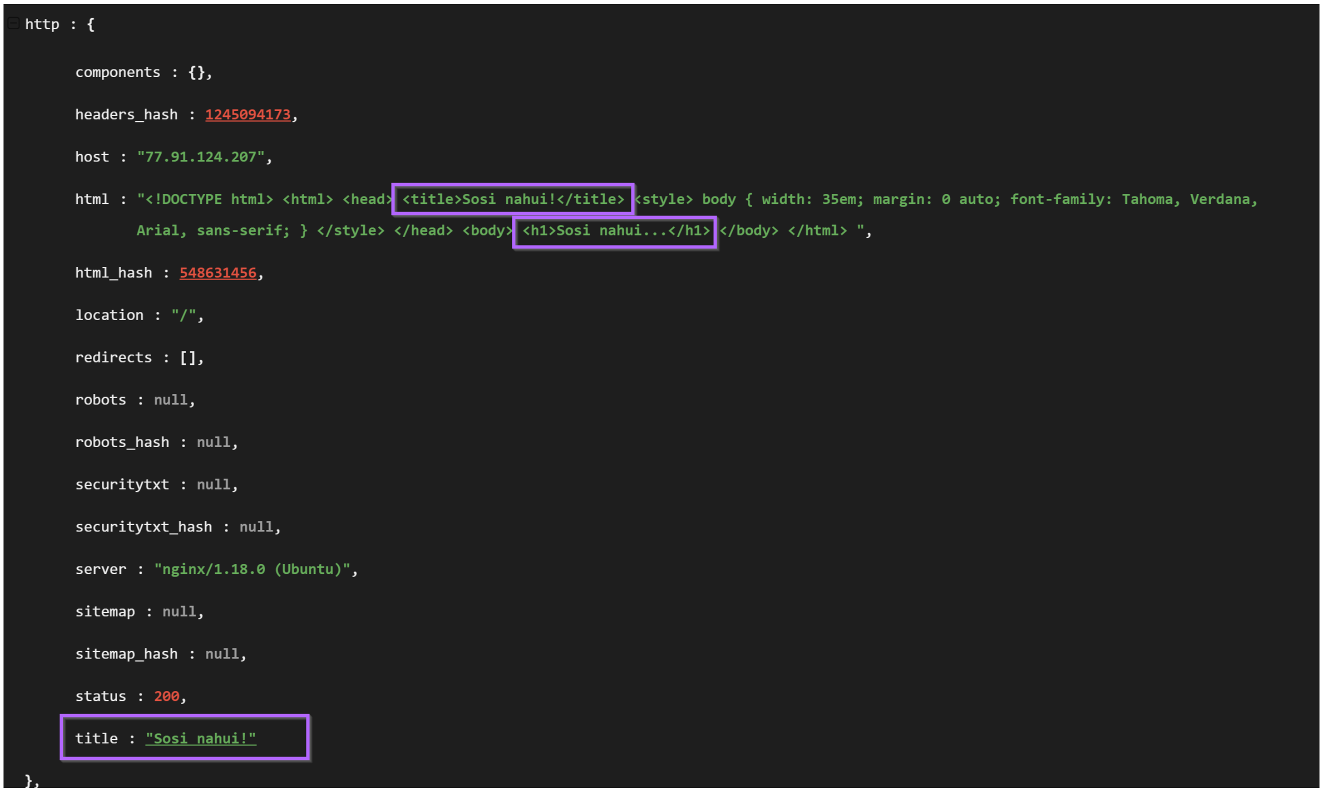
548631456 | 2023-04-28T13:55:41.023697

nginx 1.18.0

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Fri, 28 Apr 2023 13:55:53 GMT
Content-Type: text/html
Content-Length: 247
Last-Modified: Tue, 04 Apr 2023 15:11:23 GMT
Connection: keep-alive
ETag: "642c3e1b-f7"
Accept-Ranges: bytes
```

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)

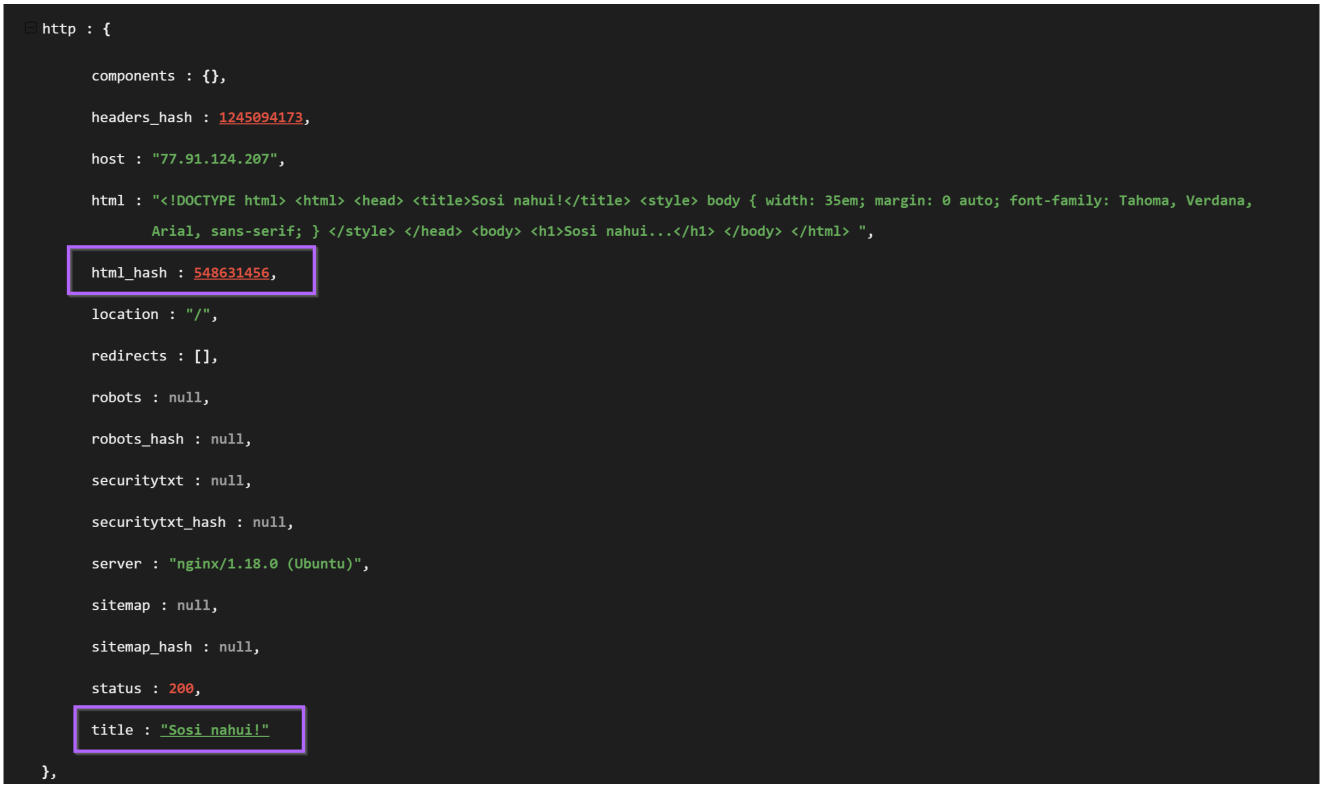
This was a reasonably unique value that could serve as a pivot point.



