Combining Pivot Points to Identify Malware Infrastructure - Redline, Smokeloader and Cobalt Strike

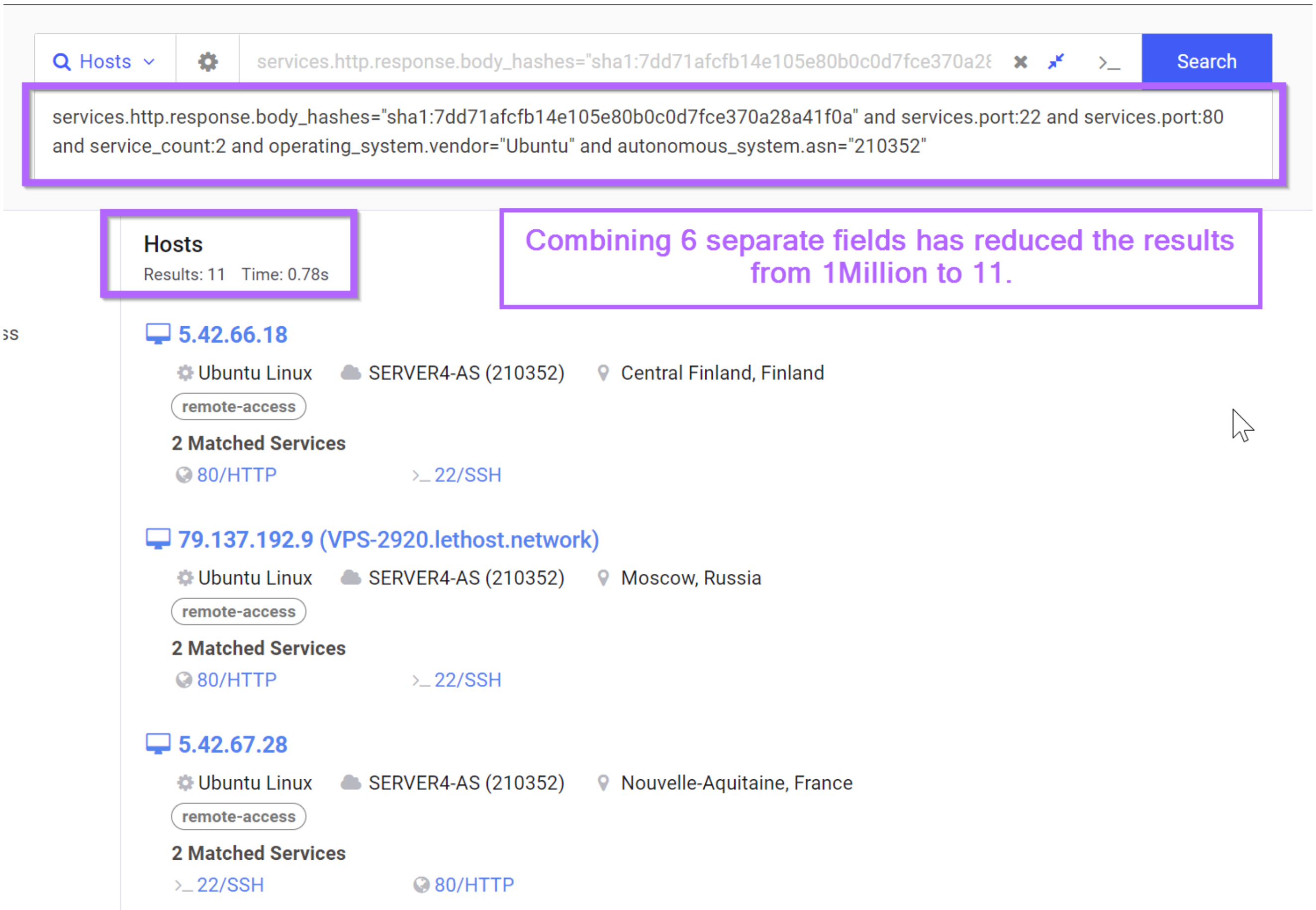
embee-research.ghost.io/combining-pivot-points-to-identify-malware-infrastructure-redline-smokeloader-and-cobalt-strike/

Matthew

November 19, 2023

Beginner

Identifying Malware infrastructure by combining weak pivot points.



services.http.response.body_hashes="sha1:7dd71afcfb14e105e80b0c0d7fce370a28

services.http.response.body_hashes="sha1:7dd71afcfb14e105e80b0c0d7fce370a28a41f0a" and services.port:22 and services.port:80 and service_count:2 and operating_system.vendor="Ubuntu" and autonomous_system.asn="210352"

Hosts
Results: 11 Time: 0.78s

Combining 6 separate fields has reduced the results from 1Million to 11.

5.42.66.18
Ubuntu Linux SERVER4-AS (210352) Central Finland, Finland
remote-access
2 Matched Services
80/HTTP 22/SSH

79.137.192.9 (VPS-2920.lethost.network)
Ubuntu Linux SERVER4-AS (210352) Moscow, Russia
remote-access
2 Matched Services
80/HTTP 22/SSH

5.42.67.28
Ubuntu Linux SERVER4-AS (210352) Nouvelle-Aquitaine, France
remote-access
2 Matched Services
22/SSH 80/HTTP

In this post, we'll demonstrate how to use Censys to pivot when there are minimal unique indicators that could be used for a single strong pivot.

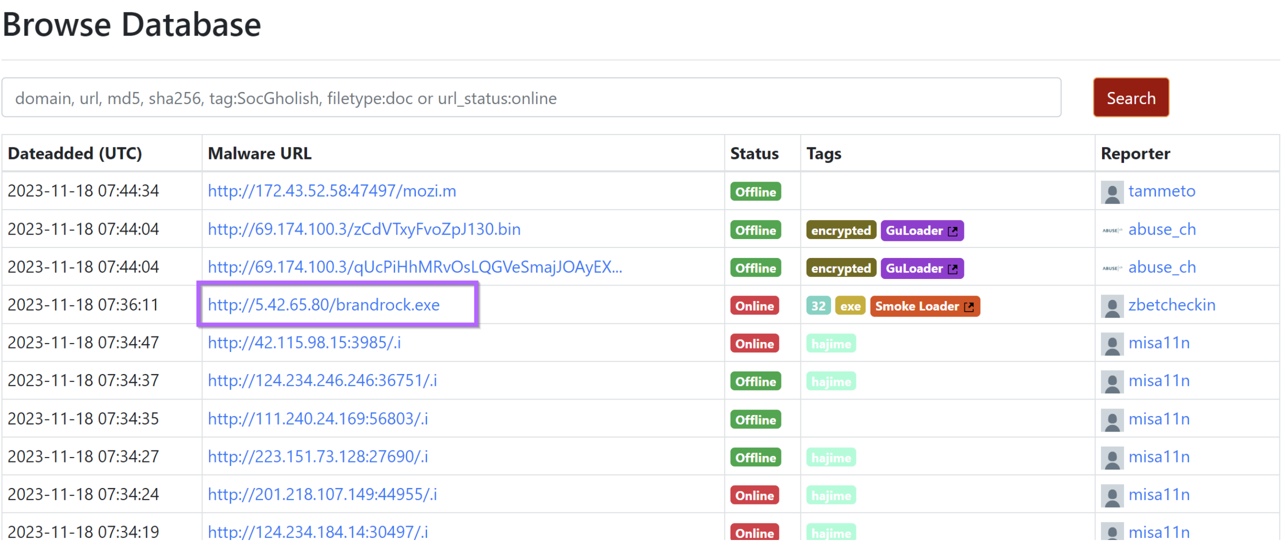
We'll combine 5 separate "weak" indicators to identify 11 malware servers from a single initial IP found on URLHaus.

The final query we will be building can be found here.

```
services.http.response.body_hashes="sha1:7dd71afcfb14e105e80b0c0d7fce370a28a41
f0a" and services.port:22 and services.port:80 and service_count:2 and
operating_system.vendor="Ubuntu" and autonomous_system.asn="210352"
```

Analysis

I'll be starting with the ip `5.42.65[.]80` . This IP was present on URLHaus and marked as Smoke Loader.



