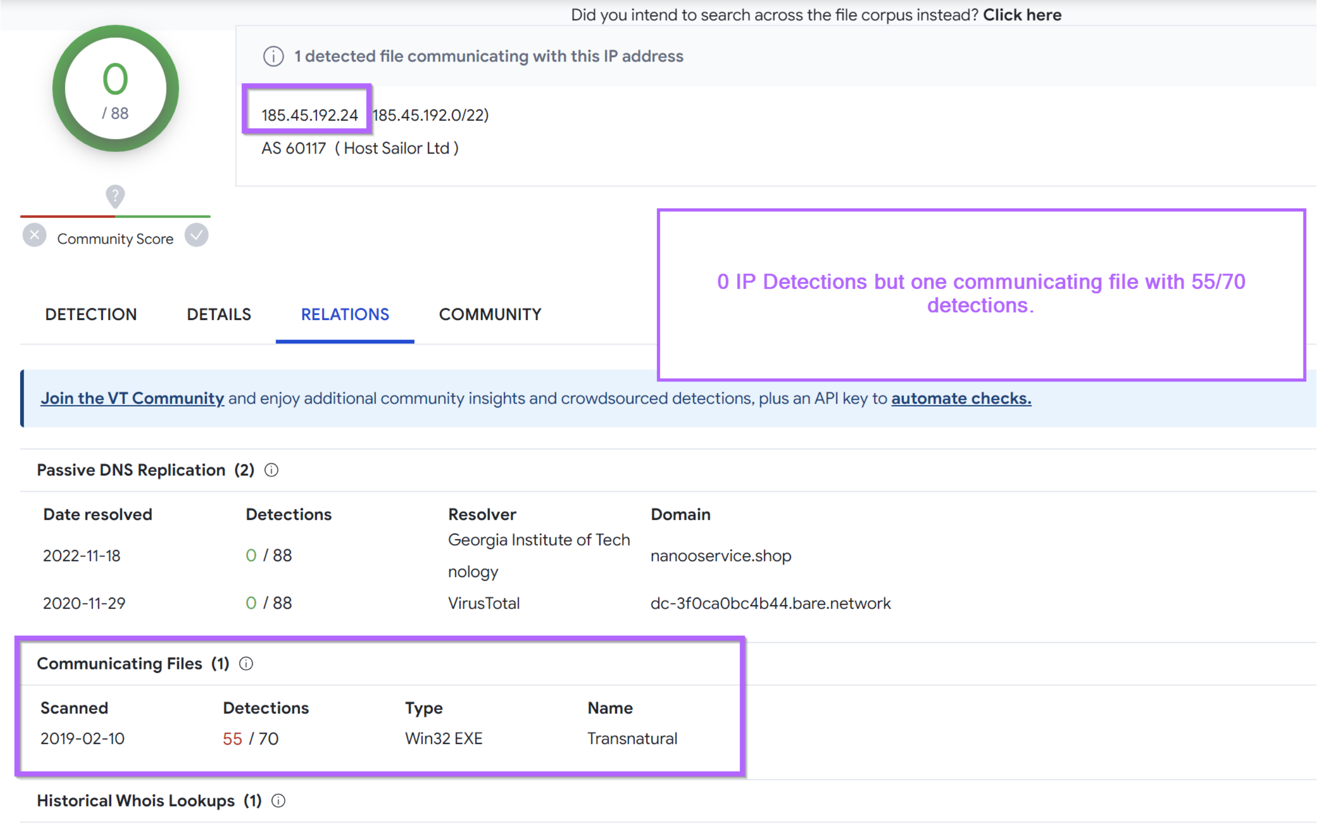
Identifying Suspected PrivateLoader Servers with Censys

embee-research.ghost.io/identifying-privateloader-servers-with-censys/

Matthew November 26, 2023

Beginner

Refining Queries and Identifying Suspicious servers using Censys.



Did you intend to search across the file corpus instead? **Click here**

0 / 88

Community Score

1 detected file communicating with this IP address

185.45.192.24 (185.45.192.0/22)

AS 60117 (Host Sailor Ltd)

0 IP Detections but one communicating file with 55/70 detections.

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to **automate checks.**

Passive DNS Replication (2)

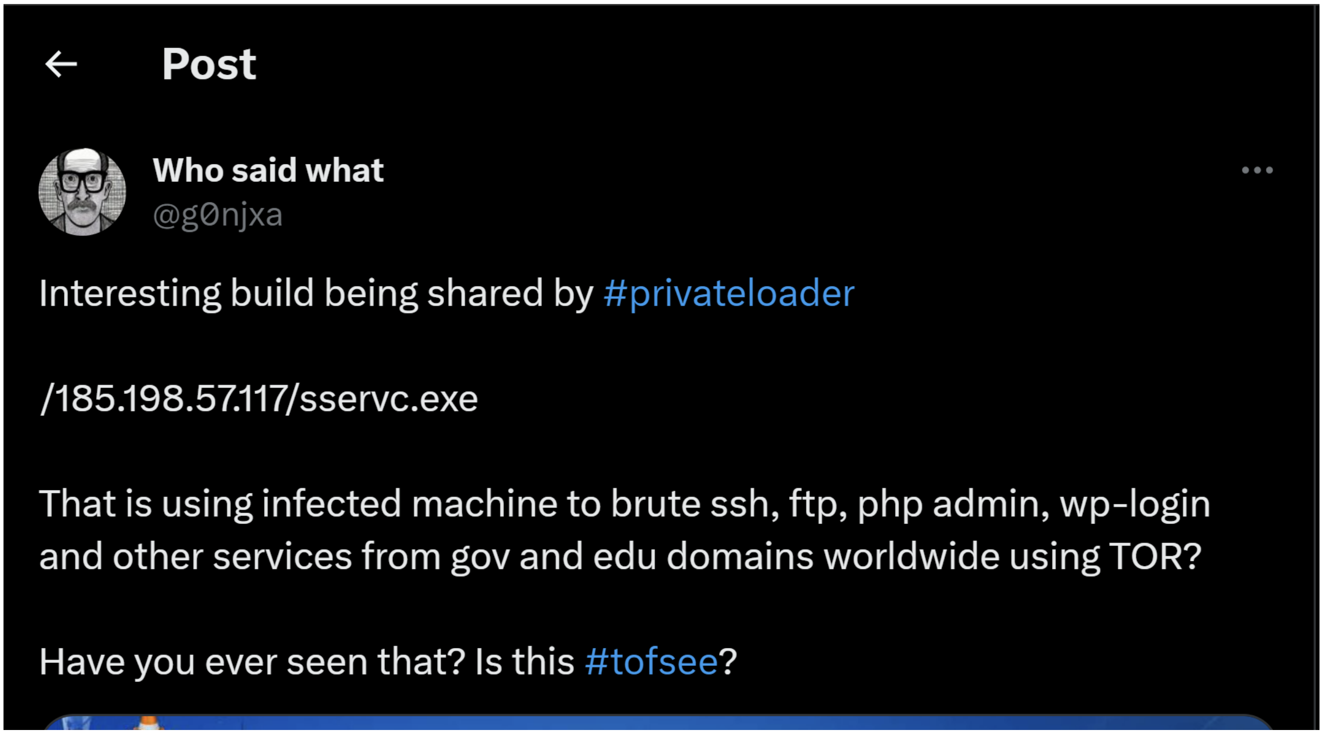
Date resolved	Detections	Resolver	Domain
2022-11-18	0 / 88	Georgia Institute of Technology	nanooservice.shop
2020-11-29	0 / 88	VirusTotal	dc-3f0ca0bc4b44.bare.network

Communicating Files (1)

Scanned	Detections	Type	Name
2019-02-10	55 / 70	Win32 EXE	Transnatural

Historical Whois Lookups (1)

This is a quick post based on a tweet shared by @g0njxa. Here we will build a Censys query to identify servers related to an IP related to PrivateLoader.