```
http : {
      components : {},
      headers_hash : 1245094173,
      host : "77.91.124.207",
      html : "<!DOCTYPE html> <html> <head> <title>Sosi nahui!</title> <style> body { width: 35em; margin: 0 auto; font-family: Tahoma, Verdana,
             Arial, sans-serif; } </style> </head> <body> <h1>Sosi nahui...</h1> </body> </html> ",
      html_hash : 548631456,
      location : "/",
      redirects : [],
      robots : null,
      robots_hash : null,
      securitytxt : null,
      securitytxt_hash : null,
      server : "nginx/1.18.0 (Ubuntu)",
      sitemap : null,
      sitemap_hash : null,
      status : 200,
      title : "Sosi nahui!"
},
```

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!*"

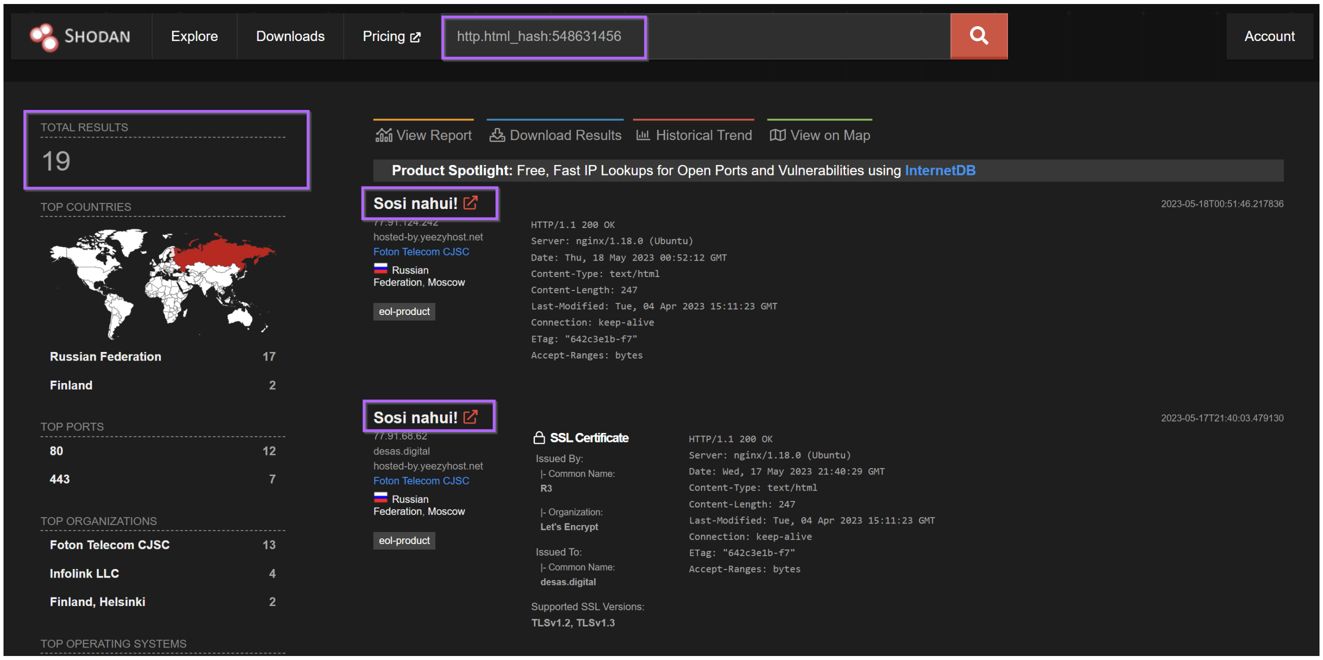


```
http : {

      components : {},

      headers_hash : 1245094173,

      host : "77.91.124.207",

      html : "<!DOCTYPE html> <html> <head> <title>Sosi nahui!</title> <style> body { width: 35em; margin: 0 auto; font-family: Tahoma, Verdana,
             Arial, sans-serif; } </style> </head> <body> <h1>Sosi nahui...</h1> </body> </html> ",

      html_hash : 548631456,

      location : "/",

      redirects : [],

      robots : null,

      robots_hash : null,

      securitytxt : null,

      securitytxt_hash : null,

      server : "nginx/1.18.0 (Ubuntu)",

      sitemap : null,

      sitemap_hash : null,

      status : 200,

      title : "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`)



TOTAL RESULTS

19

TOP COUNTRIES

Russian Federation	17
Finland	2

TOP PORTS

80	12
443	7

TOP ORGANIZATIONS

Foton Telecom CJSC	13
Infolink LLC	4
Finland, Helsinki	2

TOP OPERATING SYSTEMS

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

Sosi nahui!

77.91.124.242
hosted-by.yeezyhost.net
Foton Telecom CJSC
Russian Federation, Moscow

eol-product

2023-05-18T00:51:46.217836

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Thu, 18 May 2023 00:52:12 GMT
Content-Type: text/html
Content-Length: 247
Last-Modified: Tue, 04 Apr 2023 15:11:23 GMT
Connection: keep-alive
ETag: "642c3e1b-f7"
Accept-Ranges: bytes
```

Sosi nahui!

77.91.68.62
desas.digital
hosted-by.yeezyhost.net
Foton Telecom CJSC
Russian Federation, Moscow

eol-product

SSL Certificate

Issued By:
|- Common Name:
R3
|- Organization:
Let's Encrypt

Issued To:
|- Common Name:
desas.digital

Supported SSL Versions:
TLSv1.2, TLSv1.3

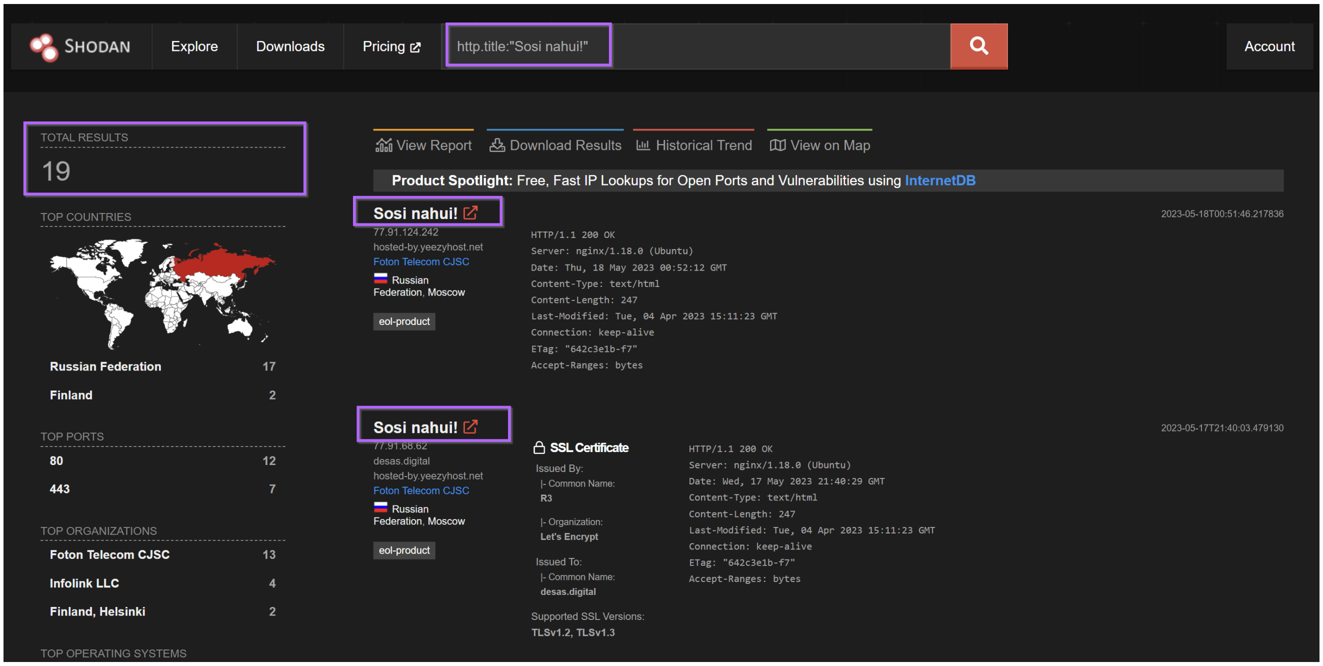
2023-05-17T21:40:03.479130

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Wed, 17 May 2023 21:40:29 GMT
Content-Type: text/html
Content-Length: 247
Last-Modified: Tue, 04 Apr 2023 15:11:23 GMT
Connection: keep-alive
ETag: "642c3e1b-f7"
Accept-Ranges: bytes
```

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.



http.title:"Sosi nahui!"

TOTAL RESULTS
19

TOP COUNTRIES

Russian Federation	17
Finland	2

TOP PORTS

80	12
443	7

TOP ORGANIZATIONS

Foton Telecom CJSC	13
Infolink LLC	4
Finland, Helsinki	2

TOP OPERATING SYSTEMS

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

Sosi nahui!
77.91.124.242
hosted-by.yeezyhost.net
Foton Telecom CJSC
Russian Federation, Moscow
eol-product