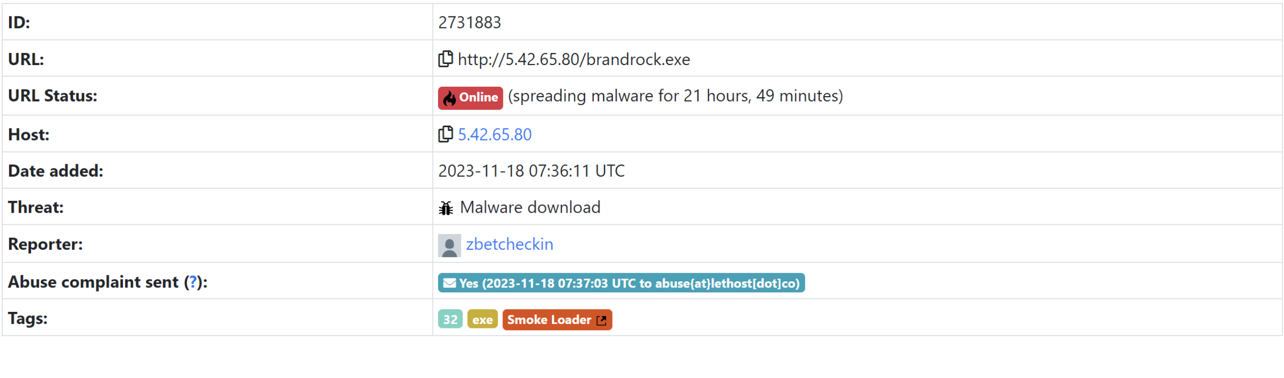
Browse Database

domain, url, md5, sha256, tag:SocGholish, filetype:doc or url_status:online

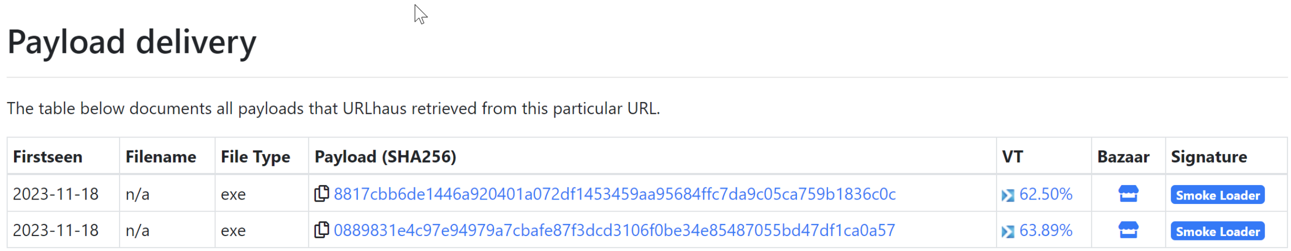
Search

Dateadded (UTC)	Malware URL	Status	Tags	Reporter
2023-11-18 07:44:34	http://172.43.52.58:47497/mozi.m	Offline		tammeto
2023-11-18 07:44:04	http://69.174.100.3/zCdVTxyFvoZpJ130.bin	Offline	encrypted GuLoader	abuse_ch
2023-11-18 07:44:04	http://69.174.100.3/qUcPiHhMRvOsLQGVeSmajJOAyEX...	Offline	encrypted GuLoader	abuse_ch
2023-11-18 07:36:11	http://5.42.65.80/brandrock.exe	Online	32 exe Smoke Loader	zbetcheckin
2023-11-18 07:34:47	http://42.115.98.15:3985/.i	Online	hajime	misa11n
2023-11-18 07:34:37	http://124.234.246.246:36751/.i	Offline	hajime	misa11n
2023-11-18 07:34:35	http://111.240.24.169:56803/.i	Offline		misa11n
2023-11-18 07:34:27	http://223.151.73.128:27690/.i	Offline	hajime	misa11n
2023-11-18 07:34:24	http://201.218.107.149:44955/.i	Online	hajime	misa11n
2023-11-18 07:34:19	http://124.234.184.14:30497/.i	Online	hajime	misa11n

Viewing additional information, we can see that the IP has been used to host Smoke Loader samples.



ID:	2731883
URL:	http://5.42.65.80/brandrock.exe
URL Status:	Online (spreading malware for 21 hours, 49 minutes)
Host:	5.42.65.80
Date added:	2023-11-18 07:36:11 UTC
Threat:	Malware download
Reporter:	zbetcheckin
Abuse complaint sent (?):	Yes (2023-11-18 07:37:03 UTC to abuse(at)lethost[dot]co)
Tags:	32 exe Smoke Loader



Payload delivery

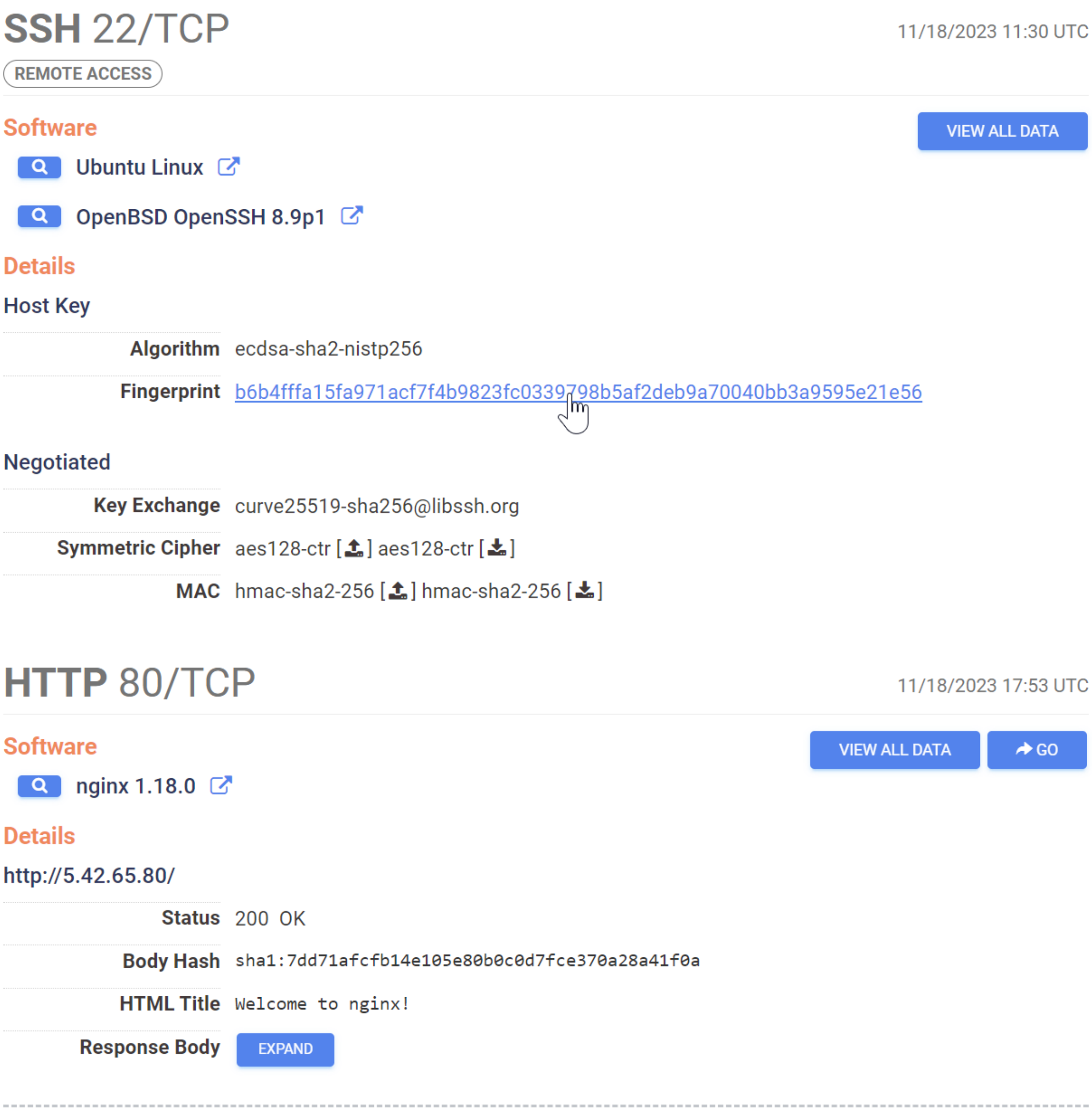
The table below documents all payloads that URLhaus retrieved from this particular URL.

Firstseen	Filename	File Type	Payload (SHA256)	VT	Bazaar	Signature
2023-11-18	n/a	exe	8817cbb6de1446a920401a072df1453459aa95684ffc7da9c05ca759b1836c0c	62.50%		Smoke Loader
2023-11-18	n/a	exe	0889831e4c97e94979a7cbafe87f3dcd3106f0be34e85487055bd47df1ca0a57	63.89%		Smoke Loader

Censys Analysis

Moving over to Censys, we can search on the IP address and attempt to determine a pivot point.

Within Censys, we can see that there are two running services. SSH on port 22 and HTTP on port 80.



SSH 22/TCP 11/18/2023 11:30 UTC

Software

Ubuntu Linux

OpenBSD OpenSSH 8.9p1

Details

Host Key

Algorithm	ecdsa-sha2-nistp256
Fingerprint	b6b4fffa15fa971acf7f4b9823fc0339798b5af2deb9a70040bb3a9595e21e56

Negotiated

Key Exchange	curve25519-sha256@libssh.org
Symmetric Cipher	aes128-ctr [⭱] aes128-ctr [⭳]
MAC	hmac-sha2-256 [⭱] hmac-sha2-256 [⭳]

HTTP 80/TCP 11/18/2023 17:53 UTC

Software

nginx 1.18.0

Details

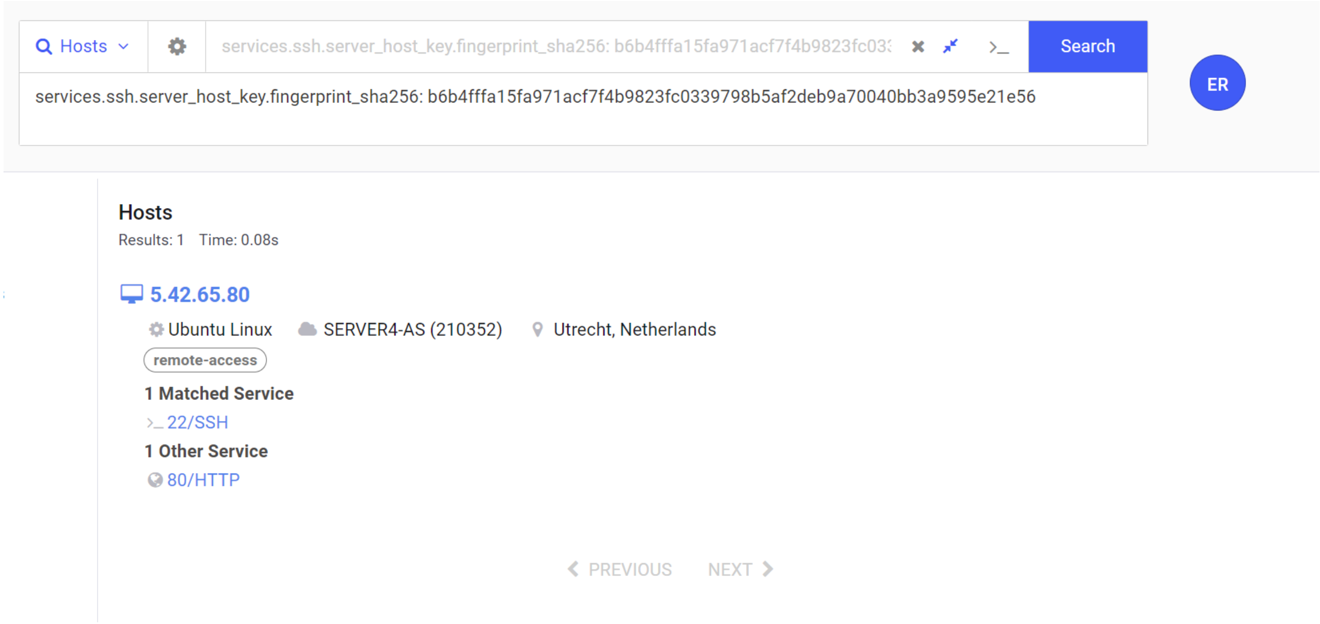
http://5.42.65.80/

Status	200 OK
Body Hash	sha1:7dd71afcfb14e105e80b0c0d7fce370a28a41f0a
HTML Title	Welcome to nginx!
Response Body	EXPAND

Pivoting on the SSH Service.