Post

Who said what
@g0njxa

Interesting build being shared by #privateloader

/185.198.57.117/sservc.exe

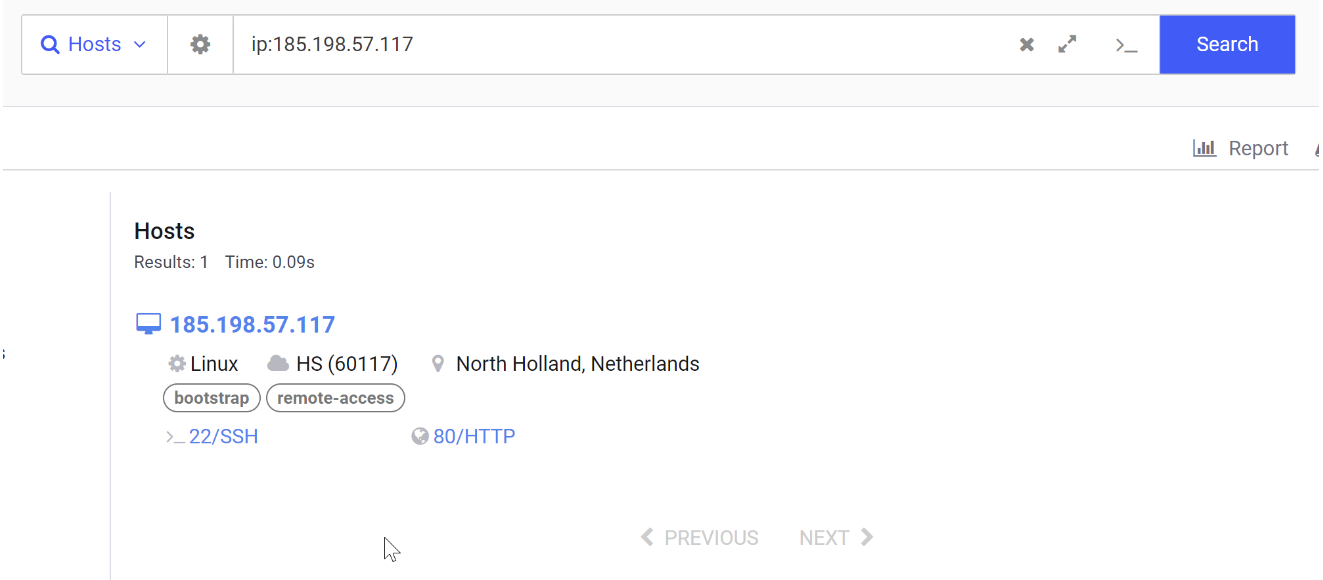
That is using infected machine to brute ssh, ftp, php admin, wp-login and other services from gov and edu domains worldwide using TOR?

Have you ever seen that? Is this #tofsee?

Initial Search

We can begin with an initial search on the IP Address using `ip:185.198.57[.]117` .

This shows that the ip address is running two services on port 22 (SSH) and 80 (HTTP).



ip:185.198.57.117

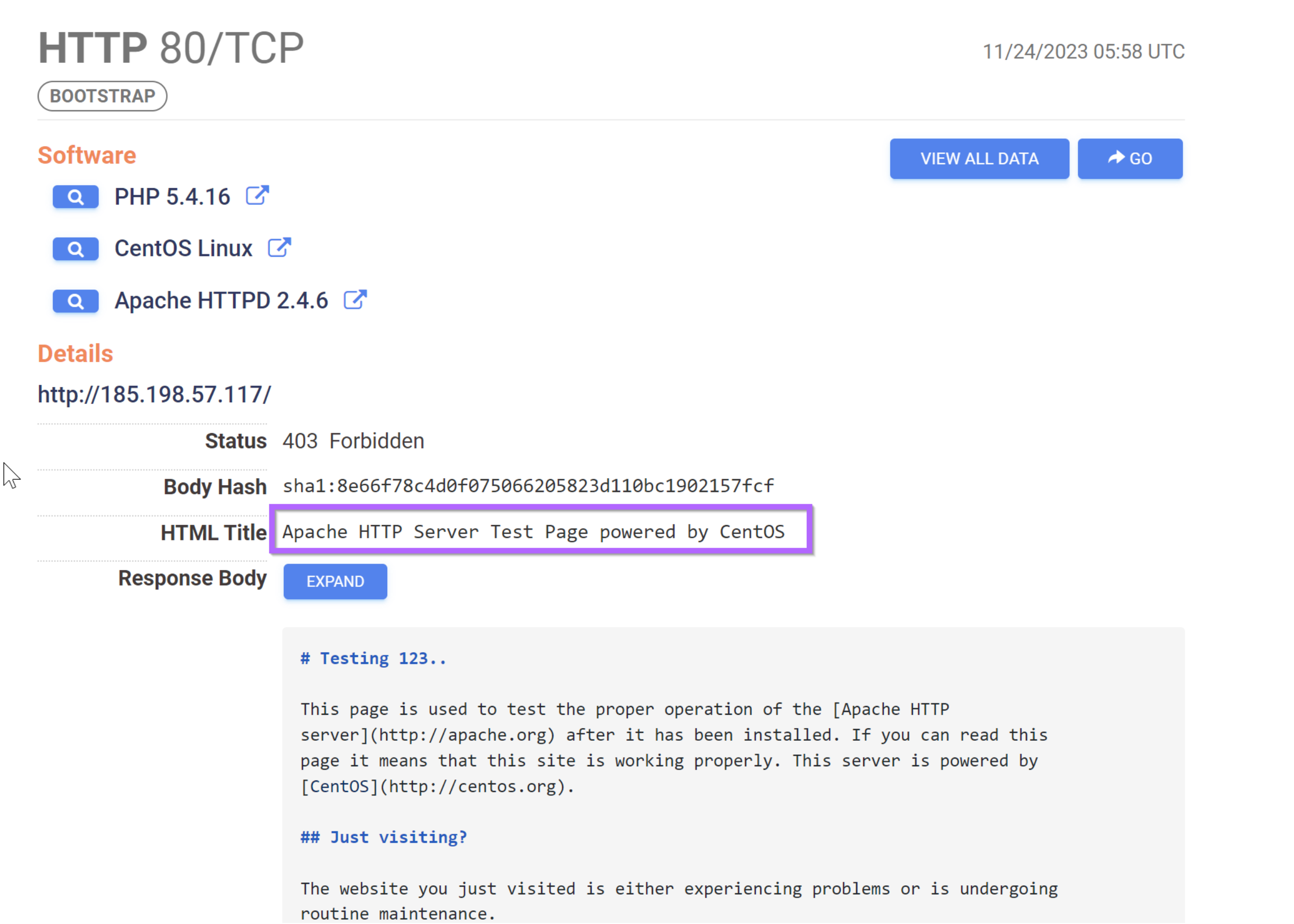
Hosts
Results: 1 Time: 0.09s

185.198.57.117
Linux HS (60117) North Holland, Netherlands
bootstrap remote-access
22/SSH 80/HTTP

Investigating the address further, we can see a standard looking setup on SSH and a simple Apache server on port 80.

Within the HTTP Service, there is a relatively long HTTP Title containing `Apache HTTP Server Test Page powered by CentOS`.

> There is also a very long response body which appears to be a default Apache page. I made the assumption that the Title and Body are both defaults and hence it doesn't really matter which one is used as a pivot.



