Identifying Simple Pivot Points in Malware Infrastructure - RisePro Stealer

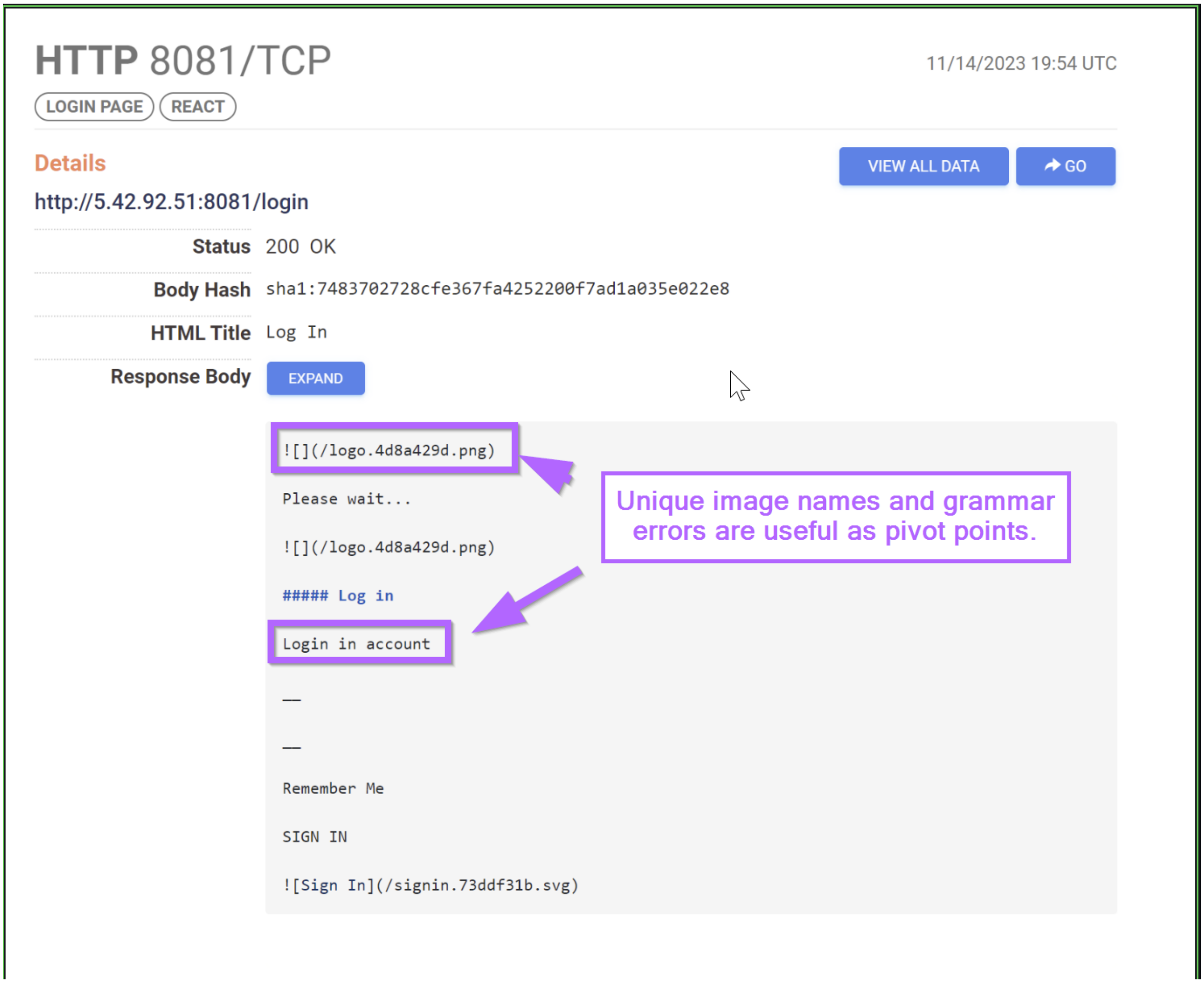
embee-research.ghost.io/identifying-risepro-panels-using-censys/

Matthew

November 15, 2023

Beginner

Identifying Simple pivot points in RisePro Stealer Infrastructure using Censys.



http://5.42.92.51:8081/login

Status	200 OK
Body Hash	sha1:7483702728cfe367fa4252200f7ad1a035e022e8
HTML Title	Log In
Response Body	

```
![](/logo.4d8a429d.png)

Please wait...

![](/logo.4d8a429d.png)

##### Log in

Login in account

—

—

Remember Me

SIGN IN

![Sign In](/signin.73ddf31b.svg)
```

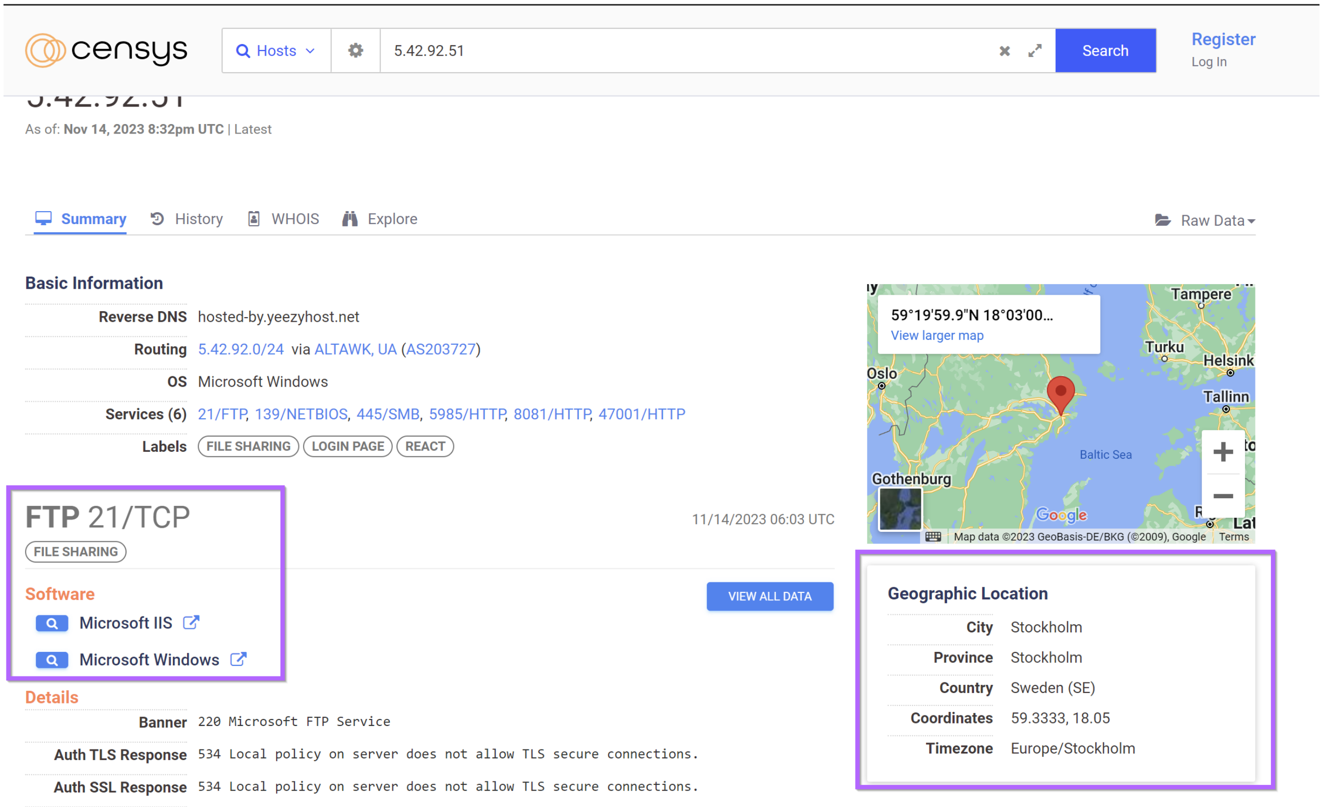
In a previous post we analysed a Redline stealer sample and obtained a C2 address of `5.42.92[.]51:19057`.