When SSH is in use it can be possible to pivot on the SSH host key, this works if the threat actor has used the same SSH setup across related infrastructure.

In this case this did not work, the SSH Host key was not re-used across any other hosts in the Censys database.



services.ssh.server_host_key.fingerprint_sha256: b6b4fffa15fa971acf7f4b9823fc0339798b5af2deb9a70040bb3a9595e21e56

Hosts

Results: 1 Time: 0.08s

5.42.65.80

Ubuntu Linux SERVER4-AS (210352) Utrecht, Netherlands

remote-access

1 Matched Service

>_ 22/SSH

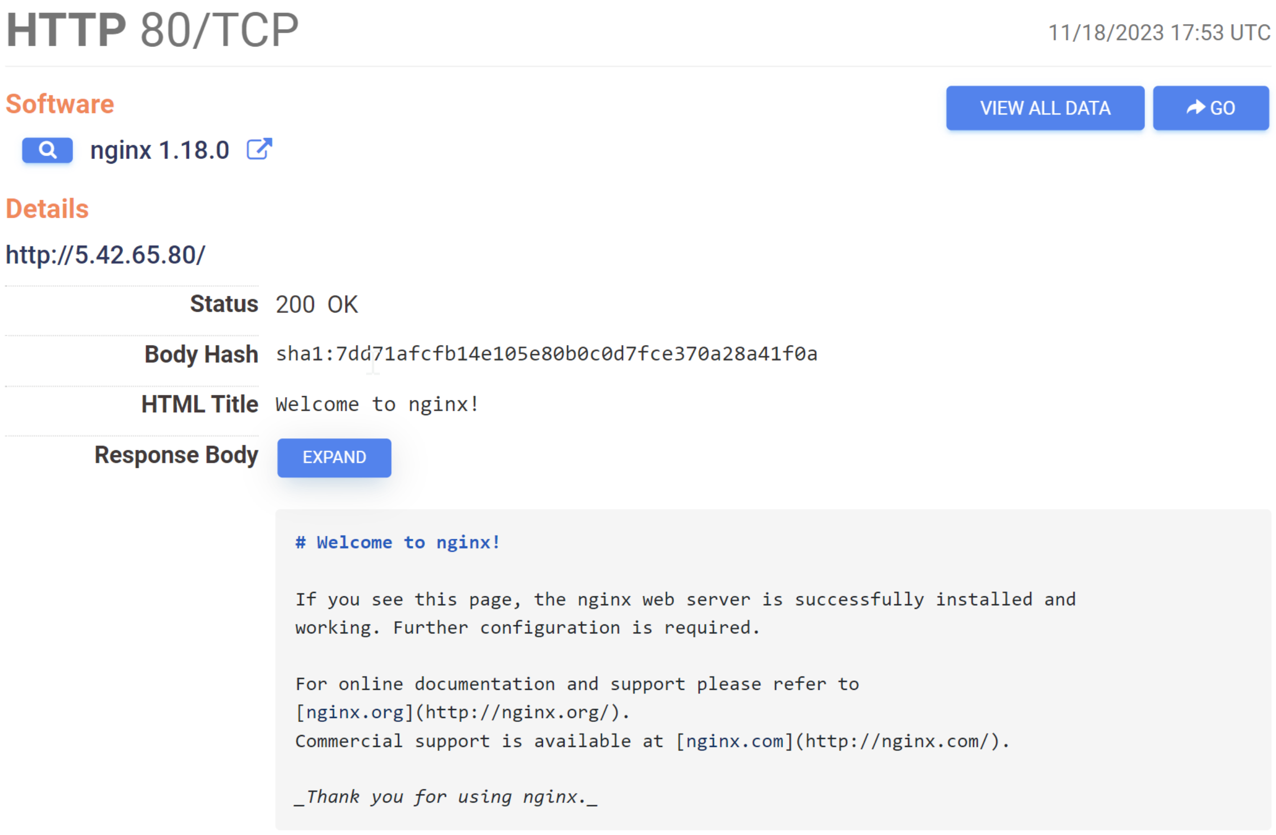
1 Other Service

80/HTTP

Pivoting on the HTTP Service

Inspecting the HTTP service on port 80, there isn't a lot of information that we can pivot from.

At first glance, everything seems to be a default install of the Nginx load balancer.



HTTP 80/TCP 11/18/2023 17:53 UTC

Software

nginx 1.18.0

Details

http://5.42.65.80/

Status	200 OK
Body Hash	sha1:7dd71afcfb14e105e80b0c0d7fce370a28a41f0a
HTML Title	Welcome to nginx!
Response Body	

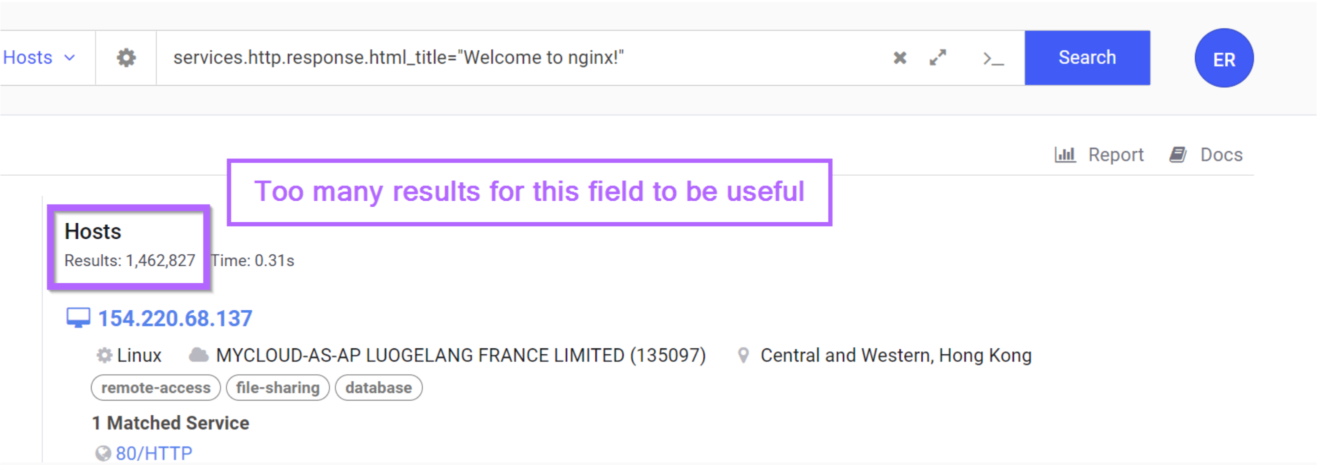
```
# Welcome to nginx!

If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.

For online documentation and support please refer to
[nginx.org](http://nginx.org/).
Commercial support is available at [nginx.com](http://nginx.com/).

_Thank you for using nginx._
```

Attempts to pivot on the html title or banner hash will result in either millions of results, or a single result (the same server). So these are not useful as pivot points.

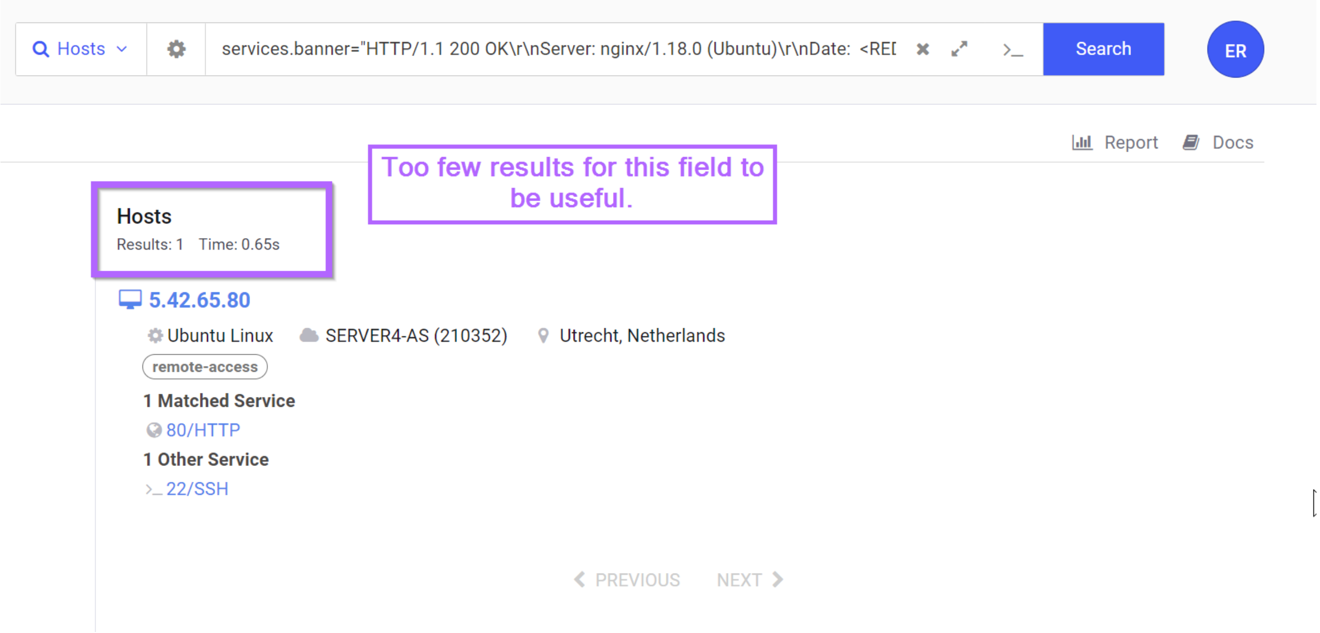


services.http.response.html_title="Welcome to nginx!"