HTTP 80/TCP

11/24/2023 05:58 UTC

BOOTSTRAP

Software

- PHP 5.4.16
- CentOS Linux
- Apache HTTPD 2.4.6

Details

http://185.198.57.117/

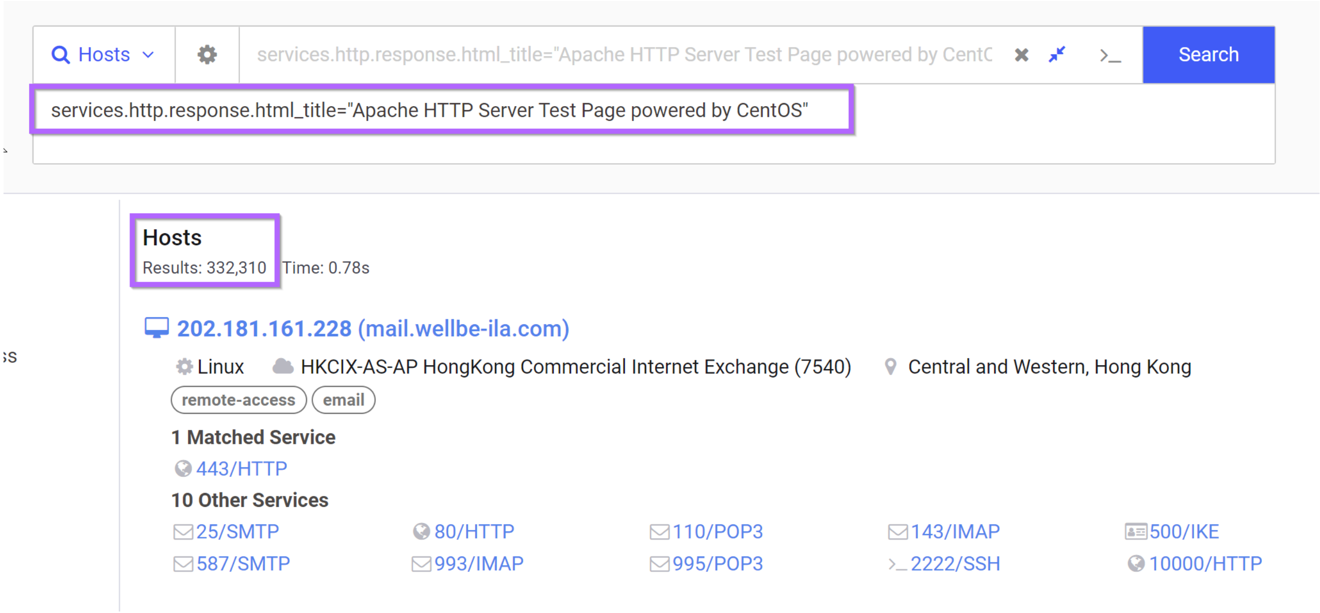
Status	403 Forbidden
Body Hash	sha1:8e66f78c4d0f075066205823d110bc1902157fcf
HTML Title	Apache HTTP Server Test Page powered by CentOS
Response Body	

```
# Testing 123..

This page is used to test the proper operation of the [Apache HTTP
server](http://apache.org) after it has been installed. If you can read this
page it means that this site is working properly. This server is powered by
[CentOS](http://centos.org).

## Just visiting?

The website you just visited is either experiencing problems or is undergoing
routine maintenance.
```

Now so far everything looks "default" and not easily signatured, but we can still go ahead and attempt a pivot on the HTML Title.

```
services.http.response.html_title="Apache HTTP Server Test Page powered by CentOS"
```

This returns ~332,310 results. Which is way too many for the HTML Title to be used on it's own.


Hosts
Search
services.http.response.html_title="Apache HTTP Server Test Page powered by CentC

services.http.response.html_title="Apache HTTP Server Test Page powered by CentOS"

Hosts
Results: 332,310 Time: 0.78s

202.181.161.228 (mail.wellbe-ila.com)
Linux HKCIX-AS-AP HongKong Commercial Internet Exchange (7540) Central and Western, Hong Kong
remote-access email
1 Matched Service
443/HTTP
10 Other Services
25/SMTP 80/HTTP 110/POP3 143/IMAP 500/IKE
587/SMTP 993/IMAP 995/POP3 2222/SSH 10000/HTTP

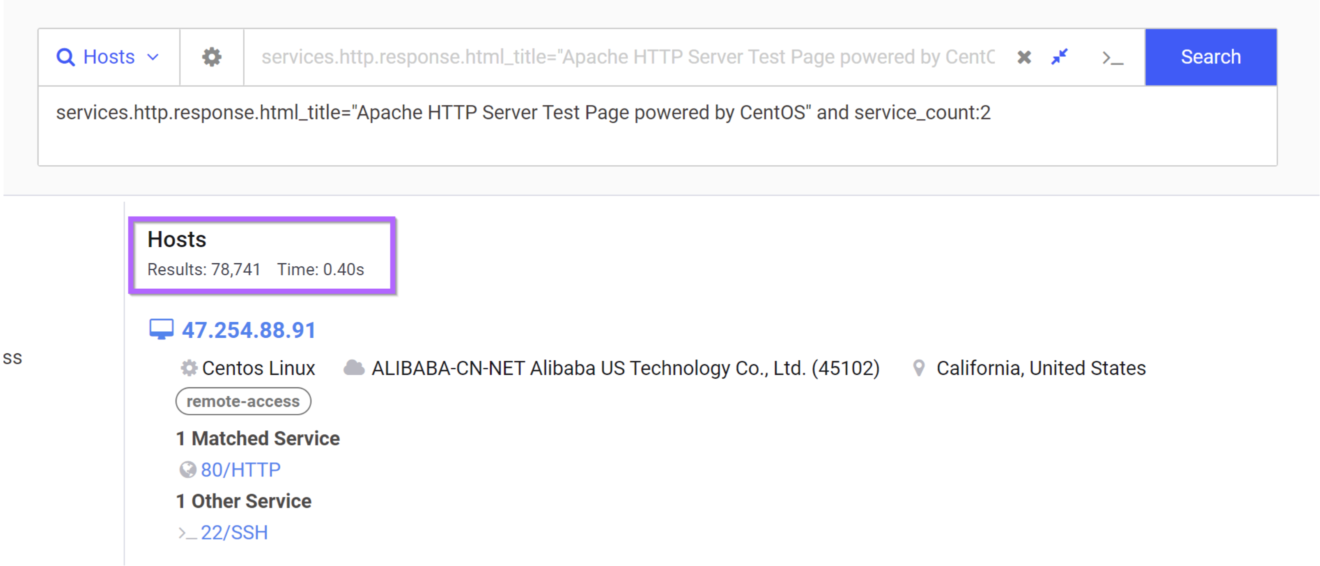
Refining The Query By Limiting Service Count

If we recall from the initial search on the ip, there are only two running services (SSH and HTTP).

We can use this information to limit the search to servers with only 2 running services.

```
services.http.response.html_title="Apache HTTP Server Test Page powered by CentOS" and service_count:2
```

This reduces the results down to `78,741`. Not great but much better than before.


Hosts
Search
services.http.response.html_title="Apache HTTP Server Test Page powered by CentC

services.http.response.html_title="Apache HTTP Server Test Page powered by CentOS" and service_count:2

Hosts
Results: 78,741 Time: 0.40s

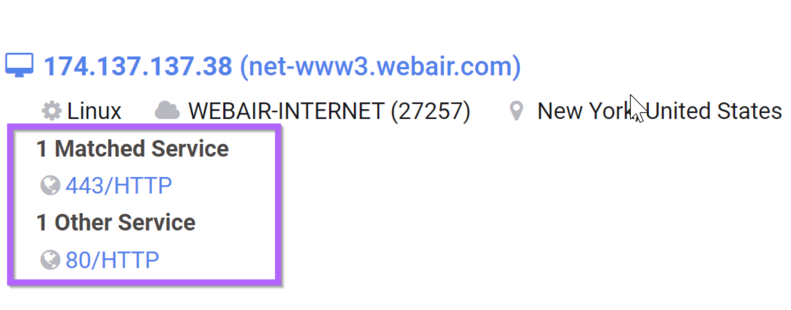
47.254.88.91
Centos Linux ALIBABA-CN-NET Alibaba US Technology Co., Ltd. (45102) California, United States
remote-access
1 Matched Service
80/HTTP
1 Other Service
22/SSH

Refining Results by Providing Specific Ports

If we look at the second result from our previous search, we can see that it is running two services.