In this post, we'll demonstrate how to pivot from this c2 address to identify a total of 16 additional related servers.

Initial Search With Censys

We can begin by performing a basic search for the c2 on Censys.

This search reveals some basic information such as running services, ASN and the location of the server.



5.42.92.51

As of: **Nov 14, 2023 8:32pm UTC** | Latest

Basic Information

Reverse DNS	hosted-by.yeezyhost.net
Routing	5.42.92.0/24 via ALTAWK, UA (AS203727)
OS	Microsoft Windows
Services (6)	21/FTP, 139/NETBIOS, 445/SMB, 5985/HTTP, 8081/HTTP, 47001/HTTP
Labels	FILE SHARING · LOGIN PAGE · REACT

FTP 21/TCP

FILE SHARING

11/14/2023 06:03 UTC

Software

- Microsoft IIS
- Microsoft Windows

Details

Banner	`220 Microsoft FTP Service`
Auth TLS Response	`534 Local policy on server does not allow TLS secure connections.`
Auth SSL Response	`534 Local policy on server does not allow TLS secure connections.`

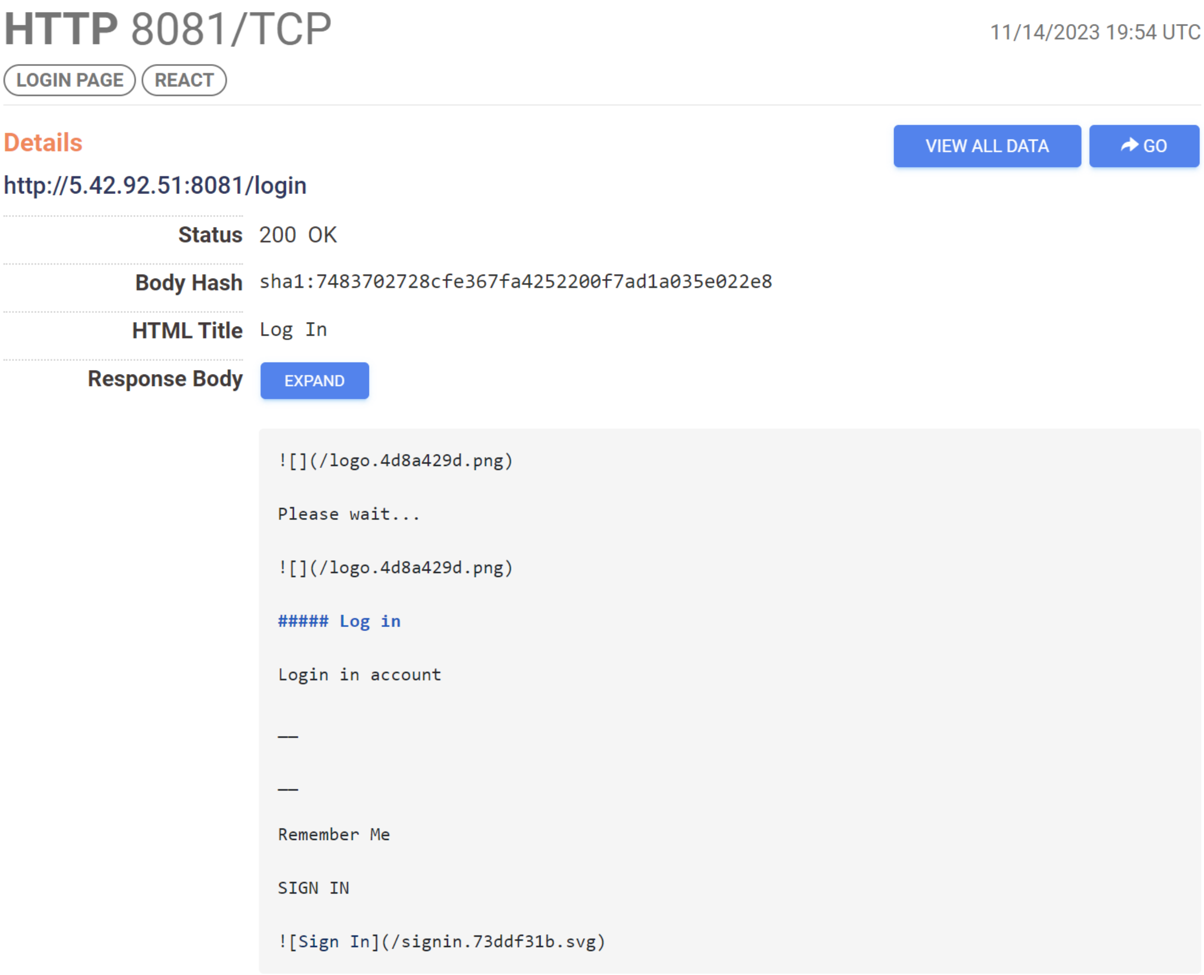
Geographic Location

City	Stockholm
Province	Stockholm
Country	Sweden (SE)
Coordinates	59.3333, 18.05
Timezone	Europe/Stockholm

The initial services do not appear to be useful, there isn't much to pivot from on ports on ports `21,139,445 and 5985`

However, there is an interesting HTTP service running on port `8081`.