2023-05-18T00:51:46.217836

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Thu, 18 May 2023 00:52:12 GMT
Content-Type: text/html
Content-Length: 247
Last-Modified: Tue, 04 Apr 2023 15:11:23 GMT
Connection: keep-alive
ETag: "642c3e1b-f7"
Accept-Ranges: bytes
```

Sosi nahui!
77.91.68.62
desas.digital
hosted-by.yeezyhost.net
Foton Telecom CJSC
Russian Federation, Moscow
eol-product

2023-05-17T21:40:03.479130

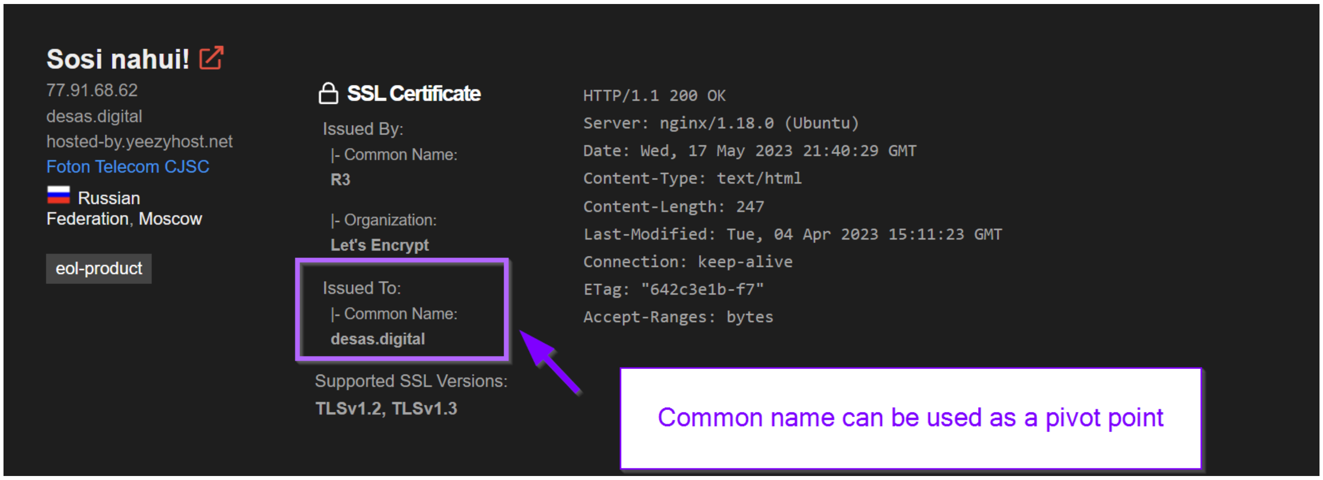
SSL Certificate
Issued By:
|- Common Name:
R3
|- Organization:
Let's Encrypt
Issued To:
|- Common Name:
desas.digital
Supported SSL Versions:
TLSv1.2, TLSv1.3

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Wed, 17 May 2023 21:40:29 GMT
Content-Type: text/html
Content-Length: 247
Last-Modified: Tue, 04 Apr 2023 15:11:23 GMT
Connection: keep-alive
ETag: "642c3e1b-f7"
Accept-Ranges: bytes
```

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.



Sosi nahui!
77.91.68.62
desas.digital
hosted-by.yeezyhost.net
Foton Telecom CJSC
Russian Federation, Moscow
eol-product

SSL Certificate
Issued By:
|- Common Name:
R3
|- Organization:
Let's Encrypt
Issued To:
|- Common Name:
desas.digital
Supported SSL Versions:
TLSv1.2, TLSv1.3

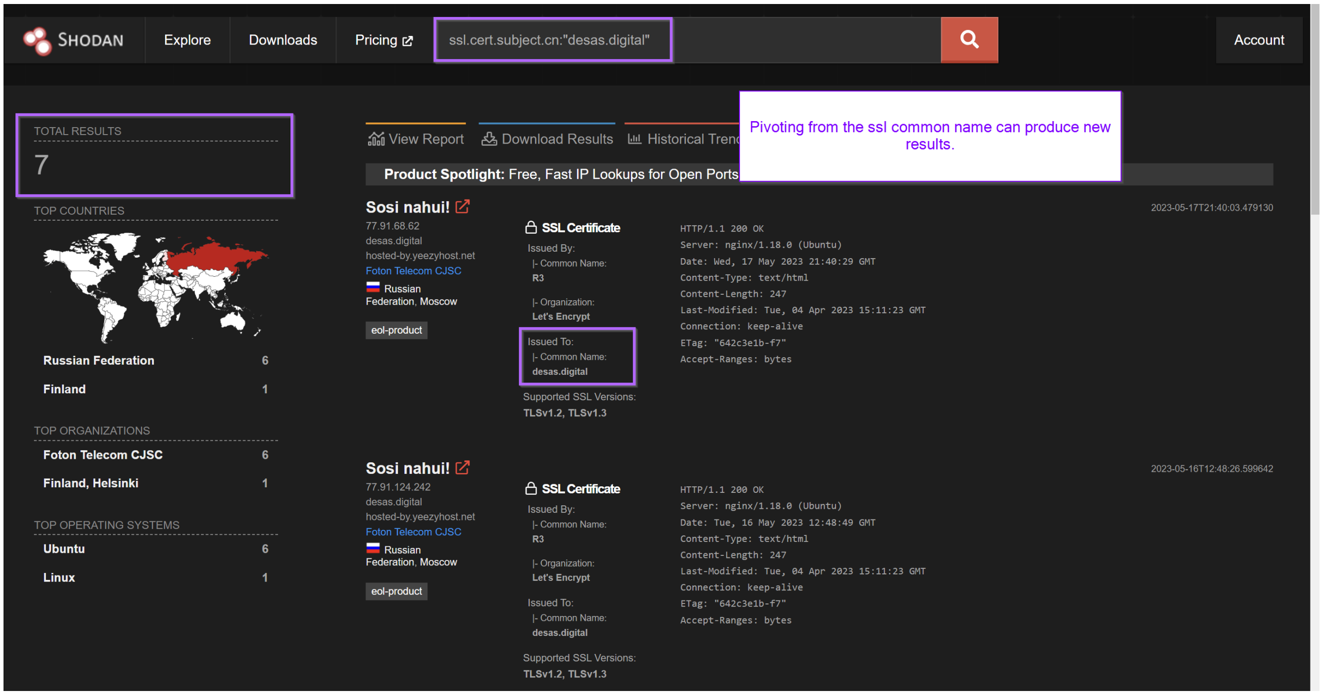
```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Wed, 17 May 2023 21:40:29 GMT
Content-Type: text/html
Content-Length: 247
Last-Modified: Tue, 04 Apr 2023 15:11:23 GMT
Connection: keep-alive
ETag: "642c3e1b-f7"
Accept-Ranges: bytes
```

Common name can 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.



ssl.cert.subject.cn:"desas.digital"

Pivoting from the ssl common name can produce new results.

TOTAL RESULTS
7

TOP COUNTRIES

Russian Federation	6
Finland	1

TOP ORGANIZATIONS

Foton Telecom CJSC	6
Finland, Helsinki	1

TOP OPERATING SYSTEMS

Ubuntu	6
Linux	1

Product Spotlight: Free, Fast IP Lookups for Open Ports

Sosi nahui! 2023-05-17T21:40:03.479130
77.91.68.62
desas.digital
hosted-by.yeezyhost.net
Foton Telecom CJSC
Russian Federation, Moscow
eol-product

SSL Certificate
Issued By:
|- Common Name:
R3
|- Organization:
Let's Encrypt
Issued To:
|- Common Name:
desas.digital
Supported SSL Versions:
TLSv1.2, TLSv1.3

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Wed, 17 May 2023 21:40:29 GMT
Content-Type: text/html
Content-Length: 247
Last-Modified: Tue, 04 Apr 2023 15:11:23 GMT
Connection: keep-alive
ETag: "642c3e1b-f7"
Accept-Ranges: bytes
```

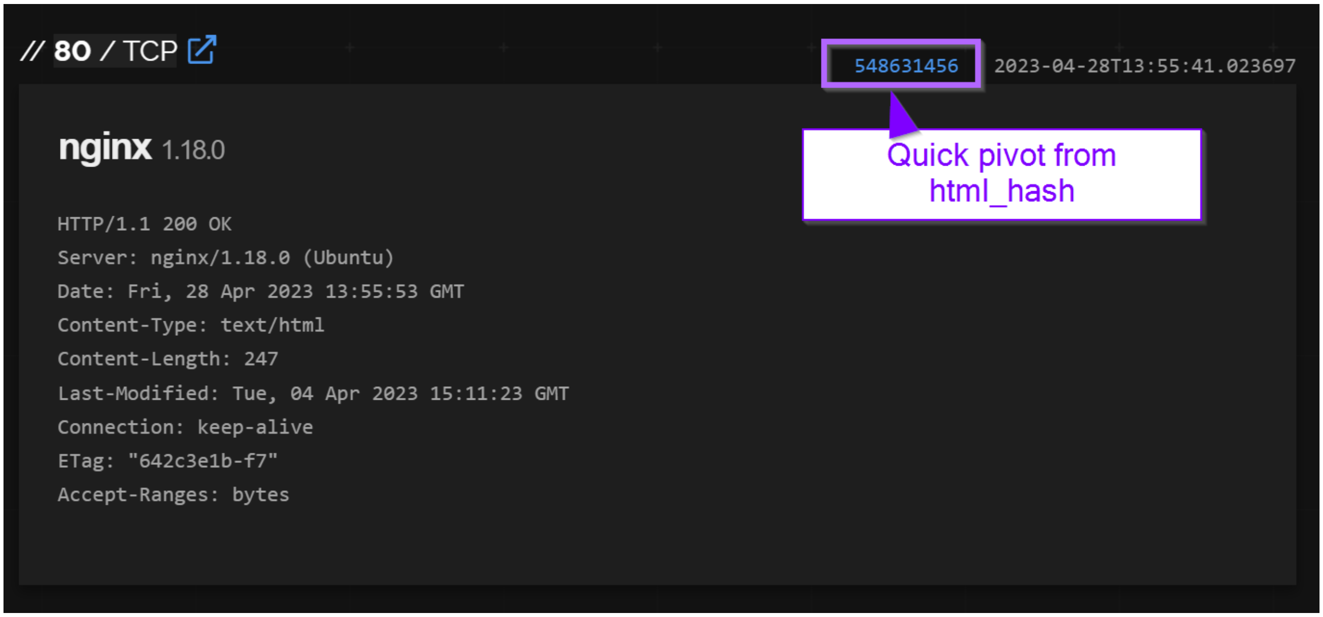
Sosi nahui! 2023-05-16T12:48:26.599642
77.91.124.242
desas.digital
hosted-by.yeezyhost.net
Foton Telecom CJSC
Russian Federation, Moscow
eol-product

SSL Certificate
Issued By:
|- Common Name:
R3
|- Organization:
Let's Encrypt
Issued To:
|- Common Name:
desas.digital
Supported SSL Versions:
TLSv1.2, TLSv1.3

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Tue, 16 May 2023 12:48:49 GMT
Content-Type: text/html
Content-Length: 247
Last-Modified: Tue, 04 Apr 2023 15:11:23 GMT
Connection: keep-alive
ETag: "642c3e1b-f7"
Accept-Ranges: bytes
```

At this point I was satisfied with my 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.