One on port 80, and one on port 443.

We can go ahead and remove these by specifying that we only want servers with port 22 and 80.



174.137.137.38 (net-www3.webair.com)

Linux WEBAIR-INTERNET (27257) New York, United States

1 Matched Service

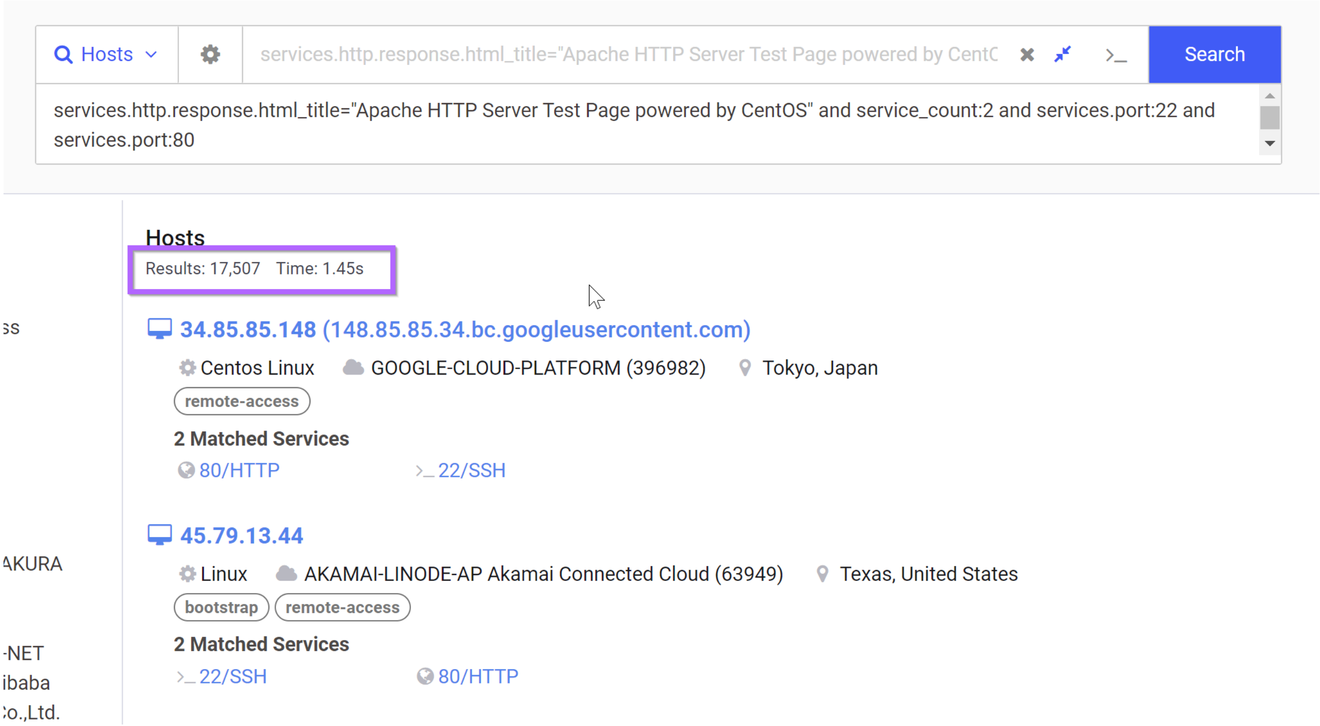
443/HTTP

1 Other Service

80/HTTP

We can refine our search with the query below, which cuts down the results to ~17000

```
services.http.response.html_title="Apache HTTP Server Test Page powered by
CentOS" and service_count:2 and services.port:22 and services.port:80
```



services.http.response.html_title="Apache HTTP Server Test Page powered by CentOS" and service_count:2 and services.port:22 and services.port:80

Hosts

Results: 17,507 Time: 1.45s

34.85.85.148 (148.85.85.34.bc.googleusercontent.com)

Centos Linux GOOGLE-CLOUD-PLATFORM (396982) Tokyo, Japan

remote-access

2 Matched Services

80/HTTP 22/SSH

45.79.13.44

Linux AKAMAI-LINODE-AP Akamai Connected Cloud (63949) Texas, United States

bootstrap remote-access

2 Matched Services

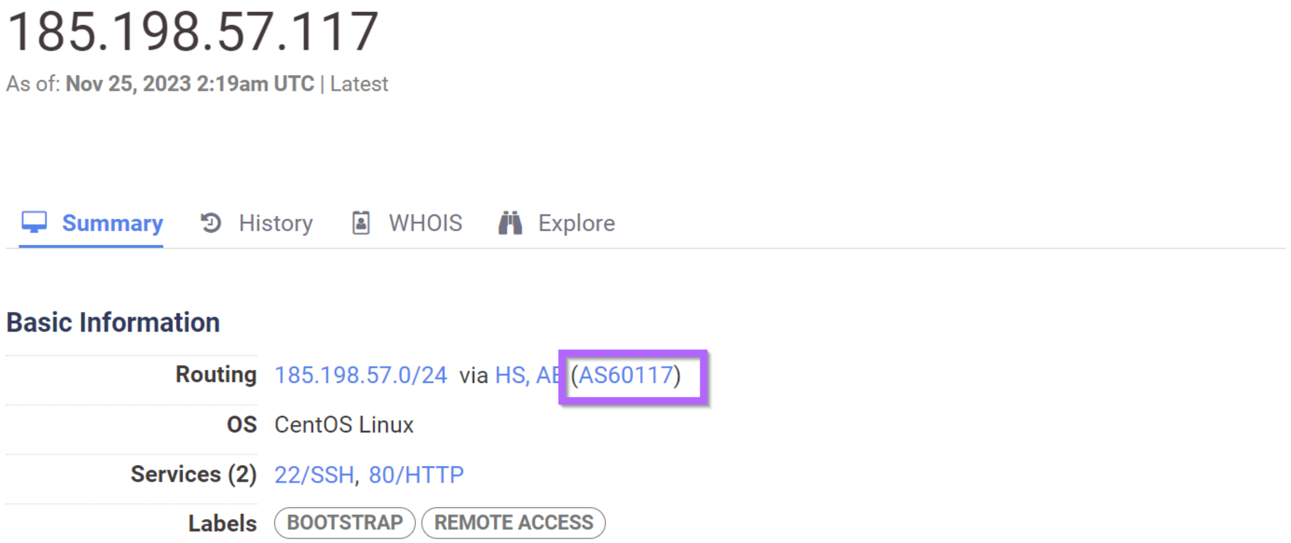
22/SSH 80/HTTP

Now at this point I wasn't able to find any other useful pivot points within the HTTP or SSH services.

We can go ahead and pivot using the Autonomous System Number (ASN). This limits the results to servers/ips within a similar geographic location (or at least hosted by a similar hosting provider).

> In my experience, the ASN should be used as a last resort when no other pivot points can be found. If an actor has set up their infrastructure well, then there will be servers across multiple ASN's and geographic locations. Limiting to a single ASN will miss servers in a separate location, but it's very useful when there aren't other options.

We can see the ASN number in the summary for the initial IP address.