This service appears to be hosting a login panel. (These panels are self hosted by RisePro users, according to this report from FlashPoint)



HTTP 8081/TCP

11/14/2023 19:54 UTC

Details

http://5.42.92.51:8081/login

Status	200 OK
Body Hash	sha1:7483702728cfe367fa4252200f7ad1a035e022e8
HTML Title	Log In
Response Body	

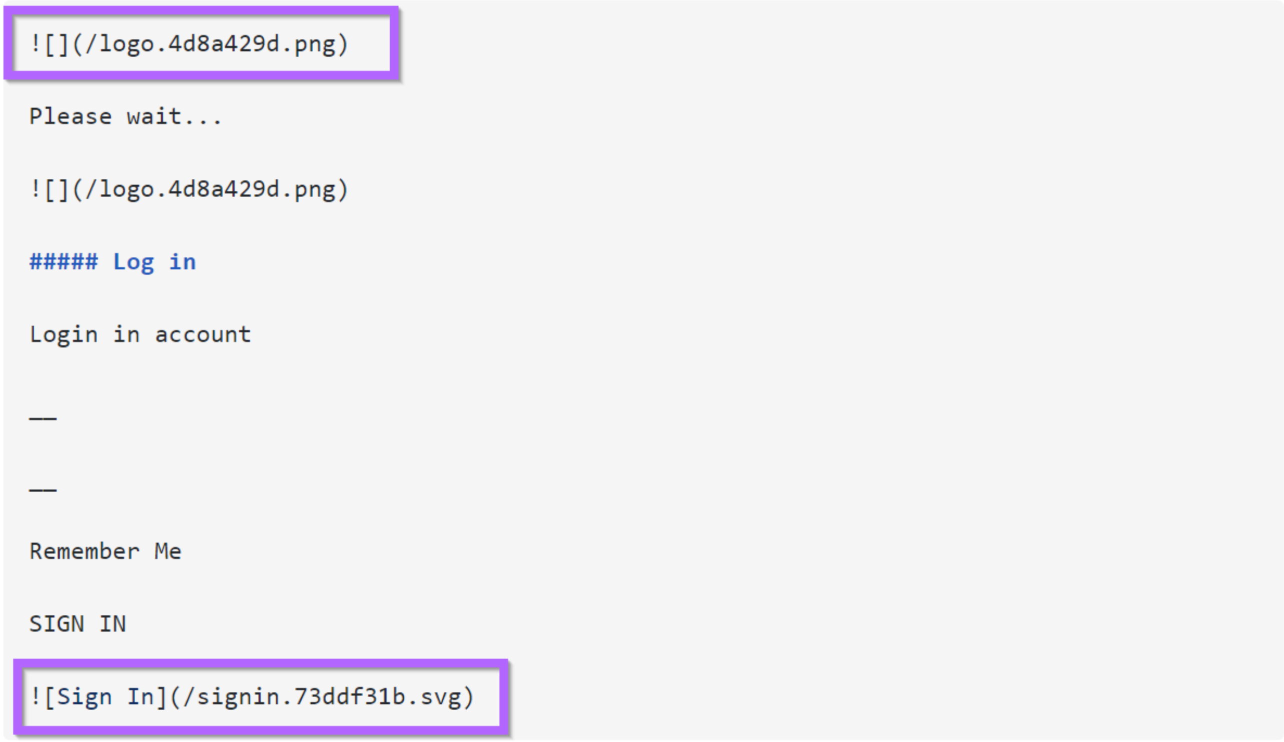
```
![](/logo.4d8a429d.png)

Please wait...

![](/logo.4d8a429d.png)

##### Log in

Login in account

—

—

Remember Me

SIGN IN

![Sign In](/signin.73ddf31b.svg)
```

This HTTP service is interesting and contains multiple opportunities for pivoting to additonal servers.

Opportunity 1: Pivoting With Image Names

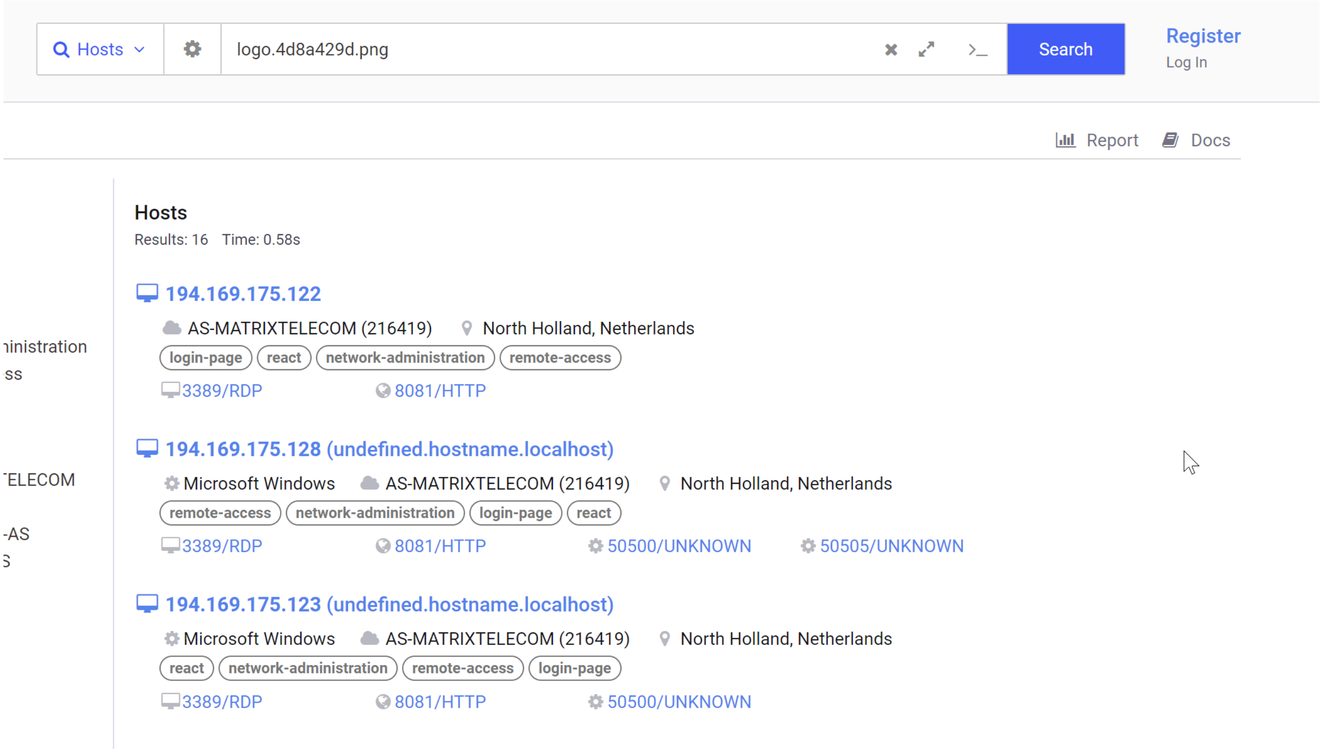
Within the screenshot above, we can see some raw html of the login page.

Looking closely, we can see some relatively unique names used for the `.png` and `.svg` images.



```
![](/logo.4d8a429d.png)

Please wait...

![](/logo.4d8a429d.png)

##### Log in

Login in account

__

__

Remember Me

SIGN IN

![Sign In](/signin.73ddf31b.svg)
```

By plugging either of these names into a Censys search, there are a total of 16 servers identified.