Too many results for this field to be useful

Hosts
Results: 1,462,827 Time: 0.31s

154.220.68.137
Linux MYCLOUD-AS-AP LUOGELANG FRANCE LIMITED (135097) Central and Western, Hong Kong
remote-access file-sharing database
1 Matched Service
80/HTTP



services.banner="HTTP/1.1 200 OK\r\nServer: nginx/1.18.0 (Ubuntu)\r\nDate: <REI

Too few results for this field to be useful.

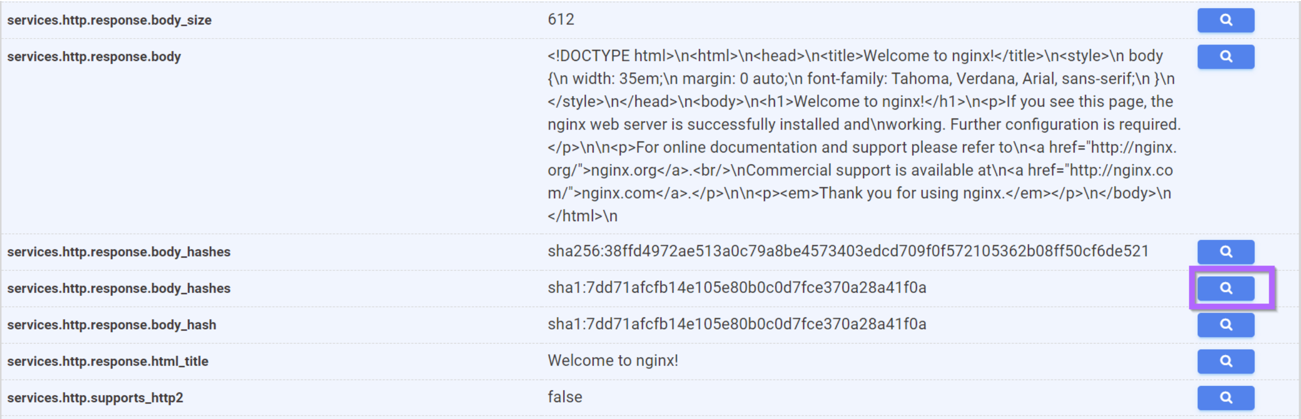
Hosts
Results: 1 Time: 0.65s

5.42.65.80
Ubuntu Linux SERVER4-AS (210352) Utrecht, Netherlands
remote-access
1 Matched Service
80/HTTP
1 Other Service
22/SSH

Pivoting On The Body Hash

The response body from one of the previous screenshots shows a default but relatively long string of text.

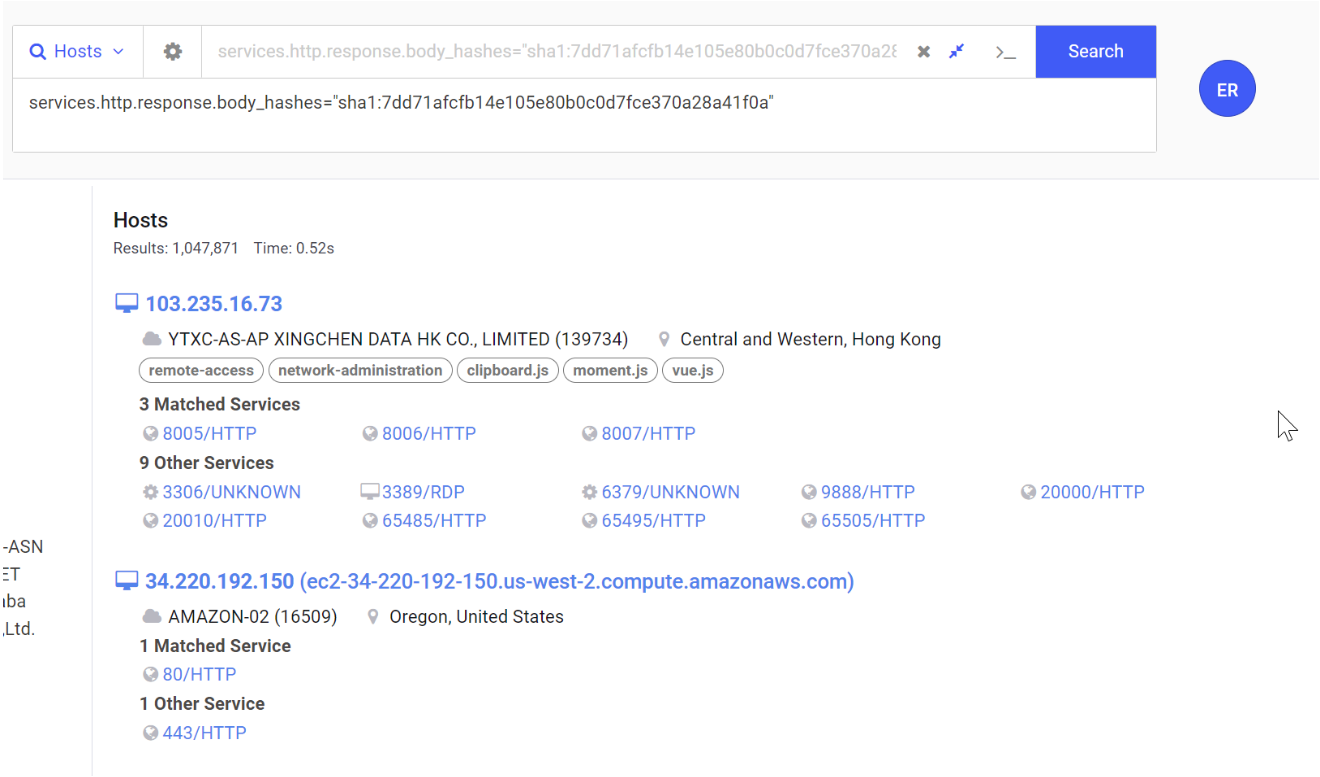
In hopes that this text is unique enough to be used as a pivot point, we can use the search button in Censys to attempt a pivot on the hash of this text. (This will search for any server that returns identical text to this one)



services.http.response.body_size	612
services.http.response.body	<!DOCTYPE html>\n<html>\n<head>\n<title>Welcome to nginx!</title>\n<style>\n body {\n width: 35em;\n margin: 0 auto;\n font-family: Tahoma, Verdana, Arial, sans-serif;\n }\n </style>\n</head>\n<body>\n<h1>Welcome to nginx!</h1>\n<p>If you see this page, the nginx web server is successfully installed and\nworking. Further configuration is required.</p>\n\n<p>For online documentation and support please refer to\n<a href="http://nginx.org/">nginx.org</a>.<br/>\nCommercial support is available at\n<a href="http://nginx.com/">nginx.com</a>.</p>\n\n<p><em>Thank you for using nginx.</em></p>\n</body>\n</html>\n
services.http.response.body_hashes	sha256:38ffd4972ae513a0c79a8be4573403edcd709f0f572105362b08ff50cf6de521
services.http.response.body_hashes	sha1:7dd71afcfb14e105e80b0c0d7fce370a28a41f0a
services.http.response.body_hash	sha1:7dd71afcfb14e105e80b0c0d7fce370a28a41f0a
services.http.response.html_title	Welcome to nginx!
services.http.supports_http2	false

Pivoting on the hash of the response body returns over a million results. So this value is also not useful as a pivot point.

At least not on its own.



services.http.response.body_hashes="sha1:7dd71afcfb14e105e80b0c0d7fce370a28a41f0a"

Hosts

Results: 1,047,871 Time: 0.52s

103.235.16.73

YTXC-AS-AP XINGCHEN DATA HK CO., LIMITED (139734) Central and Western, Hong Kong

remote-access network-administration clipboard.js moment.js vue.js

3 Matched Services

8005/HTTP 8006/HTTP 8007/HTTP

9 Other Services

3306/UNKNOWN 3389/RDP 6379/UNKNOWN 9888/HTTP 20000/HTTP
20010/HTTP 65485/HTTP 65495/HTTP 65505/HTTP

34.220.192.150 (ec2-34-220-192-150.us-west-2.compute.amazonaws.com)

AMAZON-02 (16509) Oregon, United States

1 Matched Service

80/HTTP

1 Other Service

443/HTTP

Combining Pivot Points

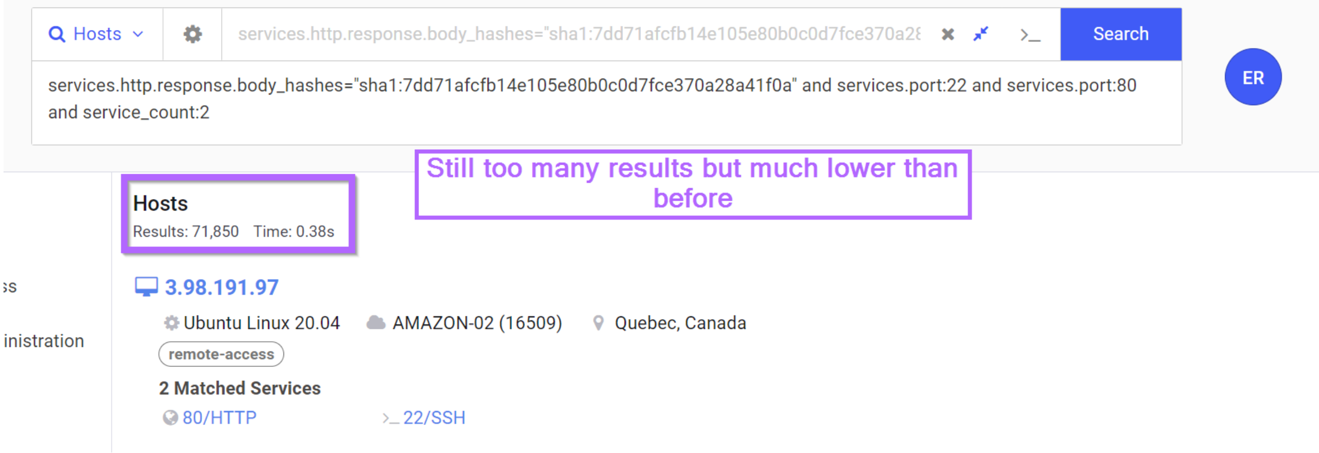
Since we weren't able to identify any useful pivot points within the HTTP or SSH services, we can instead try a different approach by limiting the location and the number of services running.