// 80 / TCP

548631456 2023-04-28T13:55:41.023697

Quick pivot from html_hash

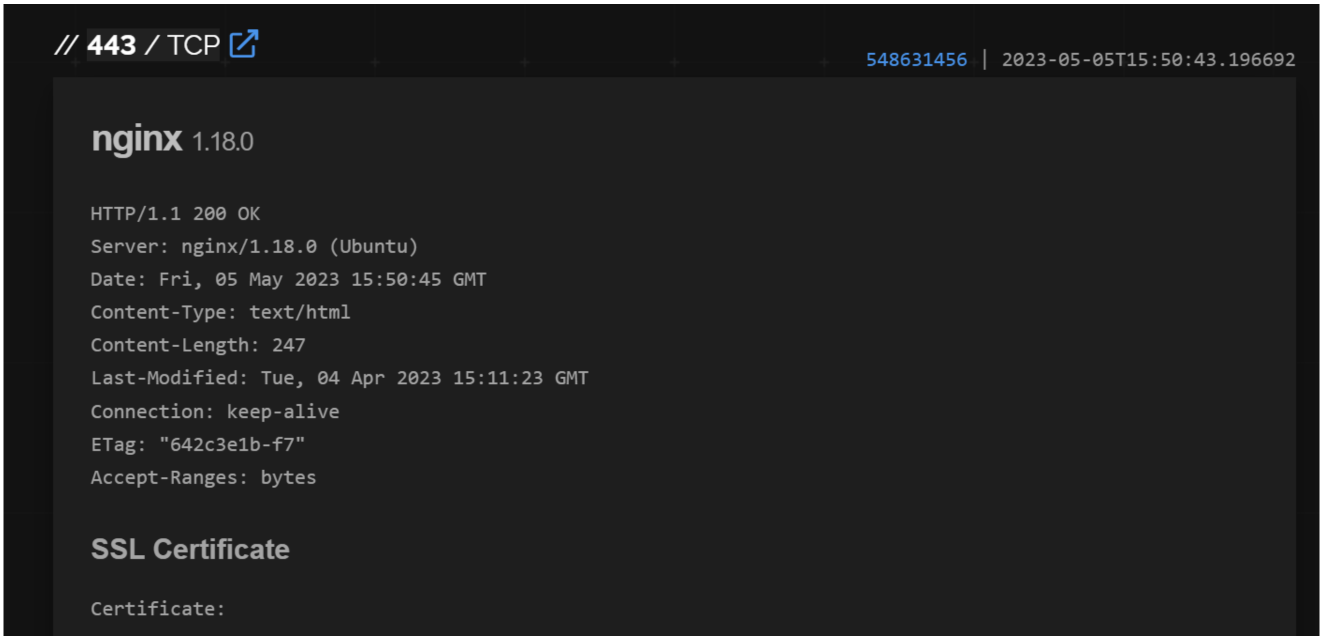
nginx 1.18.0

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Fri, 28 Apr 2023 13:55:53 GMT
Content-Type: text/html
Content-Length: 247
Last-Modified: Tue, 04 Apr 2023 15:11:23 GMT
Connection: keep-alive
ETag: "642c3e1b-f7"
Accept-Ranges: bytes
```

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.



// **443** / TCP

548631456 | 2023-05-05T15:50:43.196692

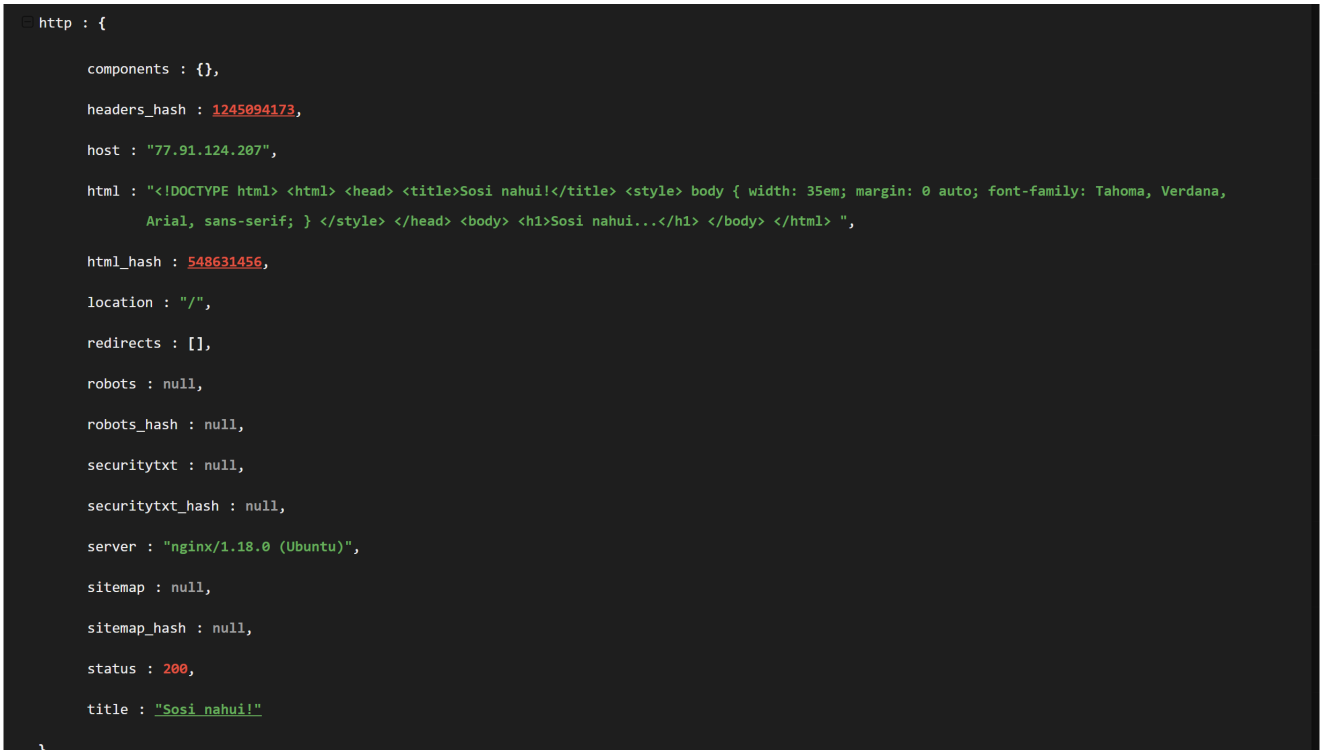
nginx 1.18.0

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Fri, 05 May 2023 15:50:45 GMT
Content-Type: text/html
Content-Length: 247
Last-Modified: Tue, 04 Apr 2023 15:11:23 GMT
Connection: keep-alive
ETag: "642c3e1b-f7"
Accept-Ranges: bytes
```