Hosts
Results: 16 Time: 0.58s

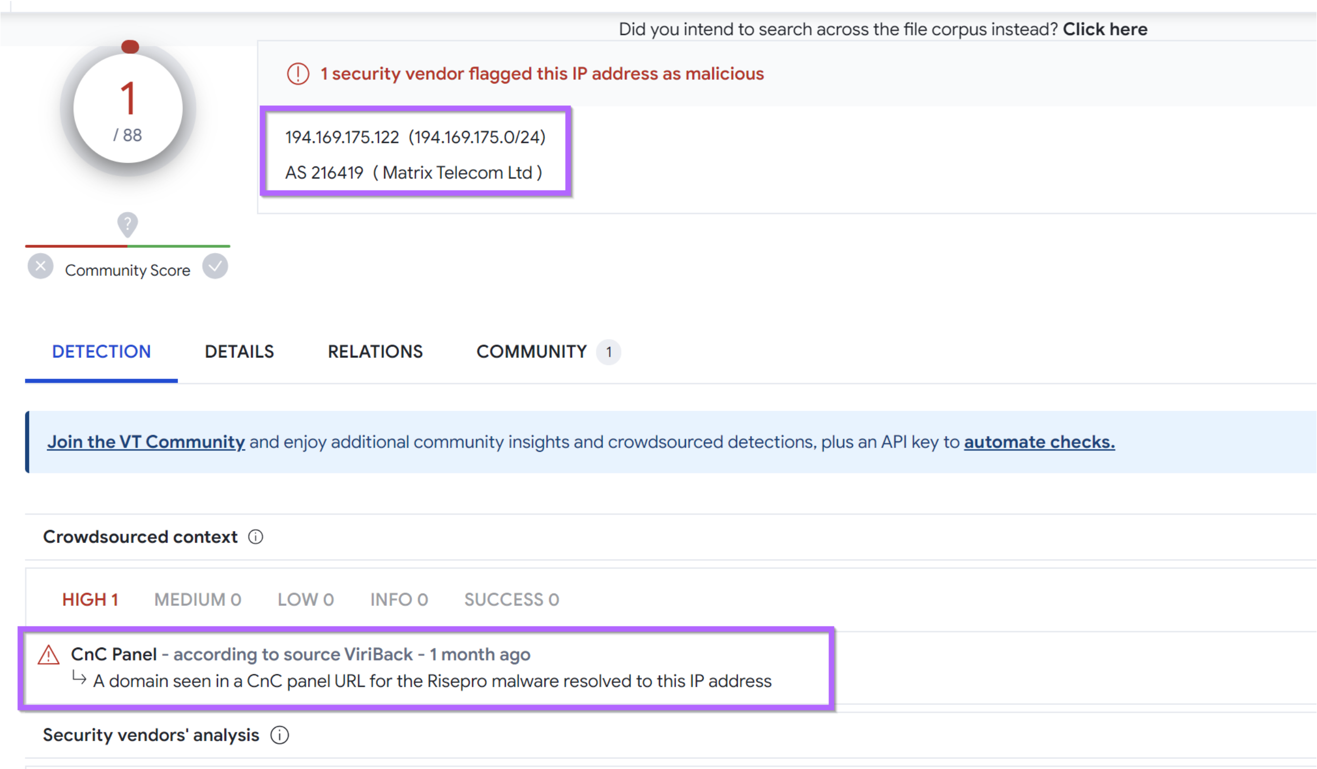
194.169.175.122
AS-MATRIXTELECOM (216419) North Holland, Netherlands
login-page react network-administration remote-access
3389/RDP 8081/HTTP

194.169.175.128 (undefined.hostname.localhost)
Microsoft Windows AS-MATRIXTELECOM (216419) North Holland, Netherlands
remote-access network-administration login-page react
3389/RDP 8081/HTTP 50500/UNKNOWN 50505/UNKNOWN

194.169.175.123 (undefined.hostname.localhost)
Microsoft Windows AS-MATRIXTELECOM (216419) North Holland, Netherlands
react network-administration remote-access login-page
3389/RDP 8081/HTTP 50500/UNKNOWN

We can take the first returned IP of `194.169.175[.]122` and search for it in Virustotal.

This returns `1/88` detections, as well as a reference to Risepro malware. (Similar results can be obtained for most the remaining 15 servers)



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

1 security vendor flagged this IP address as malicious

194.169.175.122 (194.169.175.0/24)
AS 216419 (Matrix Telecom Ltd)

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

Crowdsourced context

HIGH 1 MEDIUM 0 LOW 0 INFO 0 SUCCESS 0

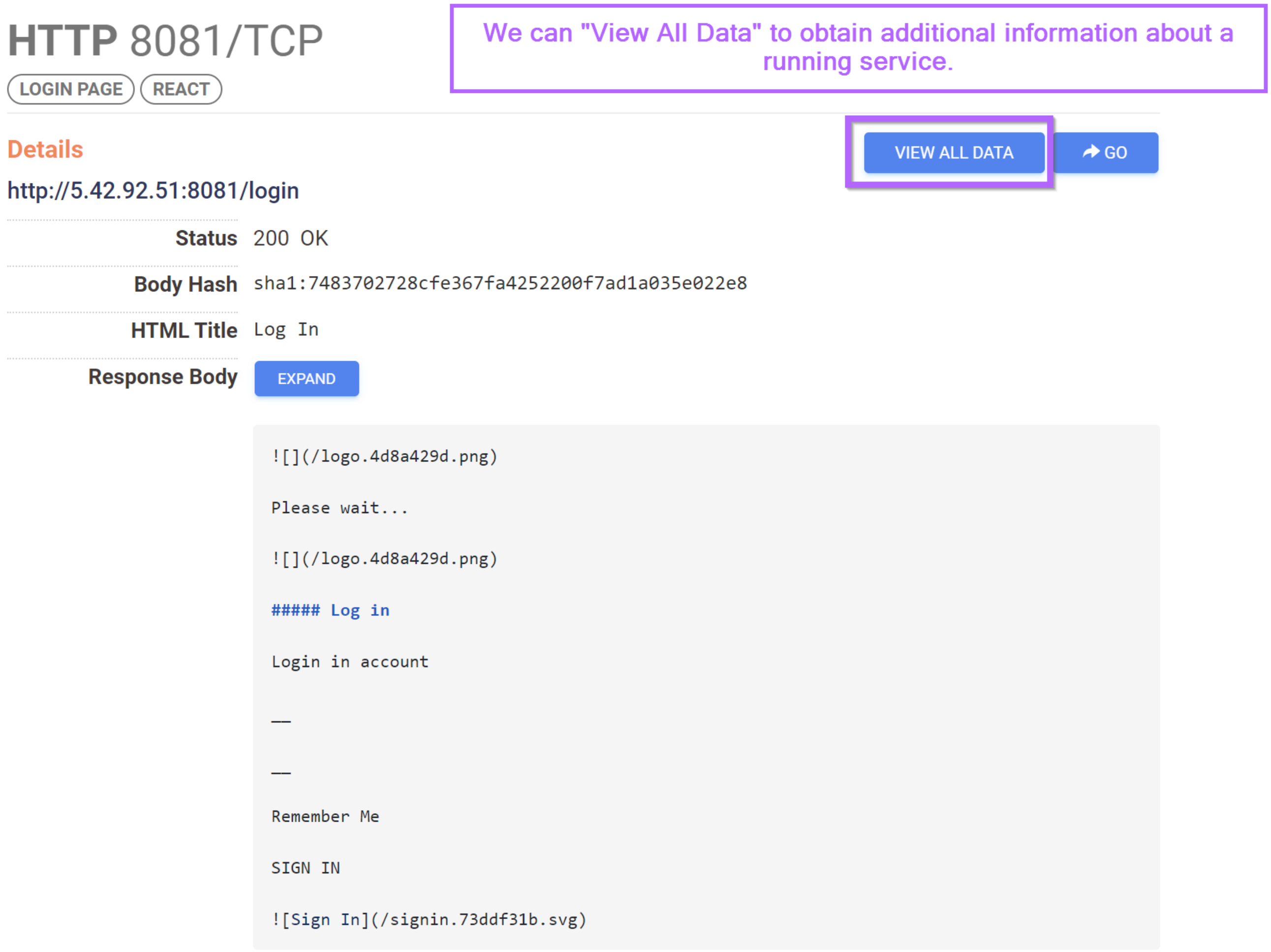
CnC Panel - according to source ViriBack - 1 month ago
↳ A domain seen in a CnC panel URL for the Risepro malware resolved to this IP address