For example, we can combine our body hash search with a requirement that the server is ONLY running SSH/22 and HTTP/80.

The below query will limit our search to servers running only port 22 and 80.

```
services.http.response.body_hashes="sha1:7dd71afcfb14e105e80b0c0d7fce370a28a41f0a" and services.port:22 and services.port:80 and service_count:2
```

This reduces our results from ~1Mil down to ~71k.



services.http.response.body_hashes="sha1:7dd71afcfb14e105e80b0c0d7fce370a28a41f0a" and services.port:22 and services.port:80 and service_count:2

Still too many results but much lower than before

Hosts
Results: 71,850 Time: 0.38s

3.98.191.97
Ubuntu Linux 20.04 AMAZON-02 (16509) Quebec, Canada
remote-access
2 Matched Services
80/HTTP 22/SSH

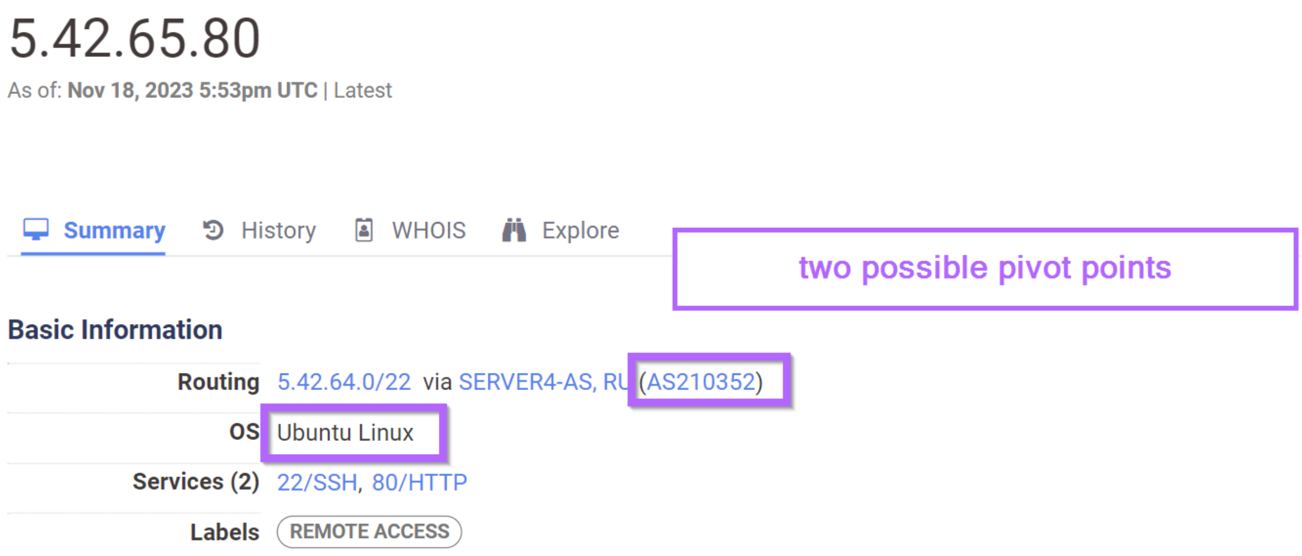
This is still too many results, but much lower than before so we may be on to something.

Looking for Additional Pivot Points

Since we've already limited our results fairly significantly (considering the lack of unique services running). We can go looking for other options for pivoting.

If we return the summary view of our initial host, we can see that it's running Ubuntu Linux and is operating on ASN 210352.

> ASN is short for "Autonomous System Number" and is used to group IP addresses with the same routing policy. This generally means that it groups IP addresses in similar locations (same datacentre) or at least roughly the same geographical area.
>
> ASN's are often useful as pivot points when other options fail.



5.42.65.80

As of: **Nov 18, 2023 5:53pm UTC** | Latest

two possible pivot points

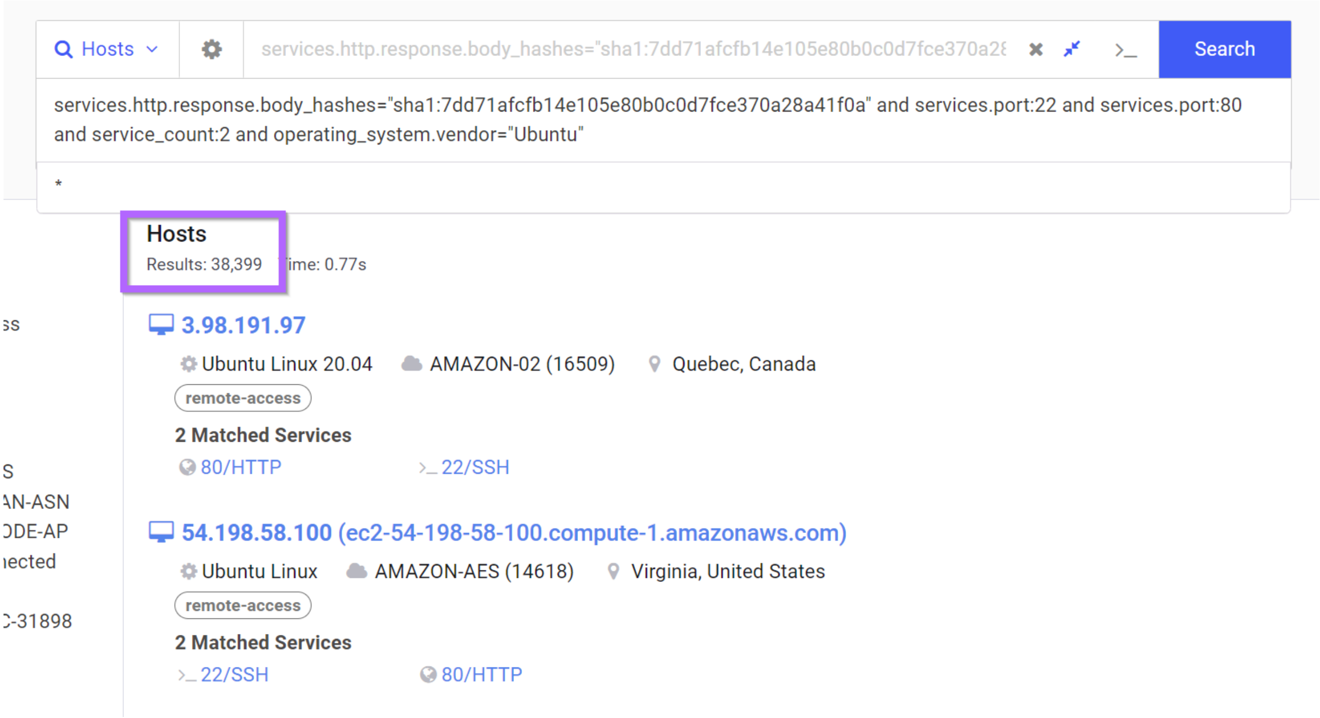
Basic Information

Routing	5.42.64.0/22 via SERVER4-AS, RU (AS210352)
OS	Ubuntu Linux
Services (2)	22/SSH, 80/HTTP
Labels	REMOTE ACCESS

Filtering on Ubuntu Operating System

If we return to our previous search and a filter on Ubuntu, we can reduce our results down to ~38K.

This is still too many but heading in the right direction.



```
services.http.response.body_hashes="sha1:7dd71afcfb14e105e80b0c0d7fce370a28a41f0a" and services.port:22 and services.port:80
and service_count:2 and operating_system.vendor="Ubuntu"
```

Hosts

Results: 38,399 Time: 0.77s

3.98.191.97

Ubuntu Linux 20.04 AMAZON-02 (16509) Quebec, Canada

remote-access

2 Matched Services

80/HTTP 22/SSH

54.198.58.100 (ec2-54-198-58-100.compute-1.amazonaws.com)

Ubuntu Linux AMAZON-AES (14618) Virginia, United States

remote-access

2 Matched Services

22/SSH 80/HTTP

Filtering on Autonomous System Number (ASN)