SSL Certificate

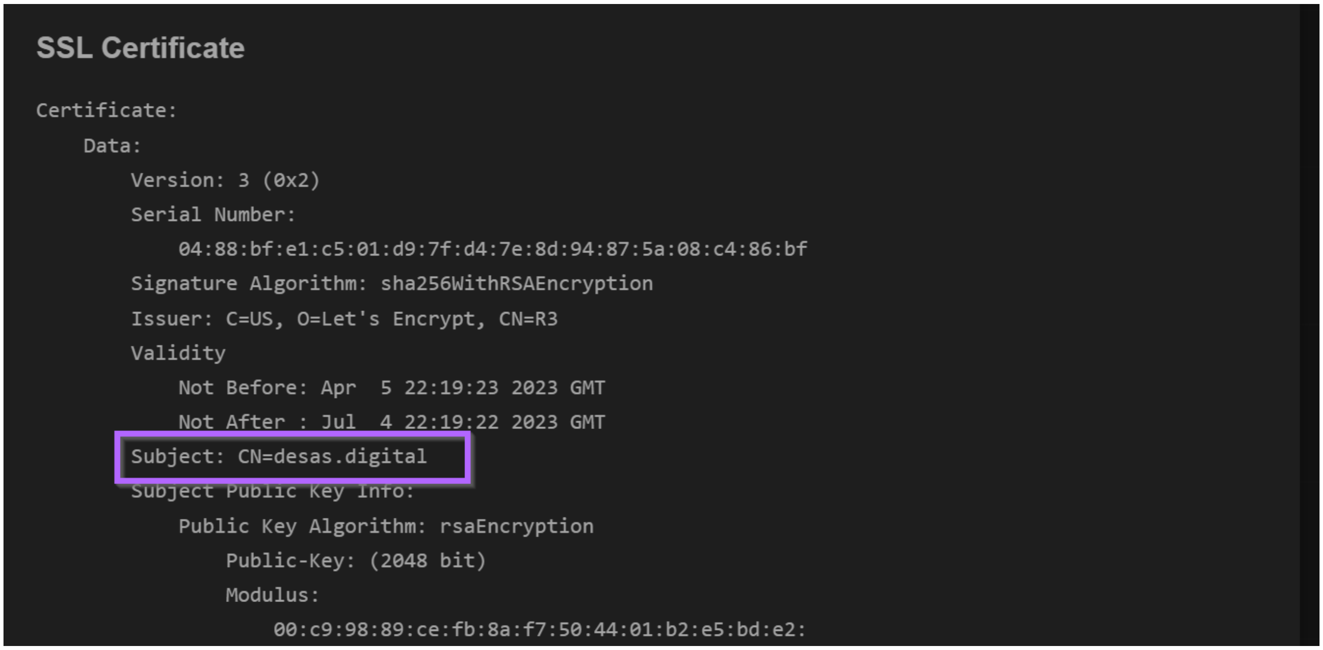
```
Certificate:
```

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



```
http : {
      components : {},
      headers_hash : 1245094173,
      host : "77.91.124.207",
      html : "<!DOCTYPE html> <html> <head> <title>Sosi nahui!</title> <style> body { width: 35em; margin: 0 auto; font-family: Tahoma, Verdana,
             Arial, sans-serif; } </style> </head> <body> <h1>Sosi nahui...</h1> </body> </html> ",
      html_hash : 548631456,
      location : "/",
      redirects : [],
      robots : null,
      robots_hash : null,
      securitytxt : null,
      securitytxt_hash : null,
      server : "nginx/1.18.0 (Ubuntu)",
      sitemap : null,
      sitemap_hash : null,
      status : 200,
      title : "Sosi nahui!"
}
```

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



SSL Certificate

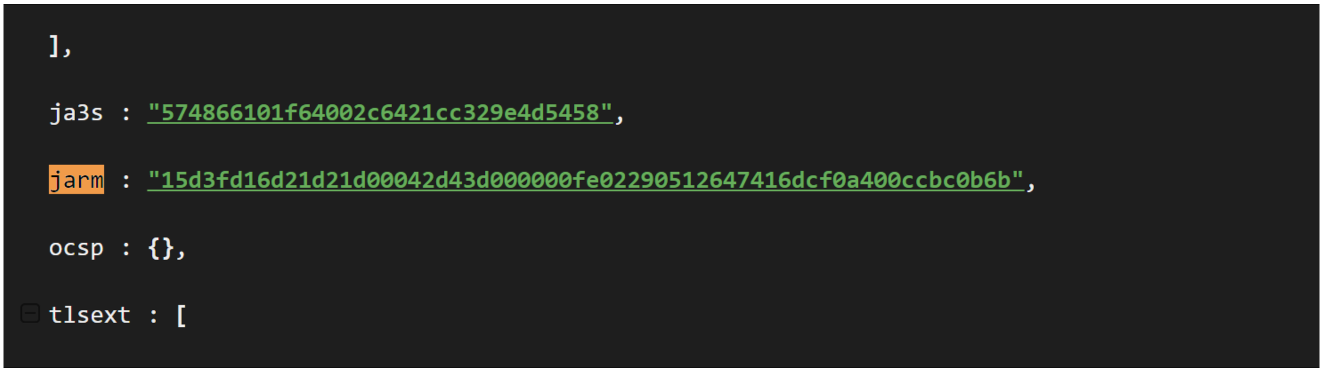
```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            04:88:bf:e1:c5:01:d9:7f:d4:7e:8d:94:87:5a:08:c4:86:bf
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=Let's Encrypt, CN=R3
        Validity
            Not Before: Apr  5 22:19:23 2023 GMT
            Not After : Jul  4 22:19:22 2023 GMT
        Subject: CN=desas.digital
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c9:98:89:ce:fb:8a:f7:50:44:01:b2:e5:bd:e2:
```

The rest of the certificate did not contain anything that I 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)

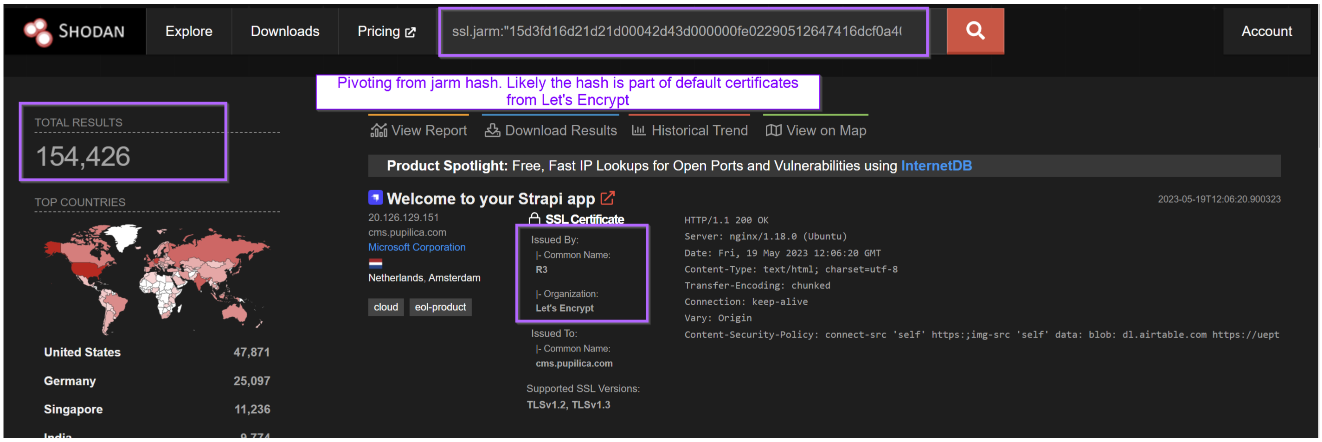


```
],

ja3s : "574866101f64002c6421cc329e4d5458",

jarm : "15d3fd16d21d21d00042d43d000000fe02290512647416dcf0a400ccbc0b6b",

ocsp : {},

tlsext : [
```

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

I 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.



ssl.jarm:"15d3fd16d21d21d00042d43d000000fe02290512647416dcf0a4(

Pivoting from jarm hash. Likely the hash is part of default certificates from Let's Encrypt

TOTAL RESULTS
154,426

TOP COUNTRIES

United States	47,871
Germany	25,097
Singapore	11,236
India	9,774

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

Welcome to your Strapi app 2023-05-19T12:06:20.900323

20.126.129.151
cms.pupilica.com
Microsoft Corporation
Netherlands, Amsterdam
cloud eol-product

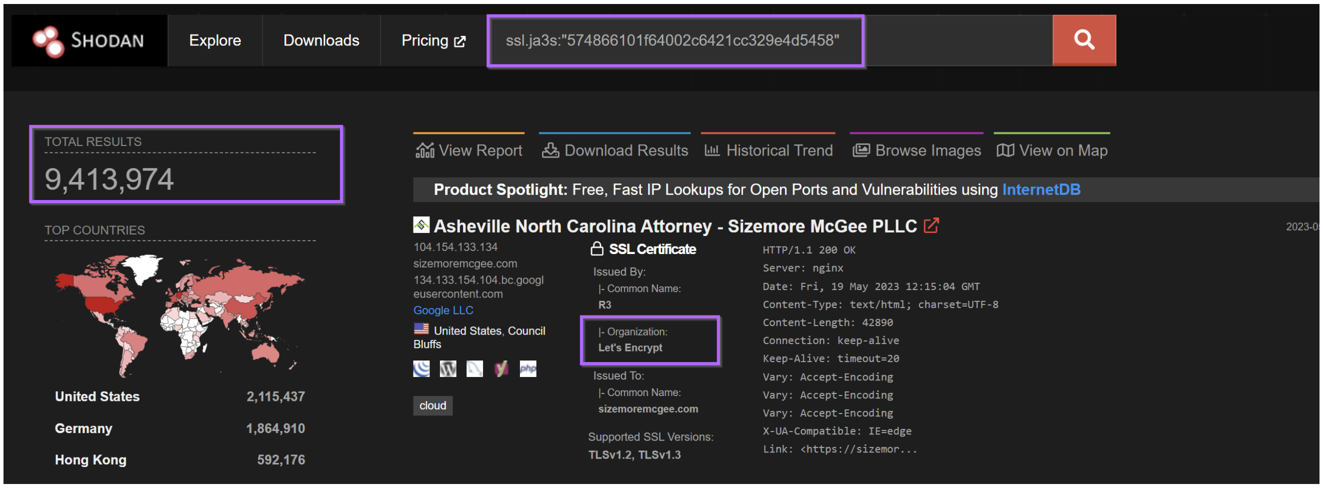
SSL Certificate
Issued By:
|- Common Name:
R3
|- Organization:
Let's Encrypt
Issued To:
|- Common Name:
cms.pupilica.com
Supported SSL Versions:
TLSv1.2, TLSv1.3