Security vendors' analysis

Opportunity 2: Pivoting With Banner Hash

Censys is able to obtain a significant amount of information about the running service, some of which is not displayed by default.

We can view this additional information by clicking on "View All Data".



We can "View All Data" to obtain additional information about a running service.

HTTP 8081/TCP

Details

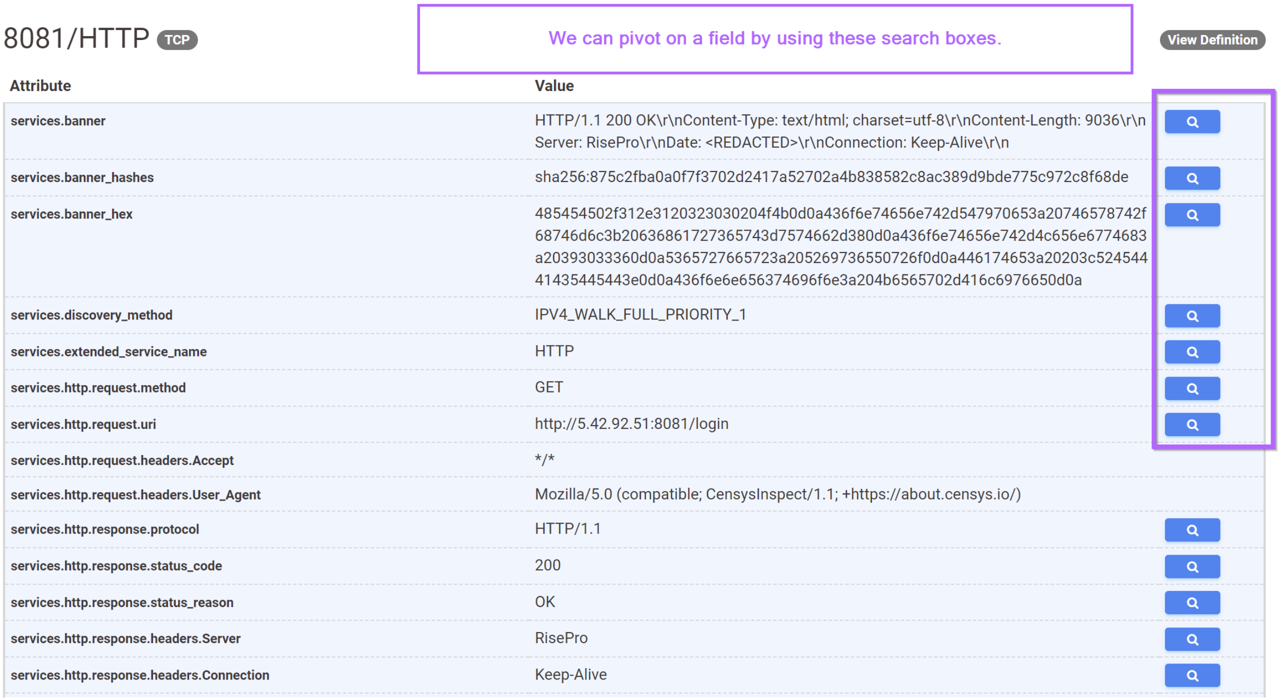
http://5.42.92.51:8081/login

Status	200 OK
Body Hash	sha1:7483702728cfe367fa4252200f7ad1a035e022e8
HTML Title	Log In
Response Body	EXPAND

```
![](/logo.4d8a429d.png)

Please wait...

![](/logo.4d8a429d.png)

##### Log in

Login in account

__

__

Remember Me

SIGN IN

![Sign In](/signin.73ddf31b.svg)
```

This returns a lot of information about the running service on port `8081`.

Each piece of information can be searched by clicking on the "search" box next to each option.