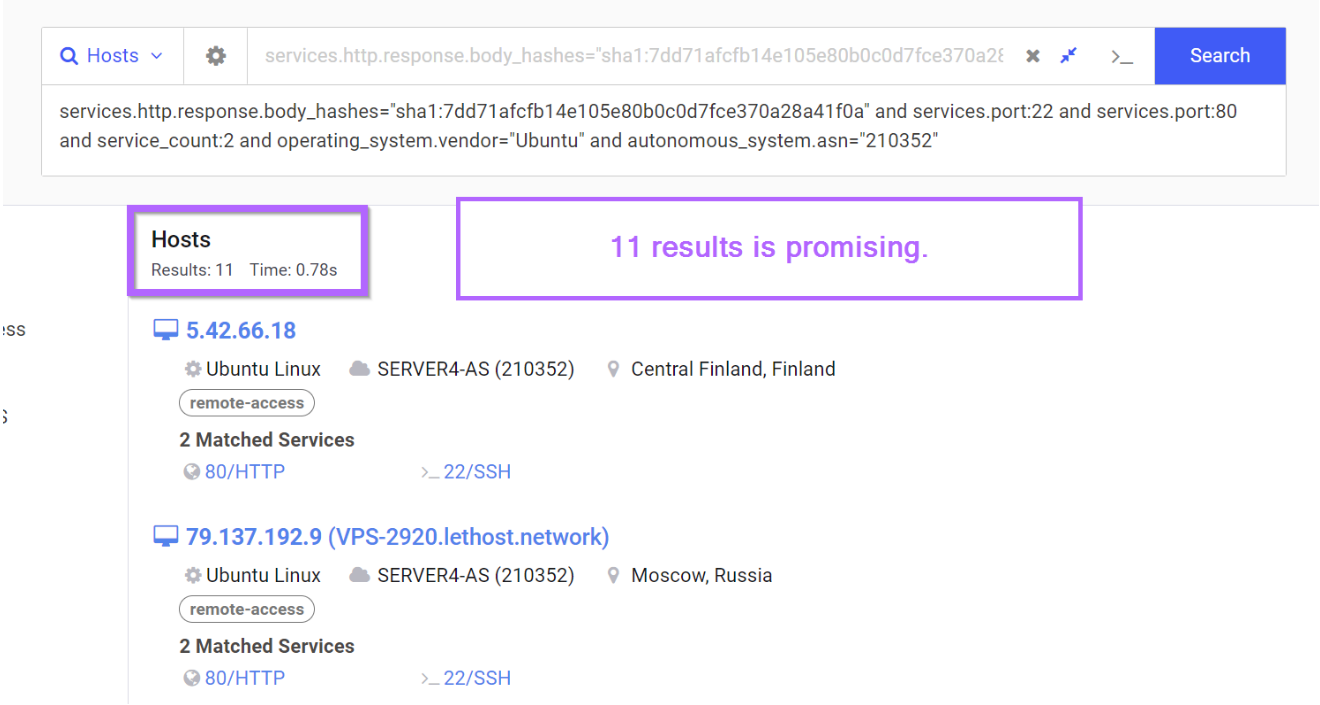
Since we still had too many results (38K) after filtering on Ubuntu. We can go ahead and filter on the ASN number `210352` present in our initial IP.

This means that our current search looks like this. Which accounts for...

- Body Hash of nginx page
- ONLY services 22 and 80
- Running Ubuntu Operating System
- Grouped by ASN Number `210352`

```
services.http.response.body_hashes="sha1:7dd71afcfb14e105e80b0c0d7fce370a28a41
f0a" and services.port:22 and services.port:80 and service_count:2 and
operating_system.vendor="Ubuntu" and autonomous_system.asn="210352"
```

Now we're down to 11 results, which looks very promising.



```
services.http.response.body_hashes="sha1:7dd71afcfb14e105e80b0c0d7fce370a28a41f0a" and services.port:22 and services.port:80
and service_count:2 and operating_system.vendor="Ubuntu" and autonomous_system.asn="210352"
```

Hosts
Results: 11 Time: 0.78s

11 results is promising.

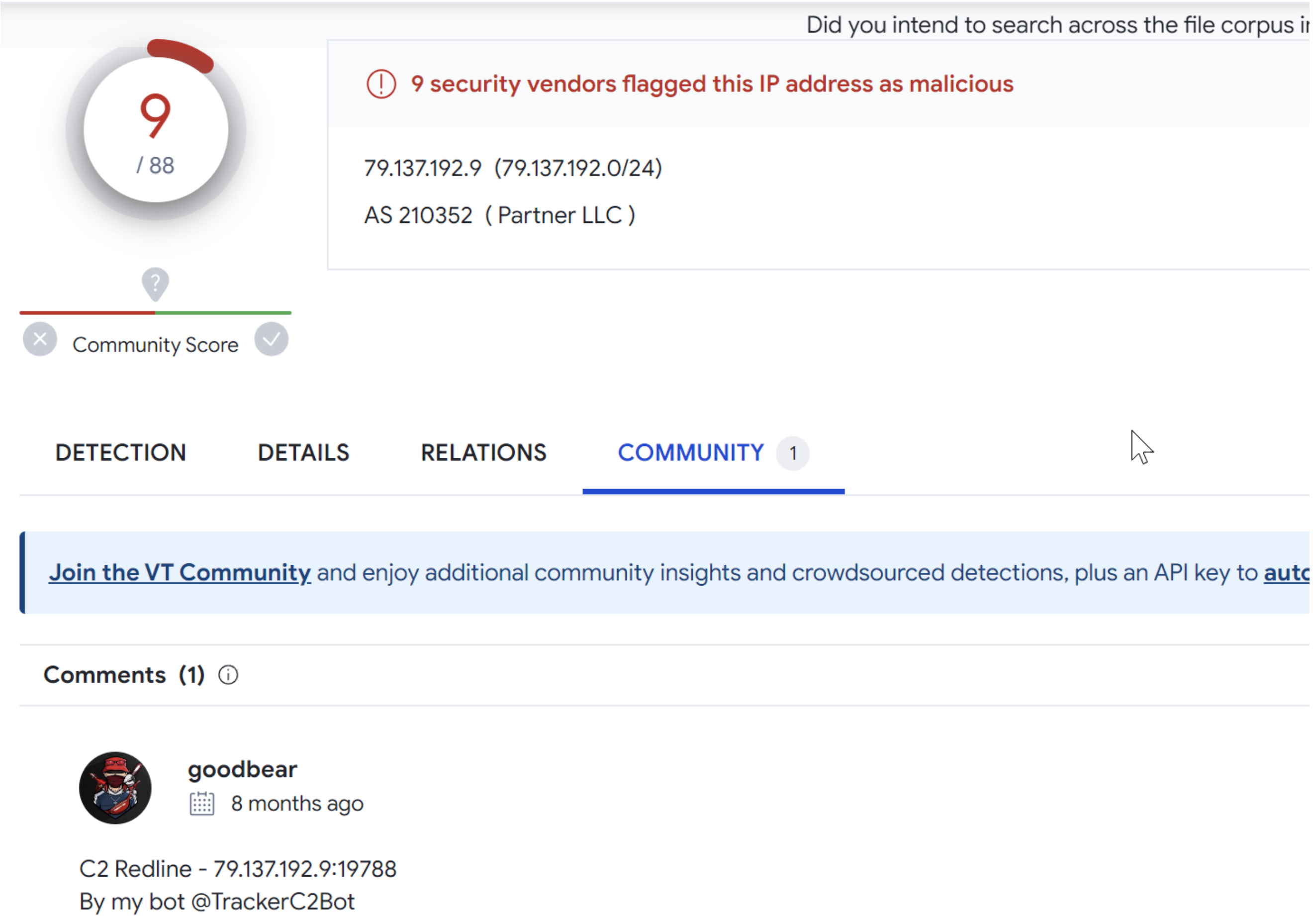
5.42.66.18
Ubuntu Linux SERVER4-AS (210352) Central Finland, Finland
remote-access
2 Matched Services
80/HTTP 22/SSH

79.137.192.9 (VPS-2920.lethost.network)
Ubuntu Linux SERVER4-AS (210352) Moscow, Russia
remote-access
2 Matched Services
80/HTTP 22/SSH

Investigating Results

With only 11 results remaining, we probably don't need to do any additional filtering. We can instead go ahead and confirm our current results.

The second result `79.137.192[.]9` has 9/88 hits on Virustotal and may be related to Redline Stealer.


Did you intend to search across the file corpus i

9 security vendors flagged this IP address as malicious

79.137.192.9 (79.137.192.0/24)

AS 210352 (Partner LLC)

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to auto

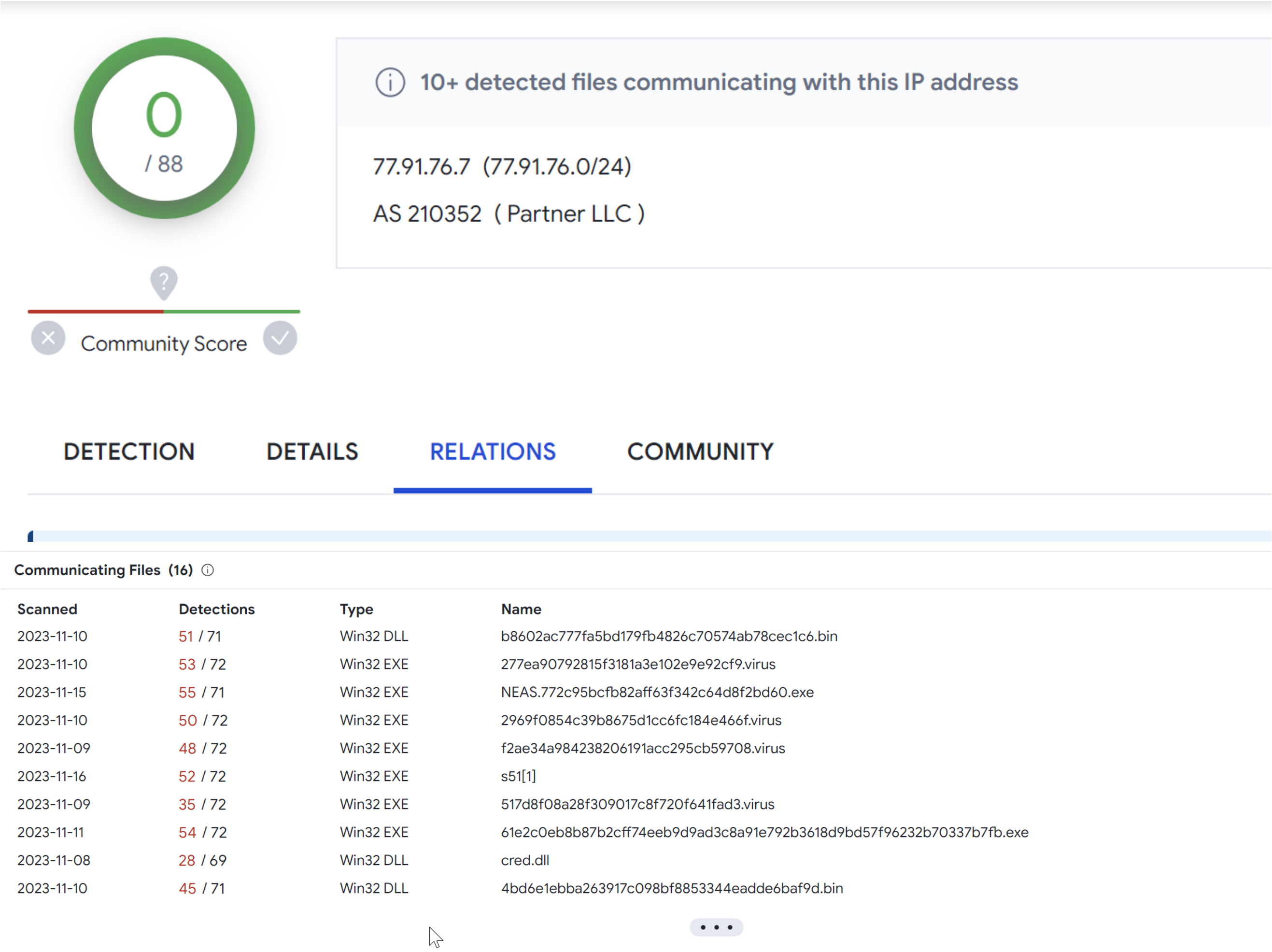
Comments (1)