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Fri, 19 May 2023 12:06:20 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Origin
Content-Security-Policy: connect-src 'self' https:;img-src 'self' data: blob: dl.airtable.com https://uept
```

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 I decided not to pursue this route when 9 Million results were returned.



ssl.ja3s:"574866101f64002c6421cc329e4d5458"

TOTAL RESULTS
9,413,974

TOP COUNTRIES

United States	2,115,437
Germany	1,864,910
Hong Kong	592,176

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

Asheville North Carolina Attorney - Sizemore McGee PLLC 2023-0

104.154.133.134
sizemoremcgee.com
134.133.154.104.bc.googleusercontent.com
Google LLC
United States, Council Bluffs
cloud

SSL Certificate
Issued By:
|- Common Name:
R3
|- Organization:
Let's Encrypt
Issued To:
|- Common Name:
sizemoremcgee.com
Supported SSL Versions:
TLSv1.2, TLSv1.3

```
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 19 May 2023 12:15:04 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 42890
Connection: keep-alive
Keep-Alive: timeout=20
Vary: Accept-Encoding
Vary: Accept-Encoding
Vary: Accept-Encoding
X-UA-Compatible: IE=edge
Link: <https://sizemor...
```

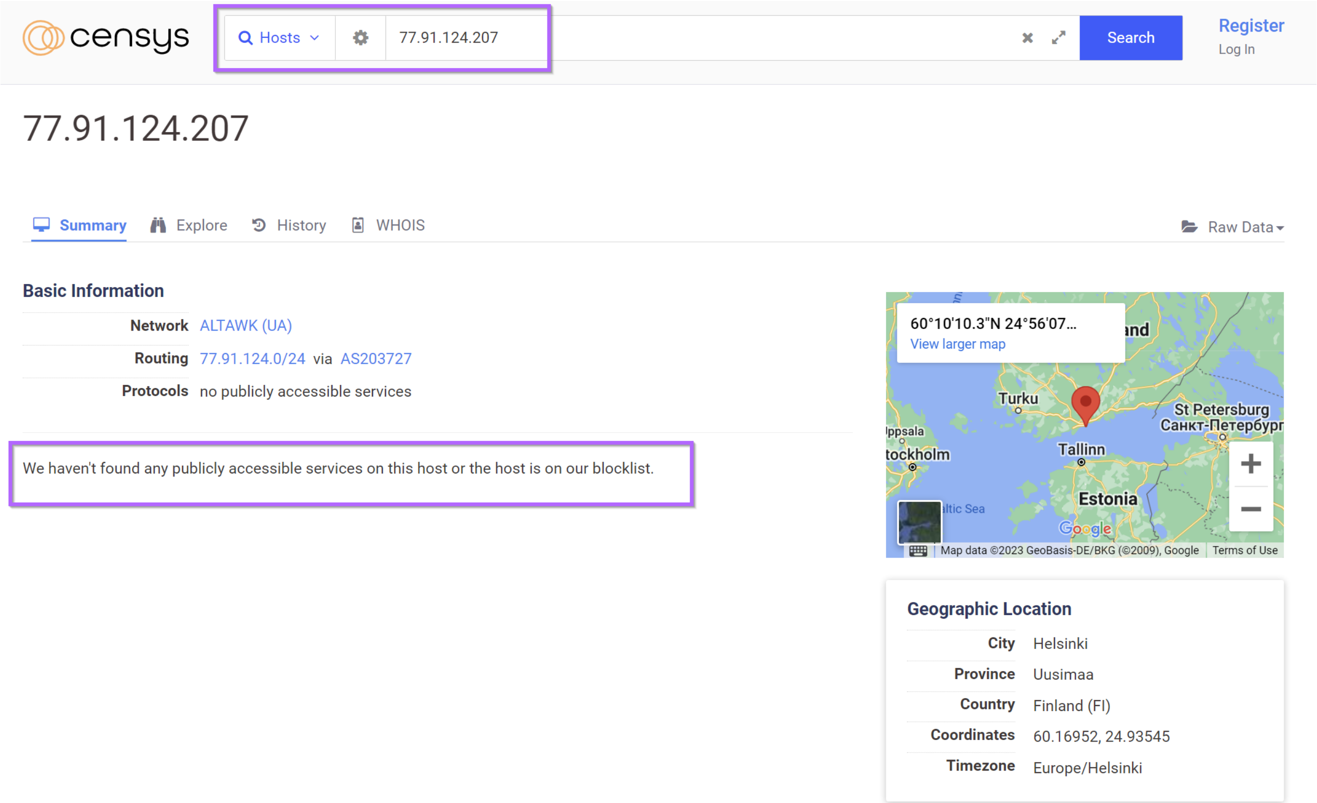
I then moved on to Censys to continue analysis.

Analysing Infrastructure With Censys

Continuing analysis using Censys, I 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.



77.91.124.207

Basic Information

Network	ALTAWK (UA)
Routing	77.91.124.0/24 via AS203727
Protocols	no publicly accessible services

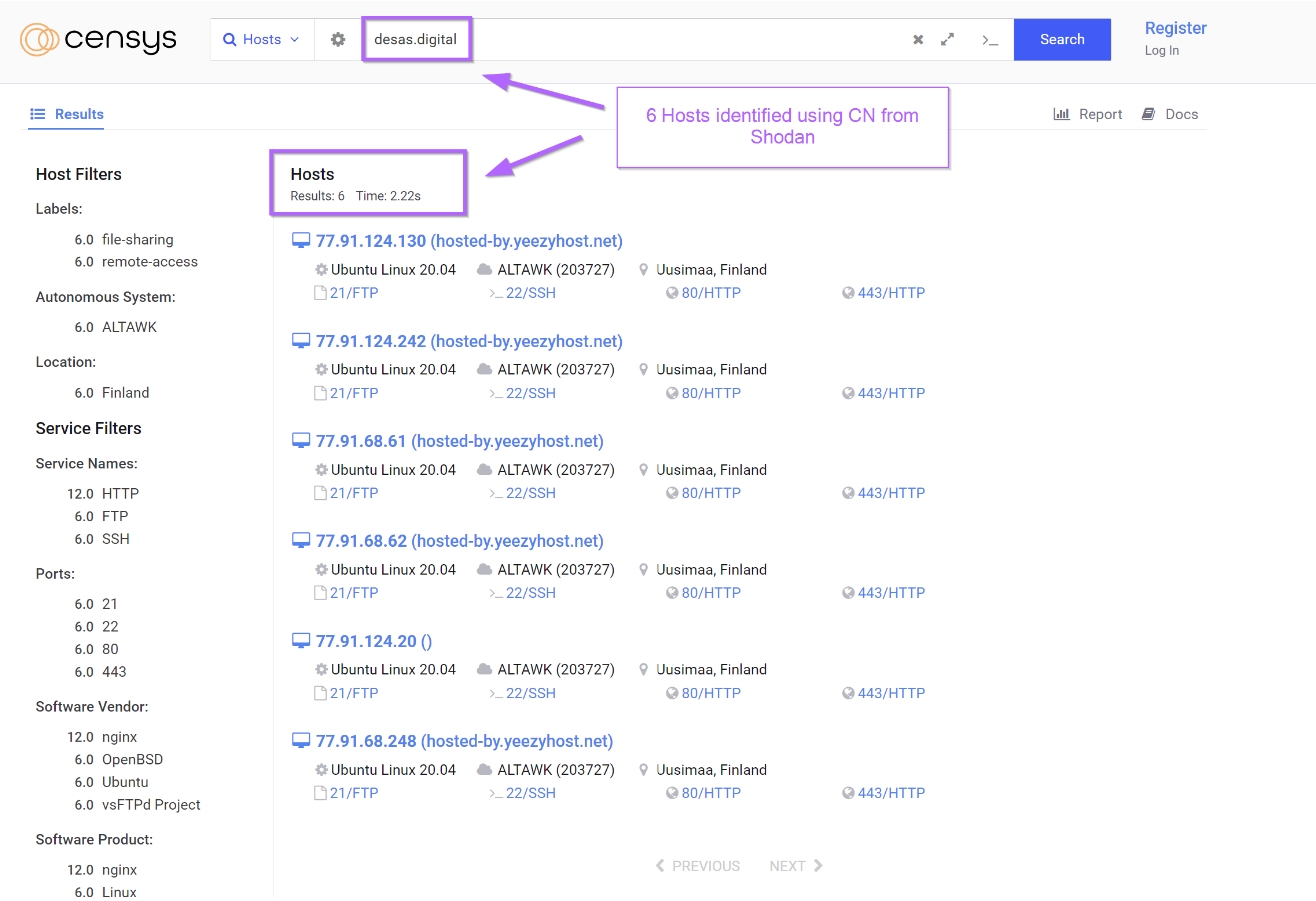
We haven't found any publicly accessible services on this host or the host is on our blocklist.

Geographic Location

City	Helsinki
Province	Uusimaa
Country	Finland (FI)
Coordinates	60.16952, 24.93545
Timezone	Europe/Helsinki

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.



desas.digital

6 Hosts identified using CN from Shodan

Hosts
Results: 6 Time: 2.22s

Host Filters

Labels:

6.0 file-sharing
6.0 remote-access

Autonomous System:

6.0 ALTAWK

Location:

6.0 Finland

Service Filters

Service Names:

12.0 HTTP
6.0 FTP
6.0 SSH

Ports:

6.0 21
6.0 22
6.0 80
6.0 443

Software Vendor:

12.0 nginx
6.0 OpenBSD
6.0 Ubuntu
6.0 vsFTPd Project

Software Product:

12.0 nginx
6.0 Linux

77.91.124.130 (hosted-by.yeezyhost.net)
Ubuntu Linux 20.04 ALTAWK (203727) Uusimaa, Finland
21/FTP 22/SSH 80/HTTP 443/HTTP

77.91.124.242 (hosted-by.yeezyhost.net)
Ubuntu Linux 20.04 ALTAWK (203727) Uusimaa, Finland
21/FTP 22/SSH 80/HTTP 443/HTTP

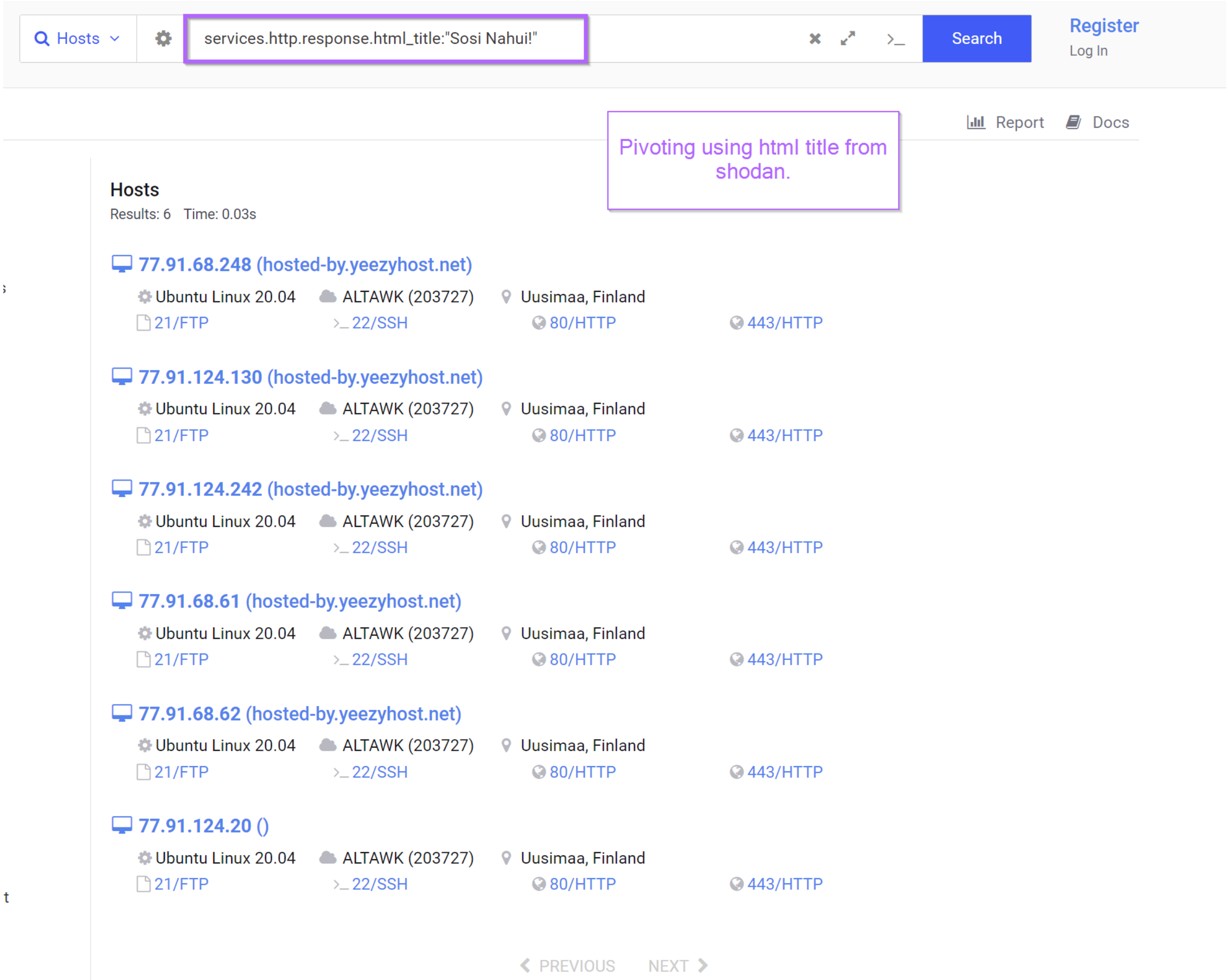
77.91.68.61 (hosted-by.yeezyhost.net)
Ubuntu Linux 20.04 ALTAWK (203727) Uusimaa, Finland
21/FTP 22/SSH 80/HTTP 443/HTTP

77.91.68.62 (hosted-by.yeezyhost.net)
Ubuntu Linux 20.04 ALTAWK (203727) Uusimaa, Finland
21/FTP 22/SSH 80/HTTP 443/HTTP

77.91.124.20 ()
Ubuntu Linux 20.04 ALTAWK (203727) Uusimaa, Finland
21/FTP 22/SSH 80/HTTP 443/HTTP

77.91.68.248 (hosted-by.yeezyhost.net)
Ubuntu Linux 20.04 ALTAWK (203727) Uusimaa, Finland
21/FTP 22/SSH 80/HTTP 443/HTTP

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



services.http.response.html_title:"Sosi Nahui!"

Pivoting using html title from shodan.

Hosts

Results: 6 Time: 0.03s

77.91.68.248 (hosted-by.yeezyhost.net)
Ubuntu Linux 20.04 ALTAWK (203727) Uusimaa, Finland
21/FTP 22/SSH 80/HTTP 443/HTTP

77.91.124.130 (hosted-by.yeezyhost.net)
Ubuntu Linux 20.04 ALTAWK (203727) Uusimaa, Finland
21/FTP 22/SSH 80/HTTP 443/HTTP

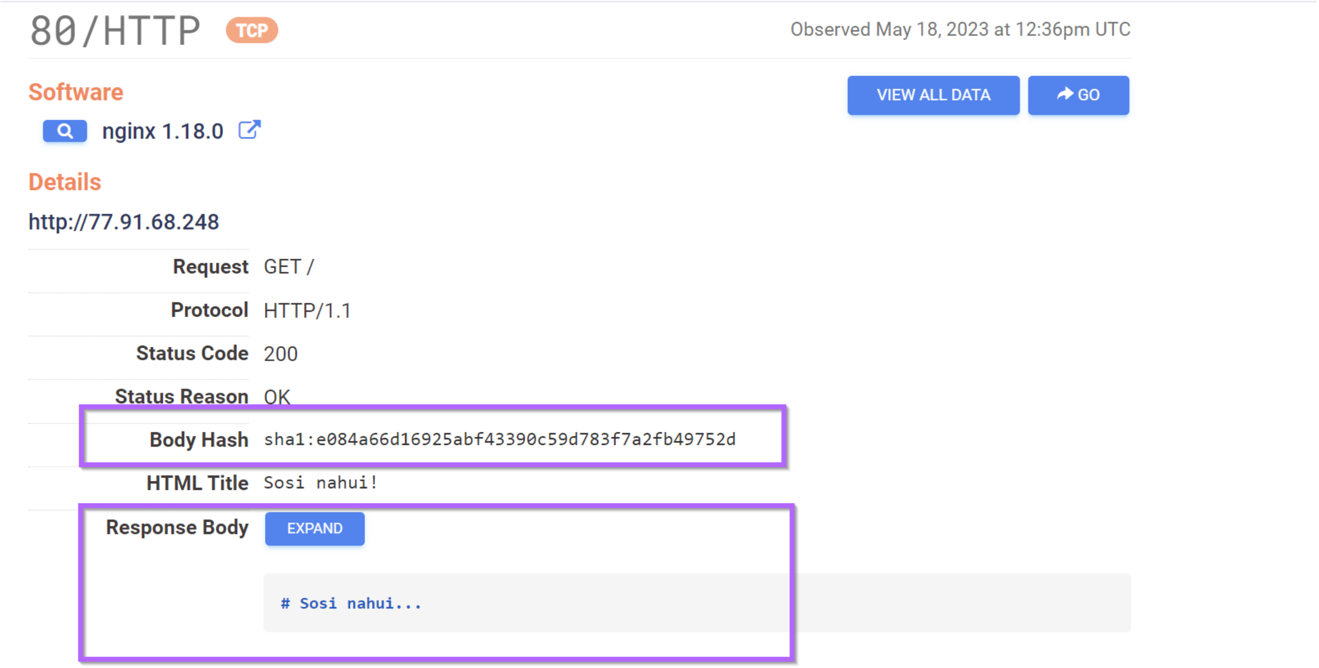
77.91.124.242 (hosted-by.yeezyhost.net)
Ubuntu Linux 20.04 ALTAWK (203727) Uusimaa, Finland
21/FTP 22/SSH 80/HTTP 443/HTTP

77.91.68.61 (hosted-by.yeezyhost.net)
Ubuntu Linux 20.04 ALTAWK (203727) Uusimaa, Finland
21/FTP 22/SSH 80/HTTP 443/HTTP

77.91.68.62 (hosted-by.yeezyhost.net)
Ubuntu Linux 20.04 ALTAWK (203727) Uusimaa, Finland
21/FTP 22/SSH 80/HTTP 443/HTTP

77.91.124.20 ()
Ubuntu Linux 20.04 ALTAWK (203727) Uusimaa, Finland
21/FTP 22/SSH 80/HTTP 443/HTTP

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