185.198.57.117

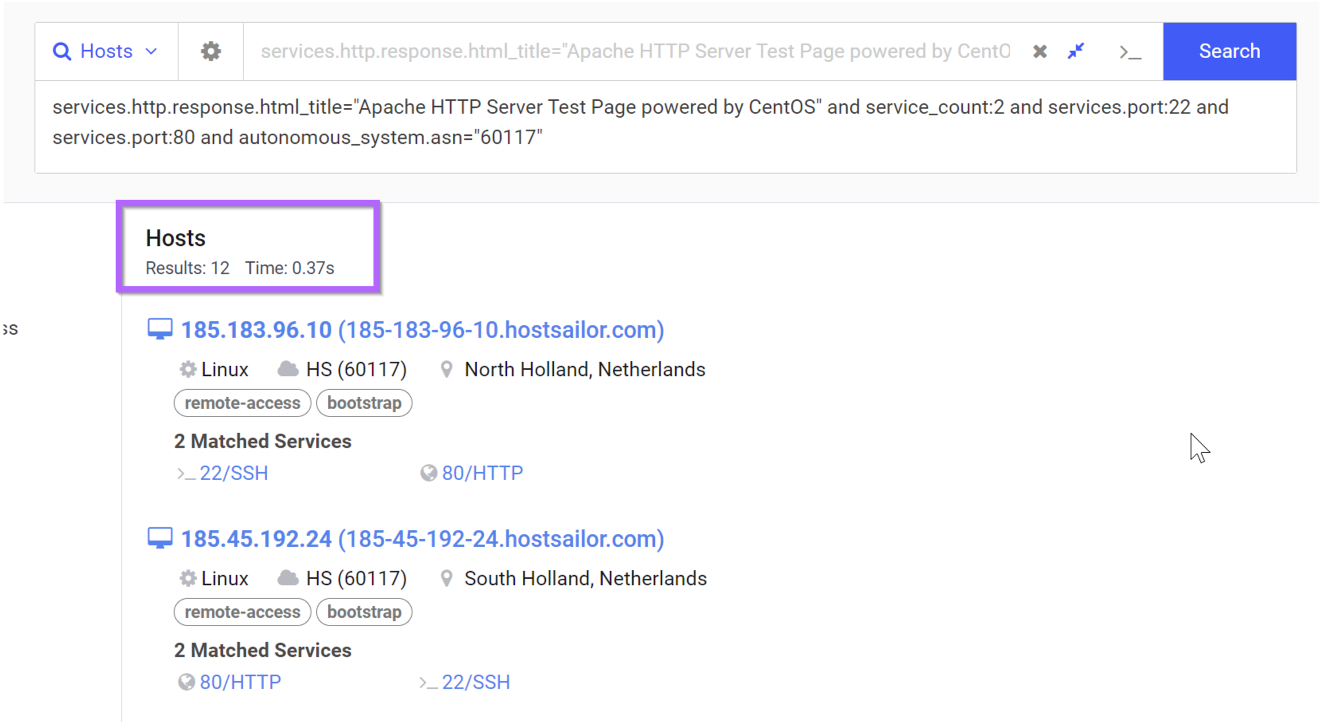
As of: **Nov 25, 2023 2:19am UTC** | Latest

Basic Information

Routing	185.198.57.0/24 via HS, AB (AS60117)
OS	CentOS Linux
Services (2)	22/SSH, 80/HTTP
Labels	BOOTSTRAP REMOTE ACCESS

Now with the ASN Number added, we are down to only 12 results. A number as small as 12 is a good indicator that the results are all related.

```
services.http.response.html_title="Apache HTTP Server Test Page powered by
CentOS" and service_count:2 and services.port:22 and services.port:80 and
autonomous_system.asn="60117"
```



services.http.response.html_title="Apache HTTP Server Test Page powered by CentOS" and service_count:2 and services.port:22 and services.port:80 and autonomous_system.asn="60117"

Hosts
Results: 12 Time: 0.37s

185.183.96.10 (185-183-96-10.hostsailor.com)
Linux HS (60117) North Holland, Netherlands
remote-access bootstrap
2 Matched Services
22/SSH 80/HTTP

185.45.192.24 (185-45-192-24.hostsailor.com)
Linux HS (60117) South Holland, Netherlands
remote-access bootstrap
2 Matched Services
80/HTTP 22/SSH

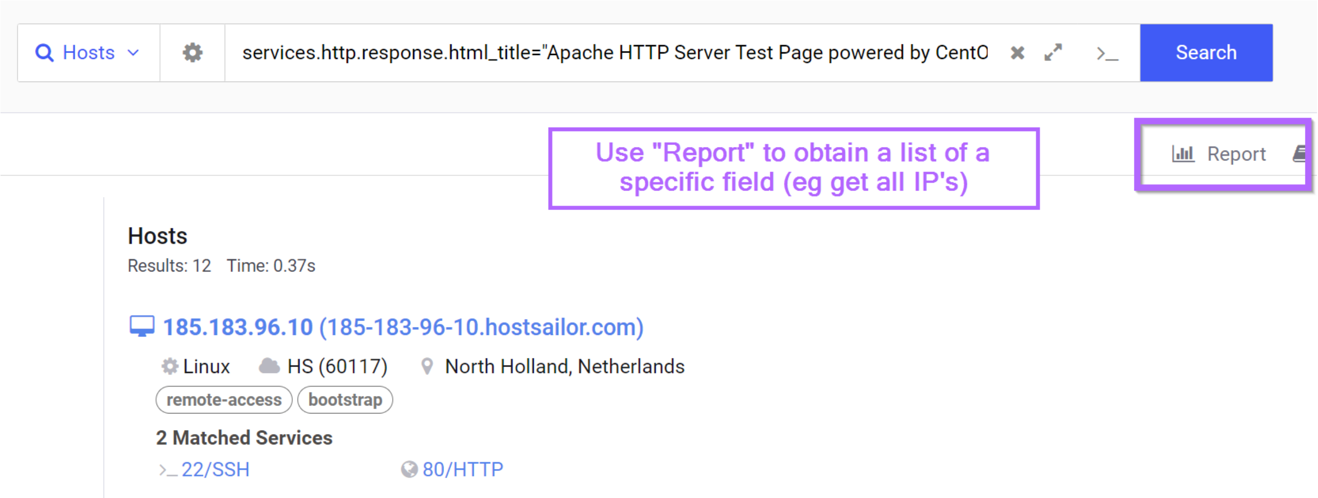
Investigating Results

Now at this point, all of the servers look the same (simple and default services), so it's difficult to determine if they are malicious using only Censys.

So we can go ahead and export a list and compare it to a reputation service like VirusTotal.

> There are likely much better services out there than Virustotal, but VT is the standard and the most accessible so it's what we will use here

We can start by exporting an easy list of results from our search. This can be done with the "report" feature of Censys.