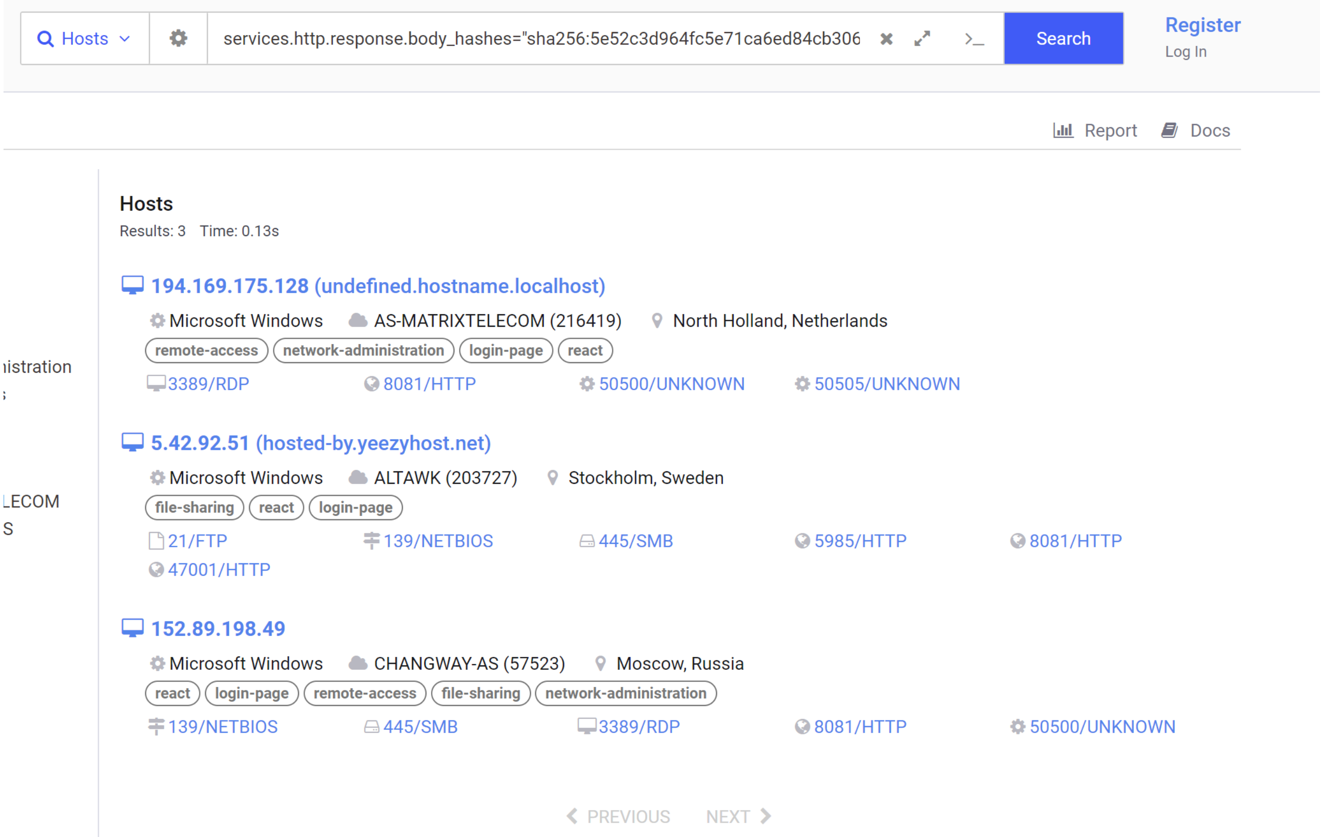
8081/HTTP TCP

We can pivot on a field by using these search boxes.

Attribute	Value
services.banner	HTTP/1.1 200 OK\r\nContent-Type: text/html; charset=utf-8\r\nContent-Length: 9036\r\n Server: RisePro\r\nDate: <REDACTED>\r\nConnection: Keep-Alive\r\n
services.banner_hashes	sha256:875c2fba0a0f7f3702d2417a52702a4b838582c8ac389d9bde775c972c8f68de
services.banner_hex	485454502f312e3120323030204f4b0d0a436f6e74656e742d547970653a20746578742f68746d6c3b20636861727365743d7574662d380d0a436f6e74656e742d4c656e6774683a20393033360d0a5365727665723a205269736550726f0d0a446174653a20203c52454441435445443e0d0a436f6e6e656374696f6e3a204b6565702d416c6976650d0a
services.discovery_method	IPV4_WALK_FULL_PRIORITY_1
services.extended_service_name	HTTP
services.http.request.method	GET
services.http.request.uri	http://5.42.92.51:8081/login
services.http.request.headers.Accept	*/*
services.http.request.headers.User_Agent	Mozilla/5.0 (compatible; CensysInspect/1.1; +https://about.censys.io/)
services.http.response.protocol	HTTP/1.1
services.http.response.status_code	200
services.http.response.status_reason	OK
services.http.response.headers.Server	RisePro
services.http.response.headers.Connection	Keep-Alive

For example, we can click on the `services.banner_hashes` search box to attempt a pivot from a hash of the banner, which contains a reference to "RisePro".

Pivoting on the banner hash returns 3 results.



services.http.response.body_hashes="sha256:5e52c3d964fc5e71ca6ed84cb306

ıistration
;
LECOM
S

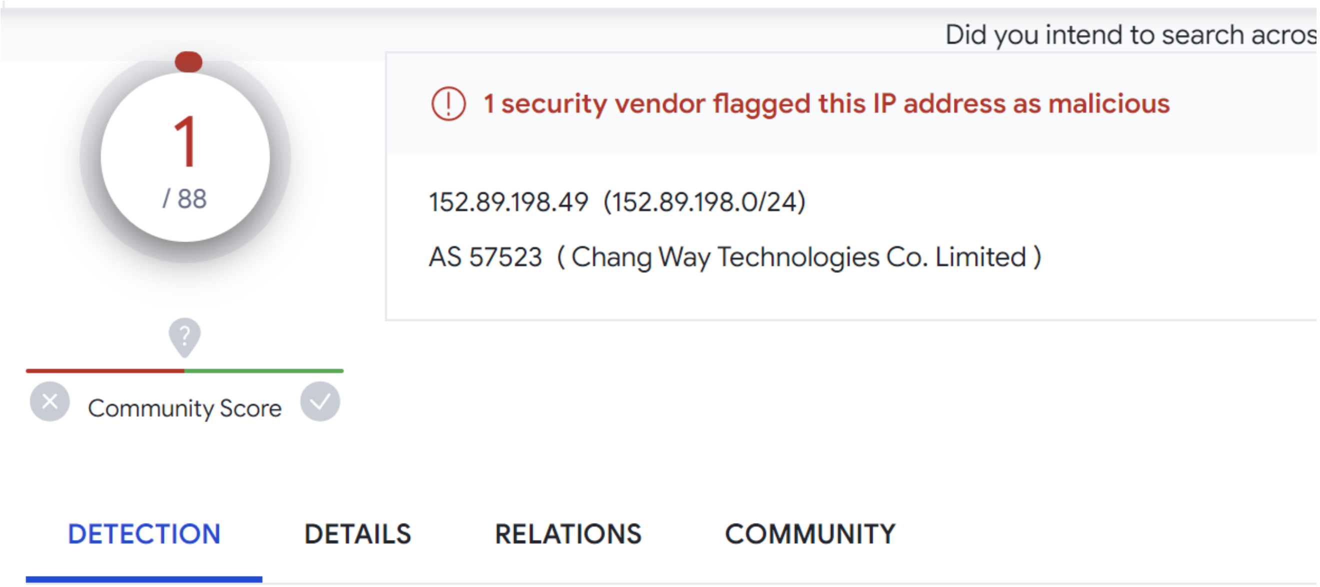
Hosts
Results: 3 Time: 0.13s

194.169.175.128 (undefined.hostname.localhost)
Microsoft Windows AS-MATRIXTELECOM (216419) North Holland, Netherlands
remote-access network-administration login-page react
3389/RDP 8081/HTTP 50500/UNKNOWN 50505/UNKNOWN

5.42.92.51 (hosted-by.yeezyhost.net)
Microsoft Windows ALTAWK (203727) Stockholm, Sweden
file-sharing react login-page
21/FTP 139/NETBIOS 445/SMB 5985/HTTP 8081/HTTP
47001/HTTP

152.89.198.49
Microsoft Windows CHANGWAY-AS (57523) Moscow, Russia
react login-page remote-access file-sharing network-administration
139/NETBIOS 445/SMB 3389/RDP 8081/HTTP 50500/UNKNOWN

Of the results is a new IP of `152.89.198[.]49`. Which has 1/88 detections on Virustotal.