80/HTTP TCP

Observed May 18, 2023 at 12:36pm UTC

Software

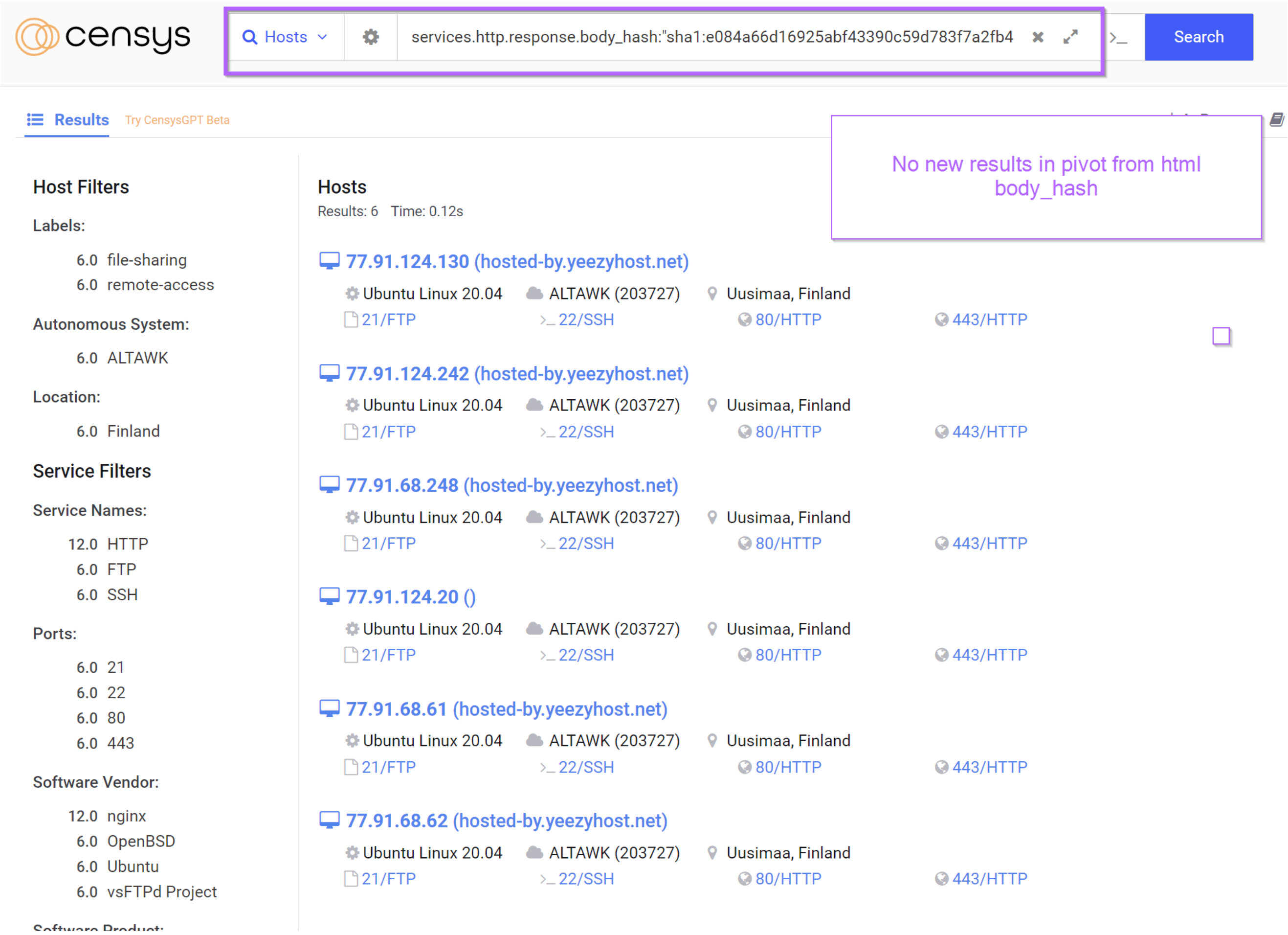
nginx 1.18.0

Details

http://77.91.68.248

Request	GET /
Protocol	HTTP/1.1
Status Code	200
Status Reason	OK
Body Hash	sha1:e084a66d16925abf43390c59d783f7a2fb49752d
HTML Title	Sosi nahui!
Response Body	EXPAND # Sosi nahui...

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



services.http.response.body_hash:"sha1:e084a66d16925abf43390c59d783f7a2fb4

No new results in pivot from html body_hash

Host Filters

Labels:
6.0 file-sharing
6.0 remote-access

Autonomous System:
6.0 ALTAWK

Location:
6.0 Finland

Service Filters

Service Names:
12.0 HTTP
6.0 FTP
6.0 SSH

Ports:
6.0 21
6.0 22
6.0 80
6.0 443

Software Vendor:
12.0 nginx
6.0 OpenBSD
6.0 Ubuntu
6.0 vsFTPd Project

Software Product:

Hosts
Results: 6 Time: 0.12s

77.91.124.130 (hosted-by.yeezyhost.net)
Ubuntu Linux 20.04 ALTAWK (203727) Uusimaa, Finland
21/FTP 22/SSH 80/HTTP 443/HTTP

77.91.124.242 (hosted-by.yeezyhost.net)
Ubuntu Linux 20.04 ALTAWK (203727) Uusimaa, Finland
21/FTP 22/SSH 80/HTTP 443/HTTP

77.91.68.248 (hosted-by.yeezyhost.net)
Ubuntu Linux 20.04 ALTAWK (203727) Uusimaa, Finland
21/FTP 22/SSH 80/HTTP 443/HTTP

77.91.124.20 ()
Ubuntu Linux 20.04 ALTAWK (203727) Uusimaa, Finland
21/FTP 22/SSH 80/HTTP 443/HTTP

77.91.68.61 (hosted-by.yeezyhost.net)
Ubuntu Linux 20.04 ALTAWK (203727) Uusimaa, Finland
21/FTP 22/SSH 80/HTTP 443/HTTP

77.91.68.62 (hosted-by.yeezyhost.net)
Ubuntu Linux 20.04 ALTAWK (203727) Uusimaa, Finland
21/FTP 22/SSH 80/HTTP 443/HTTP

Continuing analysis, I was unable to identify any additional servers with Shodan or Censys.

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

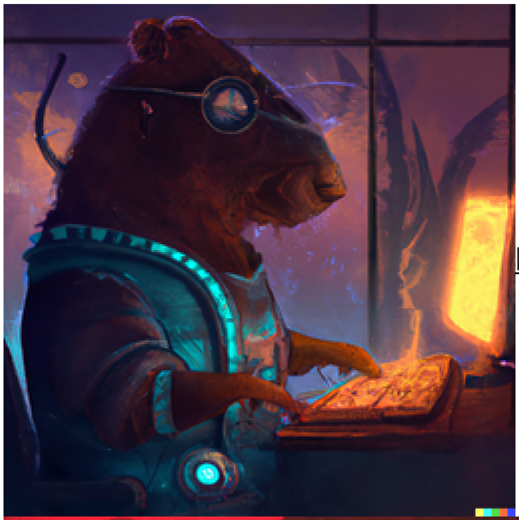
Conclusion

At this point I was happy with the 12 unique servers initially identified by Shodan and I decided to call it a day. These 12 servers all shared extremely similar html content, location and certificate information so I 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
```