goodbear
8 months ago

C2 Redline - 79.137.192.9:19788
By my bot @TrackerC2Bot

Investigating 77.91.76[.]7

The 4th result in the search has 0/88 detections on Virustotal. But has 11 recent communicating files that are very likely to be malicious.



10+ detected files communicating with this IP address

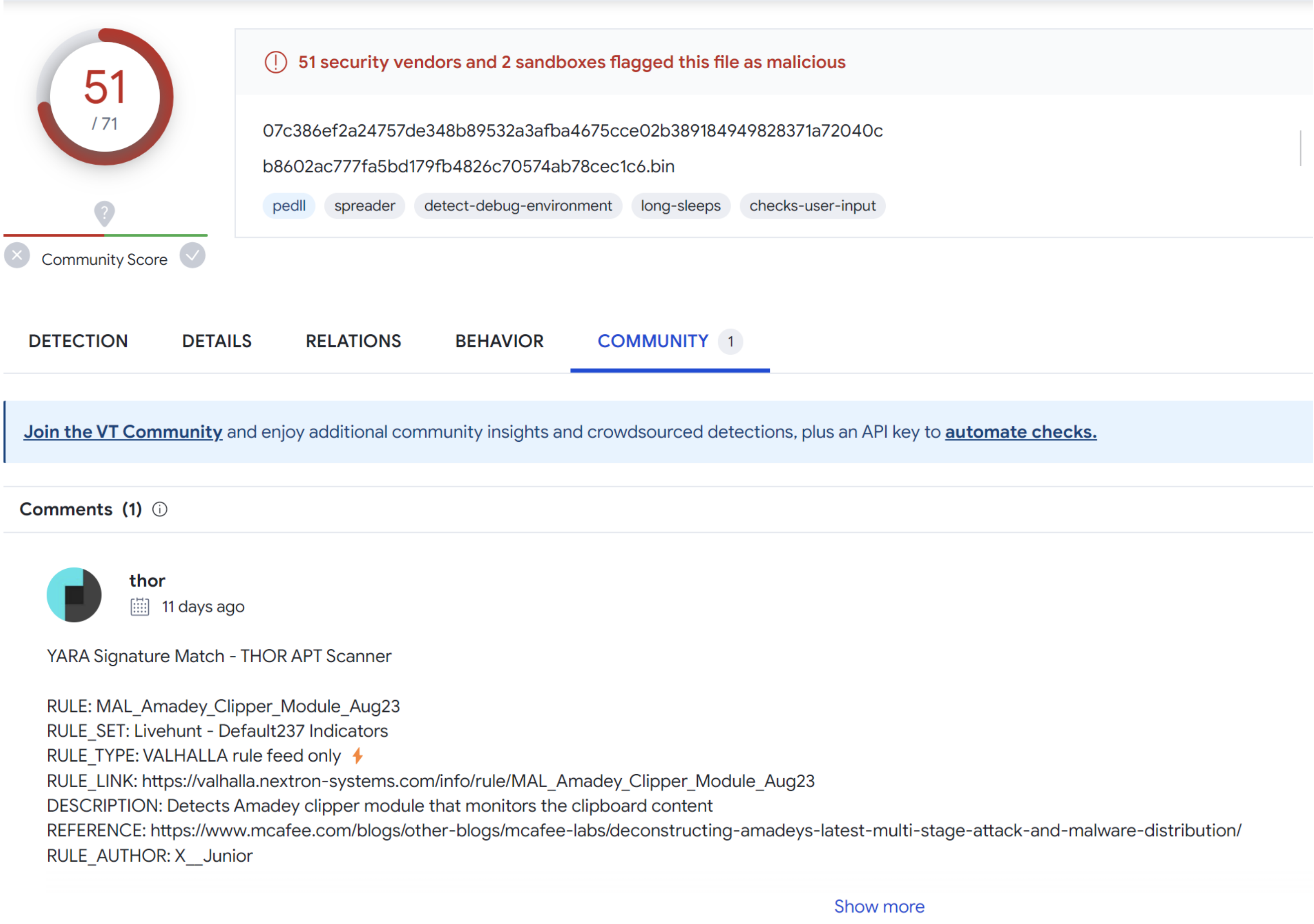
77.91.76.7 (77.91.76.0/24)

AS 210352 (Partner LLC)

Communicating Files (16)

Scanned	Detections	Type	Name
2023-11-10	51 / 71	Win32 DLL	b8602ac777fa5bd179fb4826c70574ab78cec1c6.bin
2023-11-10	53 / 72	Win32 EXE	277ea90792815f3181a3e102e9e92cf9.virus
2023-11-15	55 / 71	Win32 EXE	NEAS.772c95bcfb82aff63f342c64d8f2bd60.exe
2023-11-10	50 / 72	Win32 EXE	2969f0854c39b8675d1cc6fc184e466f.virus
2023-11-09	48 / 72	Win32 EXE	f2ae34a984238206191acc295cb59708.virus
2023-11-16	52 / 72	Win32 EXE	s51[1]
2023-11-09	35 / 72	Win32 EXE	517d8f08a28f309017c8f720f641fad3.virus
2023-11-11	54 / 72	Win32 EXE	61e2c0eb8b87b2cff74eeb9d9ad3c8a91e792b3618d9bd57f96232b70337b7fb.exe
2023-11-08	28 / 69	Win32 DLL	cred.dll
2023-11-10	45 / 71	Win32 DLL	4bd6e1ebba263917c098bf8853344eadde6baf9d.bin

The first communicating file has been marked as Amadey Clipper Module by the Thor scanner by Florian Roth.



51 / 71

Community Score

51 security vendors and 2 sandboxes flagged this file as malicious

07c386ef2a24757de348b89532a3afba4675cce02b389184949828371a72040c

b8602ac777fa5bd179fb4826c70574ab78cec1c6.bin

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

Comments (1)