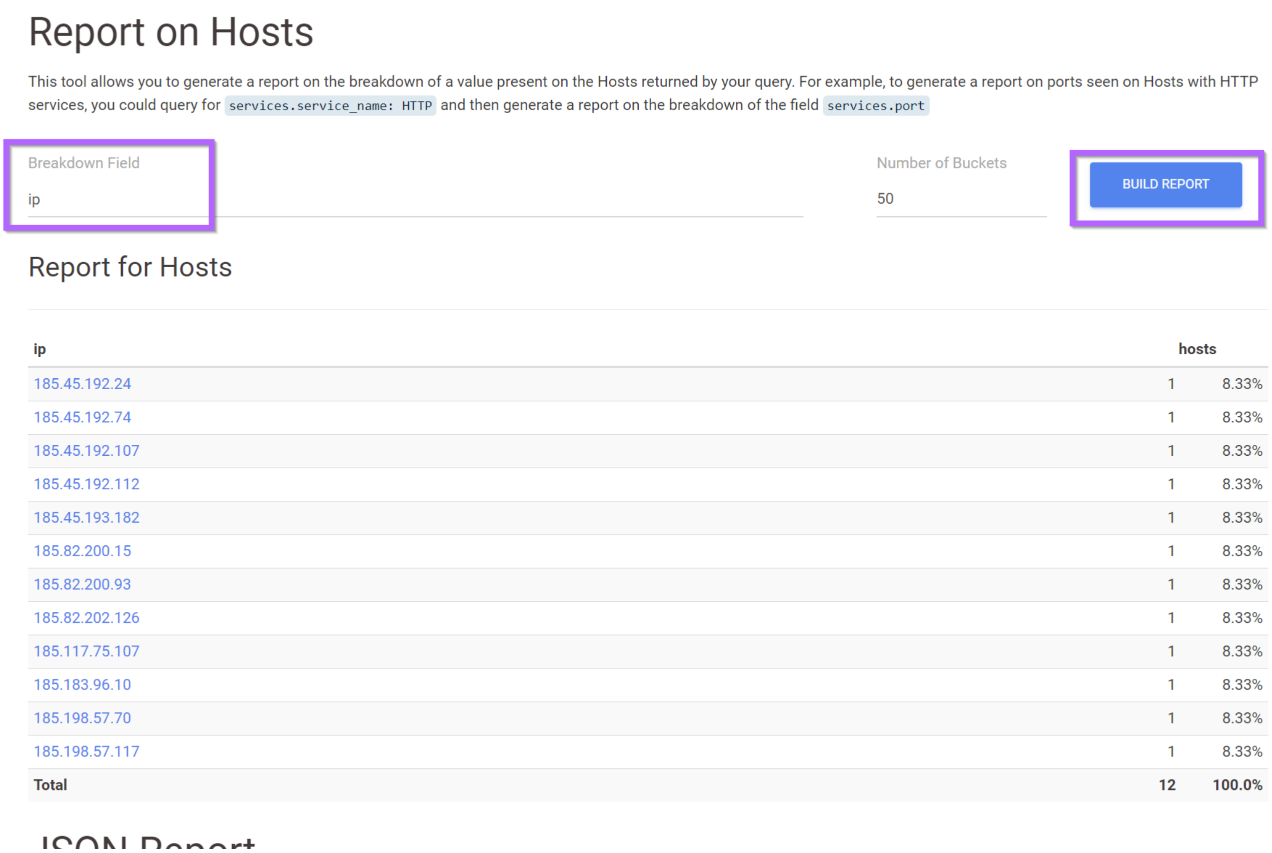
services.http.response.html_title="Apache HTTP Server Test Page powered by CentO

Use "Report" to obtain a list of a specific field (eg get all IP's)

Hosts
Results: 12 Time: 0.37s

185.183.96.10 (185-183-96-10.hostsailor.com)
Linux HS (60117) North Holland, Netherlands
remote-access bootstrap
2 Matched Services
22/SSH 80/HTTP

From the report function, we can specify the `ip` field and go ahead and build a report. (We can leave the "Number of Buckets" at 50, since our search returned less than 50 results)



Report on Hosts

This tool allows you to generate a report on the breakdown of a value present on the Hosts returned by your query. For example, to generate a report on ports seen on Hosts with HTTP services, you could query for `services.service_name: HTTP` and then generate a report on the breakdown of the field `services.port`

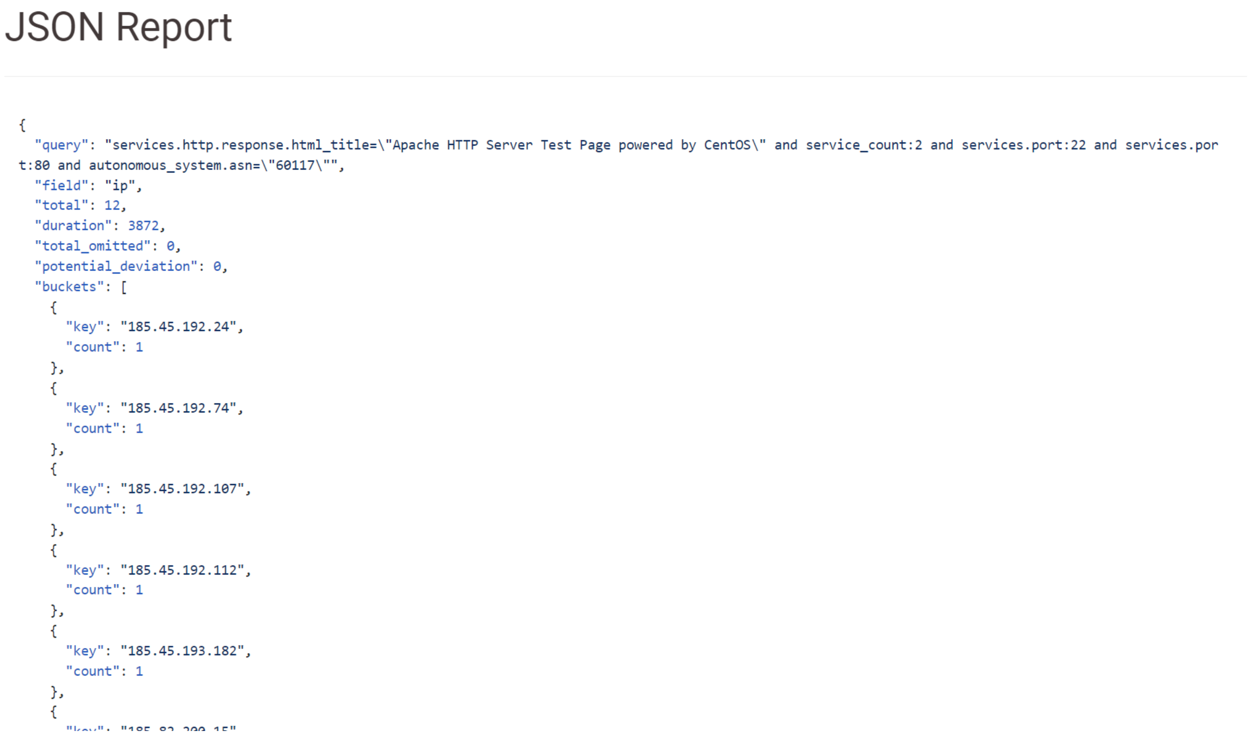
Breakdown Field: ip

Number of Buckets: 50

Report for Hosts

ip	hosts	
185.45.192.24	1	8.33%
185.45.192.74	1	8.33%
185.45.192.107	1	8.33%
185.45.192.112	1	8.33%
185.45.193.182	1	8.33%
185.82.200.15	1	8.33%
185.82.200.93	1	8.33%
185.82.202.126	1	8.33%
185.117.75.107	1	8.33%
185.183.96.10	1	8.33%
185.198.57.70	1	8.33%
185.198.57.117	1	8.33%
Total	**12**	**100.0%**