1 security vendor flagged this IP address as malicious

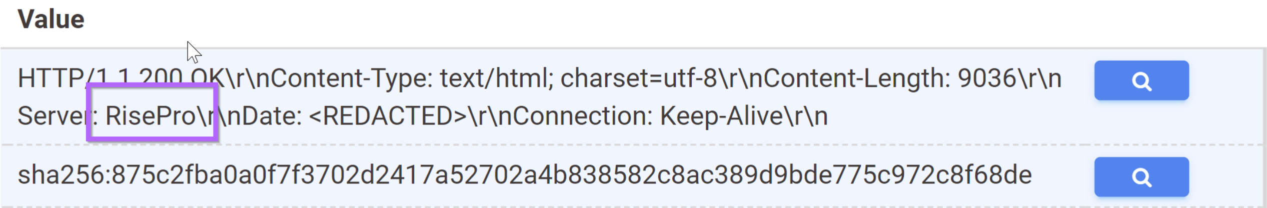
152.89.198.49 (152.89.198.0/24)

AS 57523 (Chang Way Technologies Co. Limited)

Opportunity 3: Pivoting From RisePro String

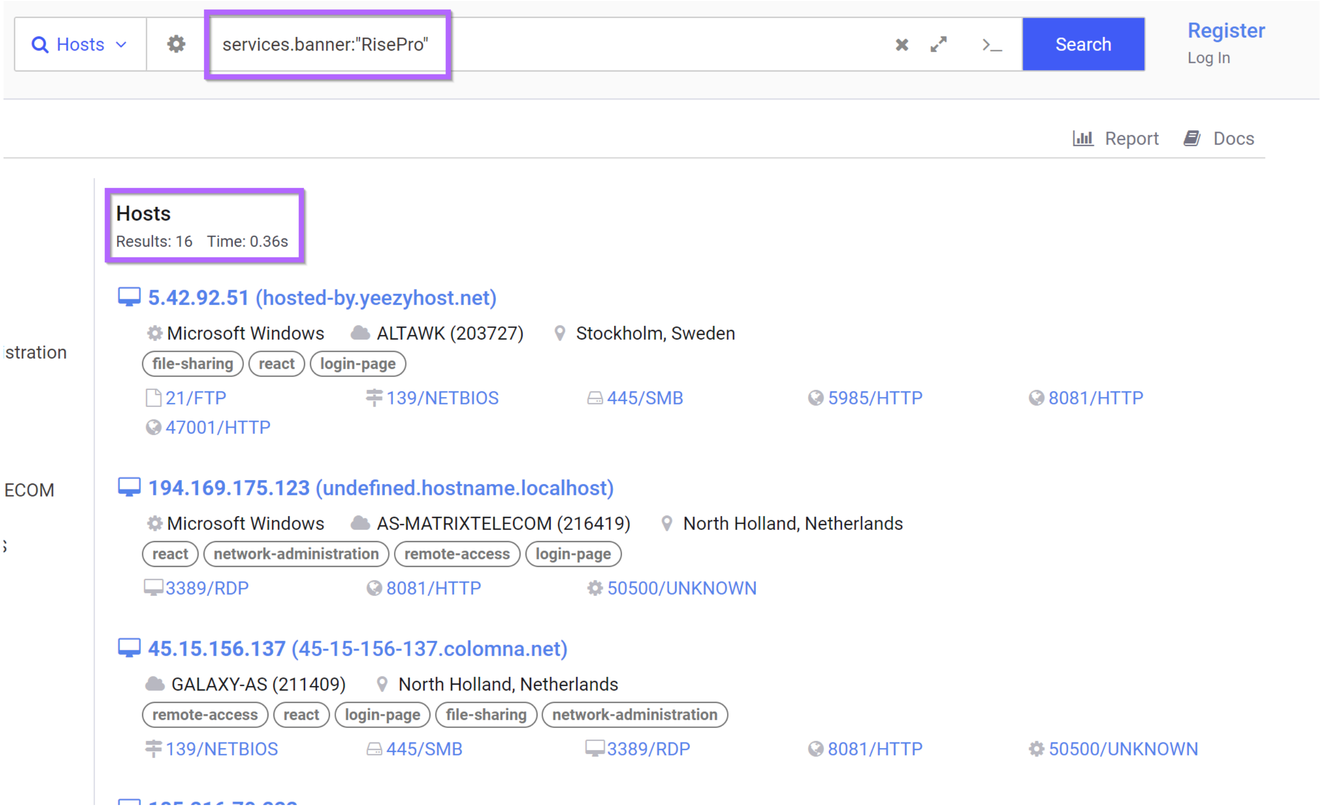
The previous search using banner hashes only returned 3 results.

Since the most interesting piece of the banner is the reference to "RisePro", we can skip using the hash and instead look for any banner with a RisePro reference.



Value
HTTP/1.1 200 OK\r\nContent-Type: text/html; charset=utf-8\r\nContent-Length: 9036\r\nServer: RisePro\r\nDate: <REDACTED>\r\nConnection: Keep-Alive\r\n
sha256:875c2fba0a0f7f3702d2417a52702a4b838582c8ac389d9bde775c972c8f68de

By searching for any banner containing a reference to "RisePro", we can obtain the same 16 results that were obtained by pivoting on the `.png` image name.



services.banner:"RisePro"

Hosts
Results: 16 Time: 0.36s

5.42.92.51 (hosted-by.yeezyhost.net)
Microsoft Windows ALTAWK (203727) Stockholm, Sweden
file-sharing react login-page
21/FTP 139/NETBIOS 445/SMB 5985/HTTP 8081/HTTP 47001/HTTP

194.169.175.123 (undefined.hostname.localhost)
Microsoft Windows AS-MATRIXTELECOM (216419) North Holland, Netherlands
react network-administration remote-access login-page
3389/RDP 8081/HTTP 50500/UNKNOWN

45.15.156.137 (45-15-156-137.colomna.net)
GALAXY-AS (211409) North Holland, Netherlands
remote-access react login-page file-sharing network-administration
139/NETBIOS 445/SMB 3389/RDP 8081/HTTP 50500/UNKNOWN