thor

11 days ago

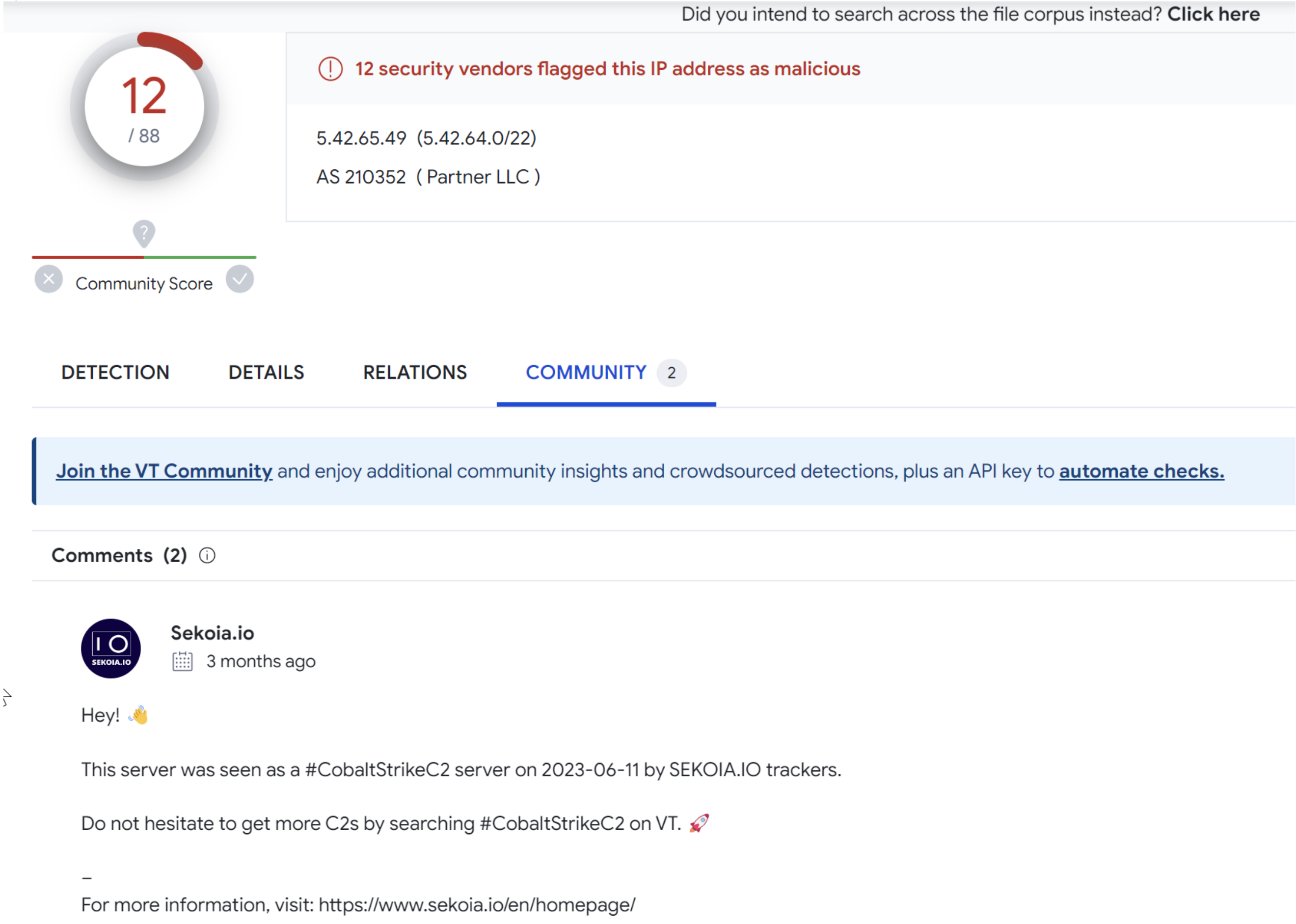
YARA Signature Match - THOR APT Scanner

RULE: MAL_Amadey_Clipper_Module_Aug23
RULE_SET: Livehunt - Default237 Indicators
RULE_TYPE: VALHALLA rule feed only
RULE_LINK: https://valhalla.nextron-systems.com/info/rule/MAL_Amadey_Clipper_Module_Aug23
DESCRIPTION: Detects Amadey clipper module that monitors the clipboard content
REFERENCE: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/deconstructing-amadeys-latest-multi-stage-attack-and-malware-distribution/
RULE_AUTHOR: X__Junior

Investigating 5.42.65[.]49

A VirusTotal search on the returned result `5.42.65[.]49` returns 12/88 results.

There are also two comments indicating that the server has been used as a Cobalt Strike C2.



12 security vendors flagged this IP address as malicious

5.42.65.49 (5.42.64.0/22)

AS 210352 (Partner LLC)

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

Sekoia.io

3 months ago

Hey! 👋

This server was seen as a #CobaltStrikeC2 server on 2023-06-11 by SEKOIA.IO trackers.

Do not hesitate to get more C2s by searching #CobaltStrikeC2 on VT. 🚀

–

For more information, visit: https://www.sekoia.io/en/homepage/

Confirming Results

So far 3 of the returned results are malware C2's related to Redline, Amadey and Cobalt Strike.

We won't go into the analysis of every one of the results, but a summary will be included below of the findings.

Some of the results had 0 detections and no indications of malware. In these cases, I would still assume that the IP is related and malicious (possibly reserved for later use).

Final Results

The final results can be observed below, based on the prevalence of malware C2's, I would assume that the 3 "clean" results are malicious but not yet in active use.

```
5.42.65[.]49 - 12/88 VT, Cobalt Strike C2
5.42.65[.]64 - 0/88 VT, Clean
5.42.65[.]80 - 19/88 VT, Smokeloader Delivery
5.42.66[.]9 - 4/88 VT, Amadey Bot C2
5.42.66[.]18 - 0/88 VT, Clean
5.42.67[.]28 - 0/88 VT, Clean
77.91.76[.]7 - 0/88 VT, Amadey C2
77.91.76[.]12 - 1/88 VT, Unsure
79.137.192[.]6 - 17/88 VT, Redline Stealer
79.137.192[.]9 - 9/88 VT, Redline Stealer
79.137.192[.]18 - 19/88 VT, Redline Stealer
```

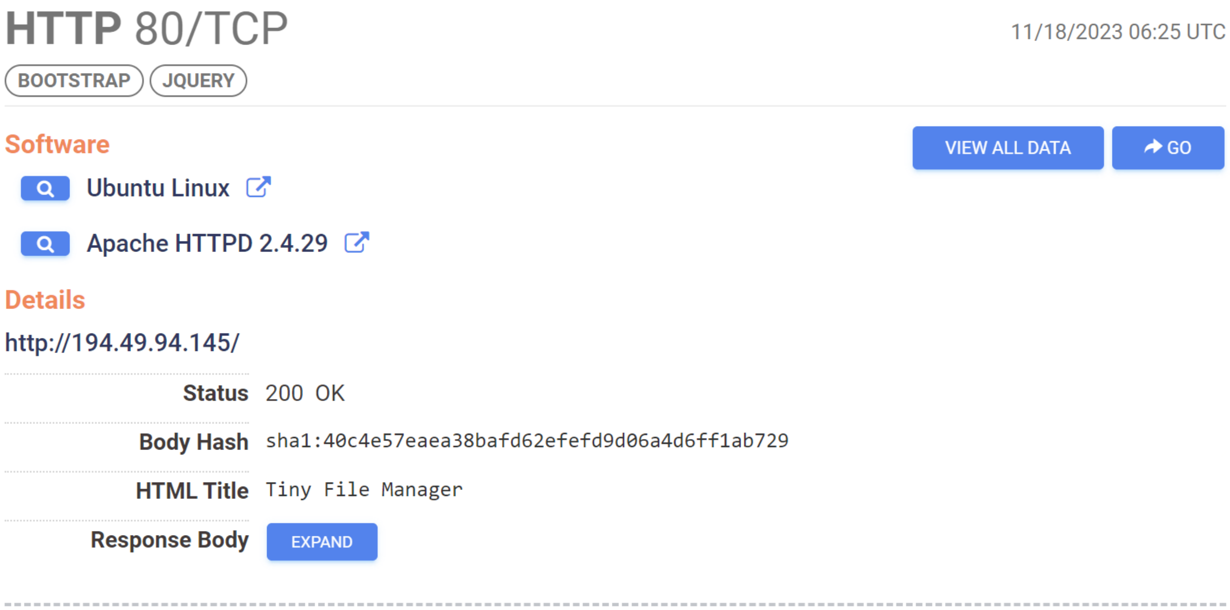
Additional Notes - Lumma Stealer

The concept covered in this post can also be applied to a Lumma C2 from URLHaus.

By combining the use of "Tiny File Manager" on port 80 with the limited port numbers and ASN, we can identify another 6 malicious servers.

Below is an example of what this looks like.

```
services.http.response.html_title="Tiny File Manager" and service_count:2 and
services.port:22 and services.port:80 and autonomous_system.asn="216419"
```



HTTP 80/TCP

11/18/2023 06:25 UTC

Software

Ubuntu Linux

Apache HTTPD 2.4.29

Details

http://194.49.94.145/

Status: 200 OK

Body Hash: sha1:40c4e57eaea38bafd62efefd9d06a4d6ff1ab729

HTML Title: Tiny File Manager

Response Body

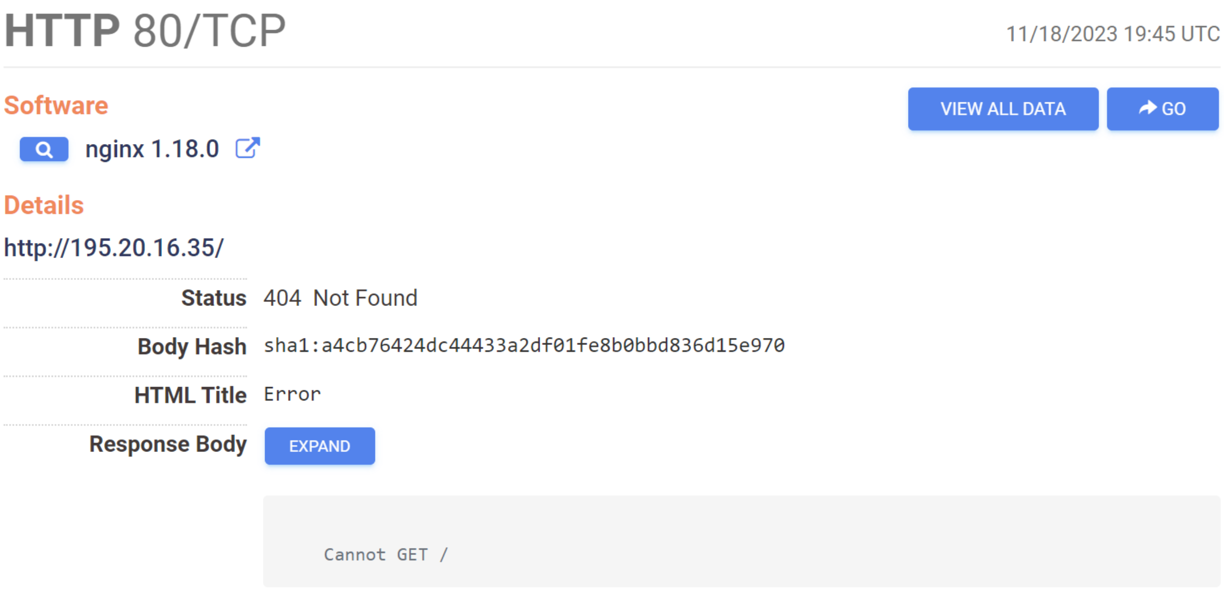
Additional Notes - RecordBreaker

The same concept can also be applied to this server from URLHaus.

You can see the Censys search here.

```
services.http.response.html_title="Error" and
services.software.product="nginx" and service_count:2 and services.port:22 and
services.port:80 and autonomous_system.asn="211409"
```

This is based on a limited number of ports, ASN and an error message in the returned page on port 80.



HTTP 80/TCP

11/18/2023 19:45 UTC

Software

nginx 1.18.0

Details

http://195.20.16.35/

Status	404 Not Found
Body Hash	sha1:a4cb76424dc44433a2df01fe8b0bbd836d15e970
HTML Title	Error
Response Body	

```
Cannot GET /
```

Additional Notes - PrivateLoader/Mirai

There is another similar pattern in the IP of `91.92.244[.]70` from URLHaus.

This search returns 10 results with hits for PrivateLoader and other malware.

```
services.http.response.html_title="403 Forbidden" and services.port:22 and
services.port:80 and service_count:2 and autonomous_system.asn="394711"
```