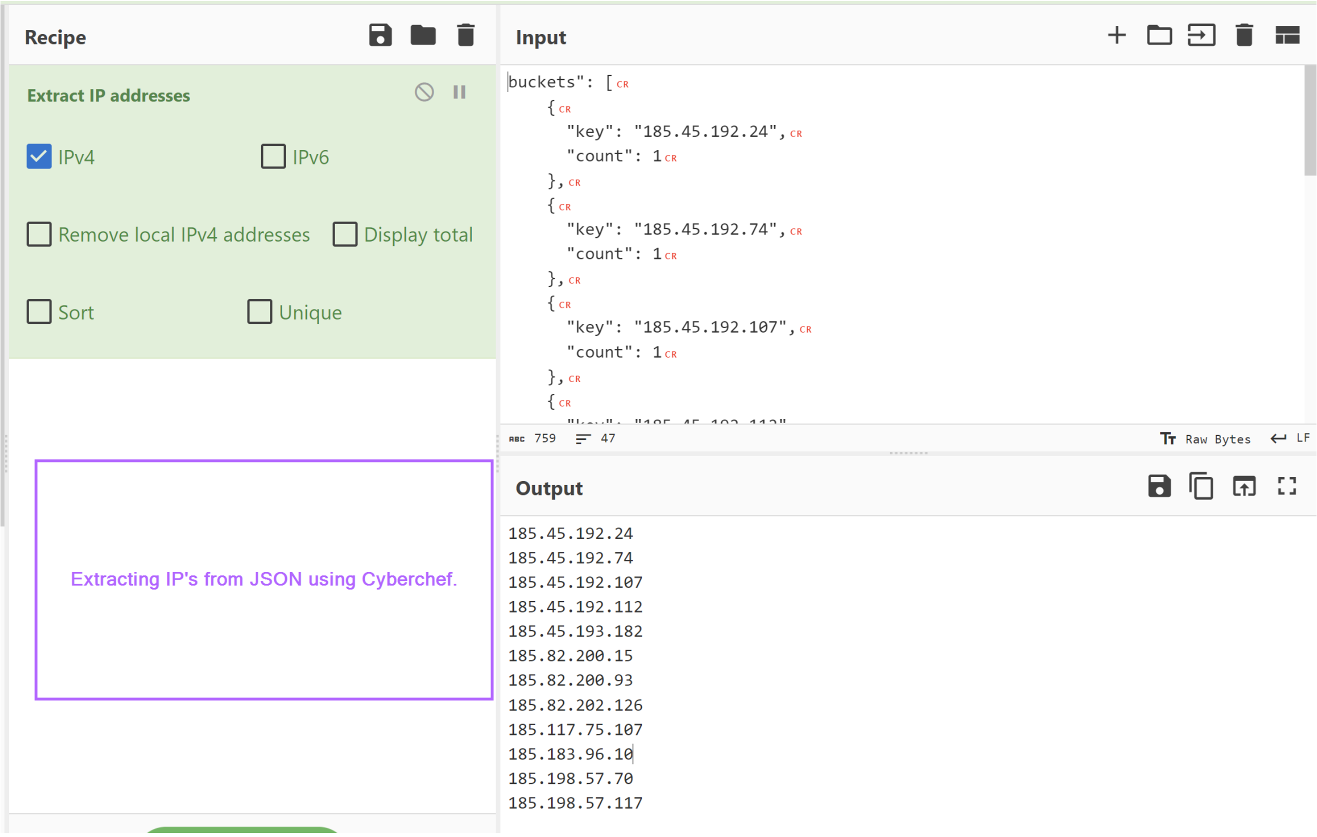
By scrolling down we can obtain the list in JSON format.



JSON Report

```
{
  "query": "services.http.response.html_title=\"Apache HTTP Server Test Page powered by CentOS\" and service_count:2 and services.port:22 and services.por
t:80 and autonomous_system.asn=\"60117\"",
  "field": "ip",
  "total": 12,
  "duration": 3872,
  "total_omitted": 0,
  "potential_deviation": 0,
  "buckets": [
    {
      "key": "185.45.192.24",
      "count": 1
    },
    {
      "key": "185.45.192.74",
      "count": 1
    },
    {
      "key": "185.45.192.107",
      "count": 1
    },
    {
      "key": "185.45.192.112",
      "count": 1
    },
    {
      "key": "185.45.193.182",
      "count": 1
    },
    {
      "key": "185.82.200.15"
```

From here we can use CyberChef and `Extract IP Addresses` to get an easy list without needing to deal with JSON.



Extract IP addresses

☑ IPv4 □ IPv6

□ Remove local IPv4 addresses □ Display total

□ Sort □ Unique

Extracting IP's from JSON using Cyberchef.

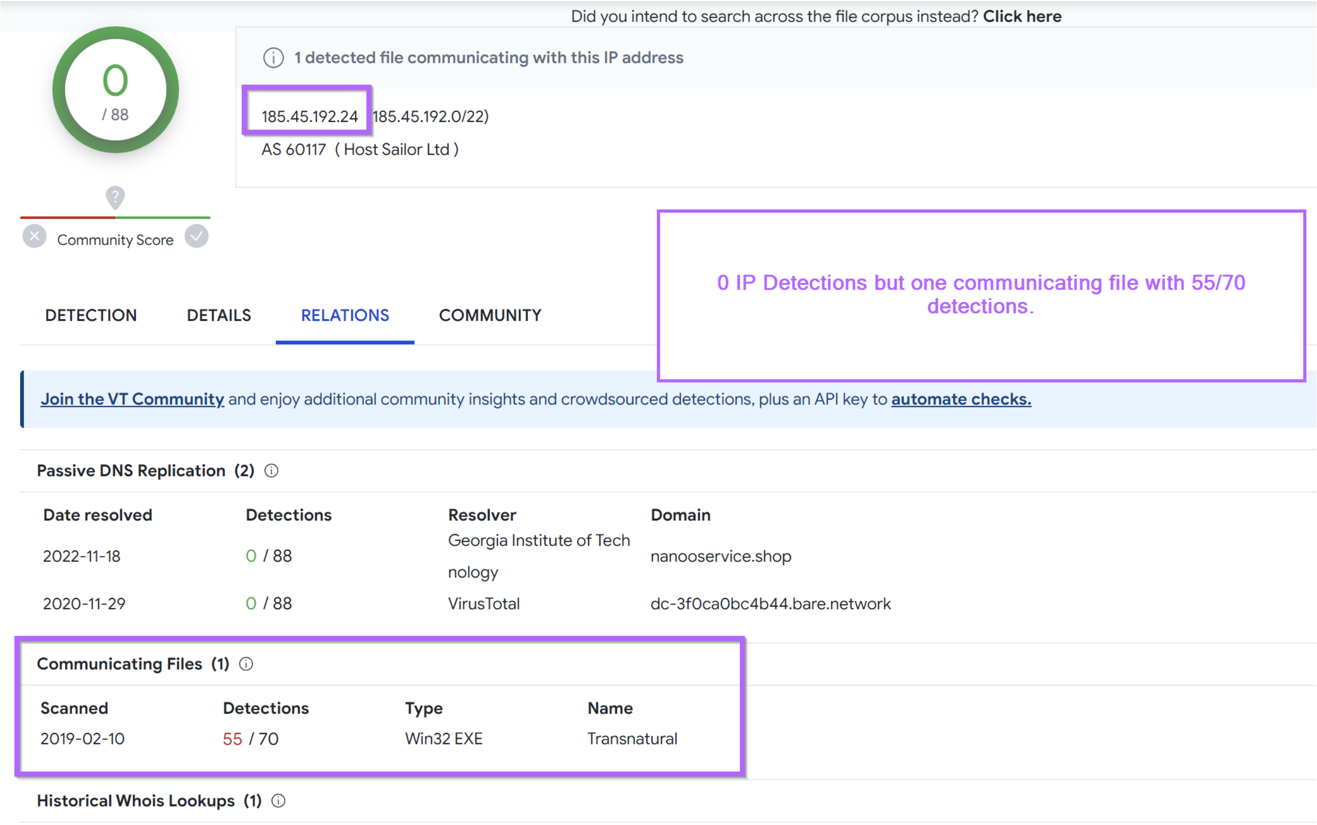
```
buckets": [
    {
      "key": "185.45.192.24",
      "count": 1
    },
    {
      "key": "185.45.192.74",
      "count": 1
    },
    {
      "key": "185.45.192.107",
      "count": 1
    },
    {
```

```
185.45.192.24
185.45.192.74
185.45.192.107
185.45.192.112
185.45.193.182
185.82.200.15
185.82.200.93
185.82.202.126
185.117.75.107
185.183.96.10
185.198.57.70
185.198.57.117
```

Checking Results in Virustotal

Looking at the first result `185.45.192[.]24`, we can see 0 detections in Virustotal. But there is one communicating file with 55/70 detections.

Given the scan date of `2019-02-10`, it's possible that the IP was previously malicious and that is no longer the case. But either way the IP is related to something shady.



Did you intend to search across the file corpus instead? **Click here**

1 detected file communicating with this IP address

185.45.192.24 185.45.192.0/22)
AS 60117 (Host Sailor Ltd)

0 IP Detections but one communicating file with 55/70 detections.

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to **automate checks.**

Passive DNS Replication (2)

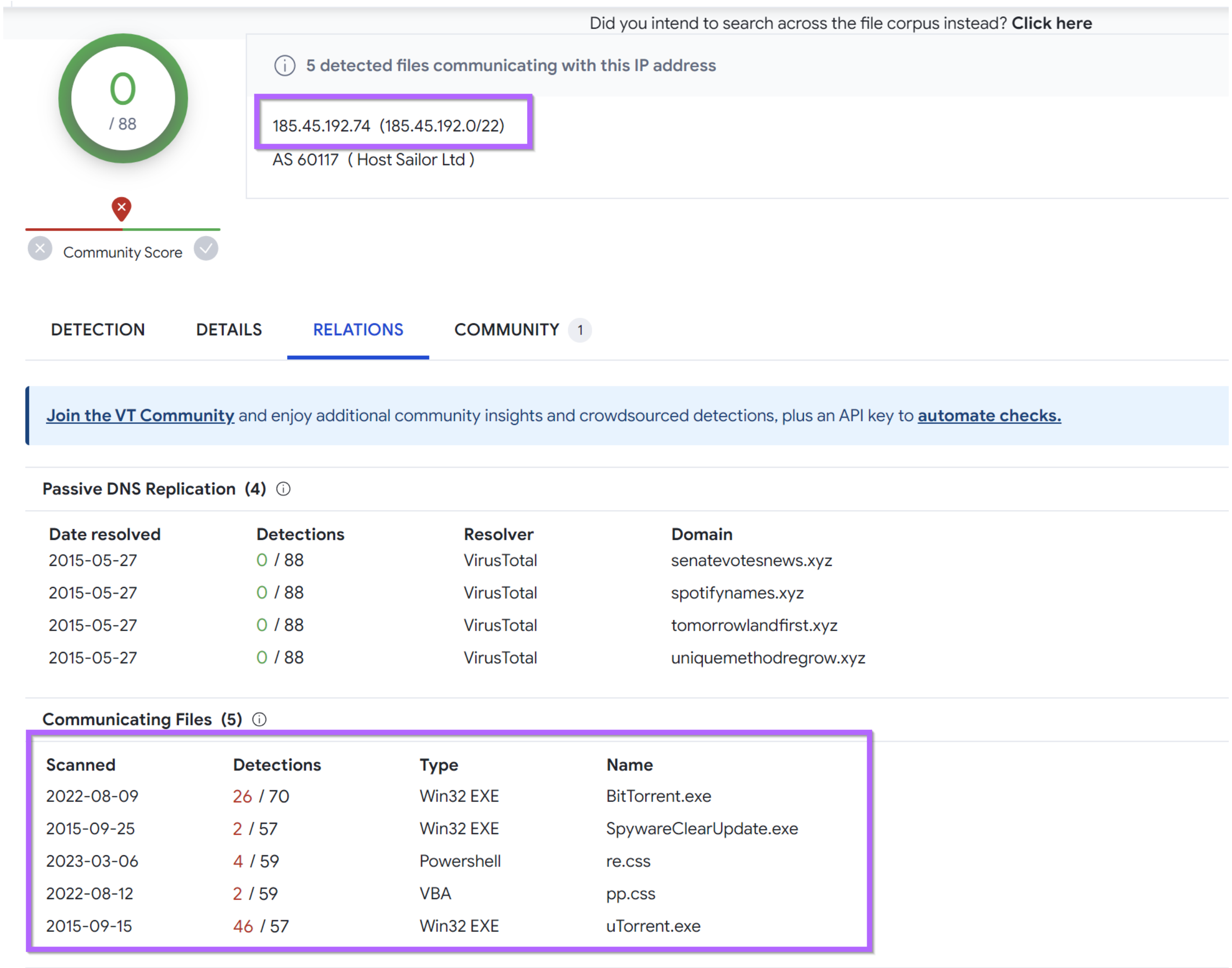
Date resolved	Detections	Resolver	Domain
2022-11-18	0 / 88	Georgia Institute of Technology	nanooservice.shop
2020-11-29	0 / 88	VirusTotal	dc-3f0ca0bc4b44.bare.network

Communicating Files (1)

Scanned	Detections	Type	Name
2019-02-10	55 / 70	Win32 EXE	Transnatural

Historical Whois Lookups (1)

Checking on the second result of `185.45.192[.]74`, we can also observe 0 IP detections, but 5 malicious communicating files.


Did you intend to search across the file corpus instead? **Click here**
0
/ 88
Community Score
DETECTION
DETAILS
RELATIONS
COMMUNITY 1

5 detected files communicating with this IP address

185.45.192.74 (185.45.192.0/22)

AS 60117 (Host Sailor Ltd)

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to **automate checks.**

Passive DNS Replication (4)

Date resolved	Detections	Resolver	Domain
2015-05-27	0 / 88	VirusTotal	senatevotesnews.xyz
2015-05-27	0 / 88	VirusTotal	spotifynames.xyz
2015-05-27	0 / 88	VirusTotal	tomorrowlandfirst.xyz
2015-05-27	0 / 88	VirusTotal	uniquemethodregrow.xyz

Communicating Files (5)

Scanned	Detections	Type	Name
2022-08-09	26 / 70	Win32 EXE	BitTorrent.exe
2015-09-25	2 / 57	Win32 EXE	SpywareClearUpdate.exe
2023-03-06	4 / 59	Powershell	re.css
2022-08-12	2 / 59	VBA	pp.css
2015-09-15	46 / 57	Win32 EXE	uTorrent.exe

Moving on, we can continue the same process and use it to determine more information.

Now there isn't enough information to strongly correlate the servers back to PrivateLoader, but given the very similar setups and small number of results. We can assume they are suspicious.

> In cases like these, typically the servers are related and used by the same group, but not yet actively used for malicious activities. Some servers are often reserved for later use or the usage is (so far) so minimal that it hasn't yet showed up on VT and other "Free" services.

It's also entirely possible that some of these are benign, but I think the likelihood is low. All results should be considered suspicious and blocked where possible.

```
185.45.192[.]24 - 0/88 Detections, 1 communicating with with 55 detections.
185.45.192[.]74 - 0/88 VT, 5 malicious communicating files.
185.45.192[.]107 -  0/88 VT, no related files.
185.45.192[.]112 -  0/88 VT, no related files.
185.45.193[.]182 - 0/88 VT, no related files.
185.82.200[.]15 -  0/88 VT, no related files.
185.82.200[.]93 -  0/88 VT, no related files.
185.82.202[.]126 - 5/88 VT, Observed SSH Brute Forcing
185.117.75[.]107 - 0/88 VT, no related files.
185.183.96[.]10 - 4/88 VT, Hosting Malware, Previously Trickbot
185.198.57[.]70 - 12/88 VT, Previously Hosting Malware
185.198.57[.]117 -  9/88 VT, Initial PrivateLoader IP
```