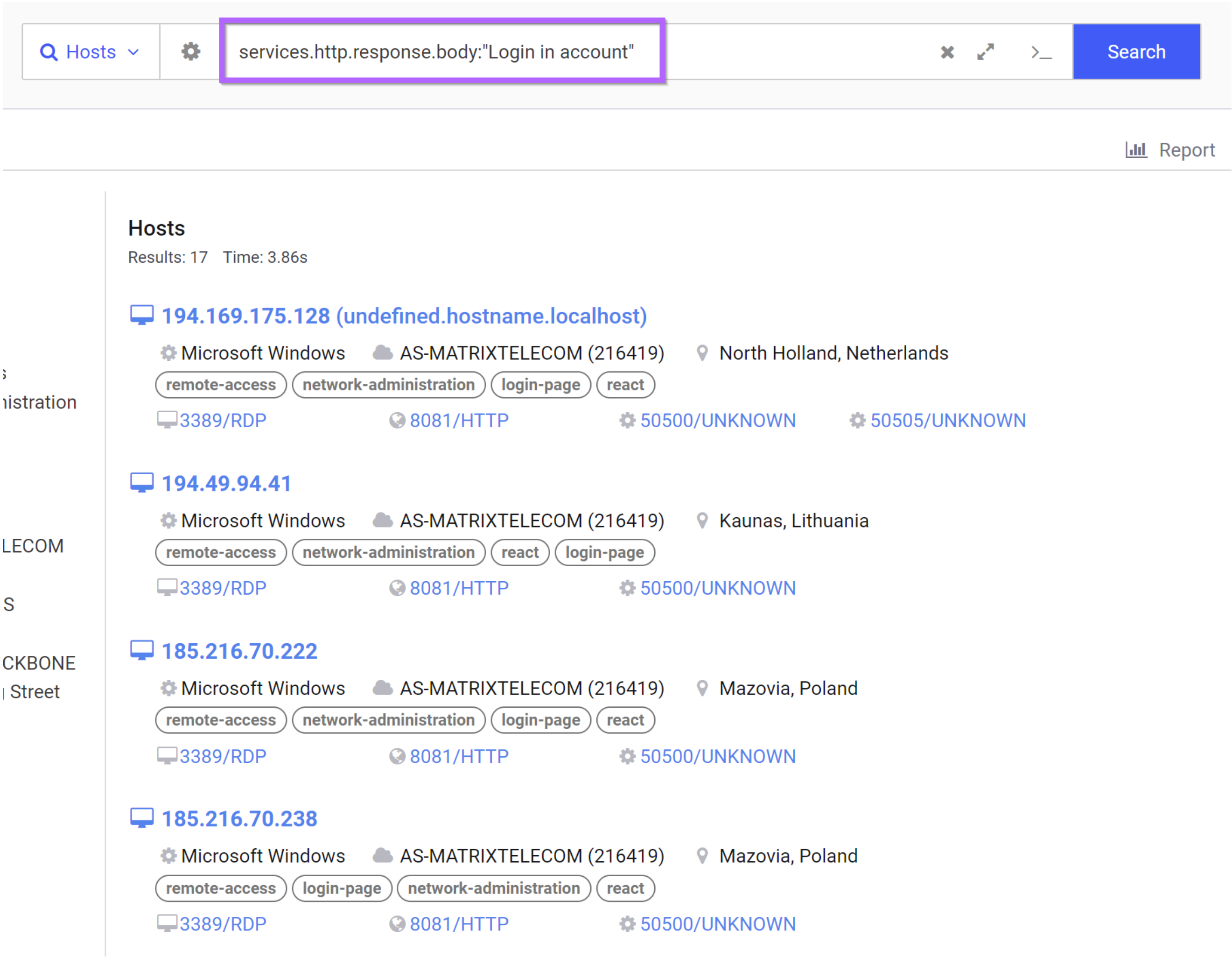
Opportunity 4: Pivoting From Grammatical Errors

There is a small grammatical error contained in the initial html.

If we assume that this error is present across login panels, then we can use it as an additional pivot point.

```
![](/logo.4d8a429d.png)

Please wait...

![](/logo.4d8a429d.png)

##### Log in

Login in account

—

—

Remember Me

SIGN IN

![Sign In](/signin.73ddf31b.svg)
```

By searching for the error inside of the response body, we can again obtain the same 16 results, as well as one additional server.



services.http.response.body:"Login in account"

Hosts

Results: 17 Time: 3.86s

194.169.175.128 (undefined.hostname.localhost)
Microsoft Windows AS-MATRIXTELECOM (216419) North Holland, Netherlands
remote-access network-administration login-page react
3389/RDP 8081/HTTP 50500/UNKNOWN 50505/UNKNOWN

194.49.94.41
Microsoft Windows AS-MATRIXTELECOM (216419) Kaunas, Lithuania
remote-access network-administration react login-page
3389/RDP 8081/HTTP 50500/UNKNOWN

185.216.70.222
Microsoft Windows AS-MATRIXTELECOM (216419) Mazovia, Poland
remote-access network-administration login-page react
3389/RDP 8081/HTTP 50500/UNKNOWN

185.216.70.238
Microsoft Windows AS-MATRIXTELECOM (216419) Mazovia, Poland
remote-access login-page network-administration react
3389/RDP 8081/HTTP 50500/UNKNOWN

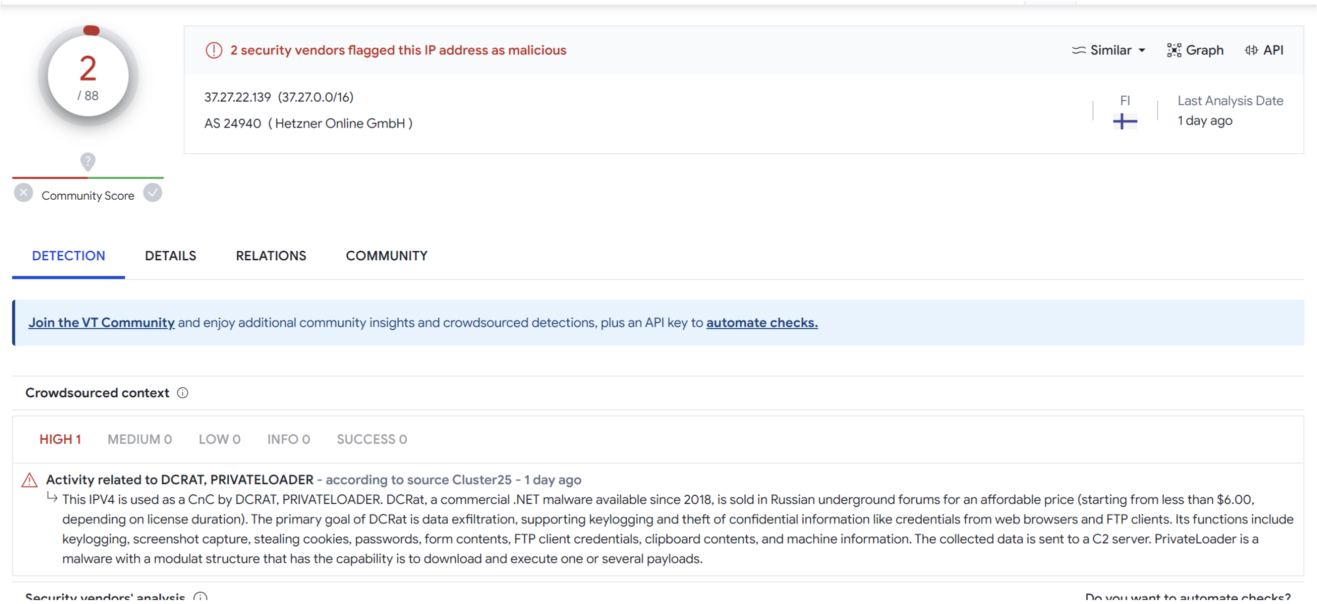
The additional server has an ip of `61.134.65[.]198` and appears to be a chinese site unrelated to RisePro.

Despite the 1 additional false positive, the remaining 16 results appear malicious and related to RisePro Stealer. This confirms that the grammar error is useful as an additional pivot point.

Basic Analysis of Newly Identified Servers

Using the 16 RisePro servers returned from our search, there are some interesting observations.

Here is an example where `37.27.22[.]139` is marked as "DCRAT,PRIVATELOADER" and yet only has 2/88 detections.



2 security vendors flagged this IP address as malicious

37.27.22.139 (37.27.0.0/16)
AS 24940 (Hetzner Online GmbH)

FI

Last Analysis Date
1 day ago

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

Crowdsourced context

HIGH 1 MEDIUM 0 LOW 0 INFO 0 SUCCESS 0

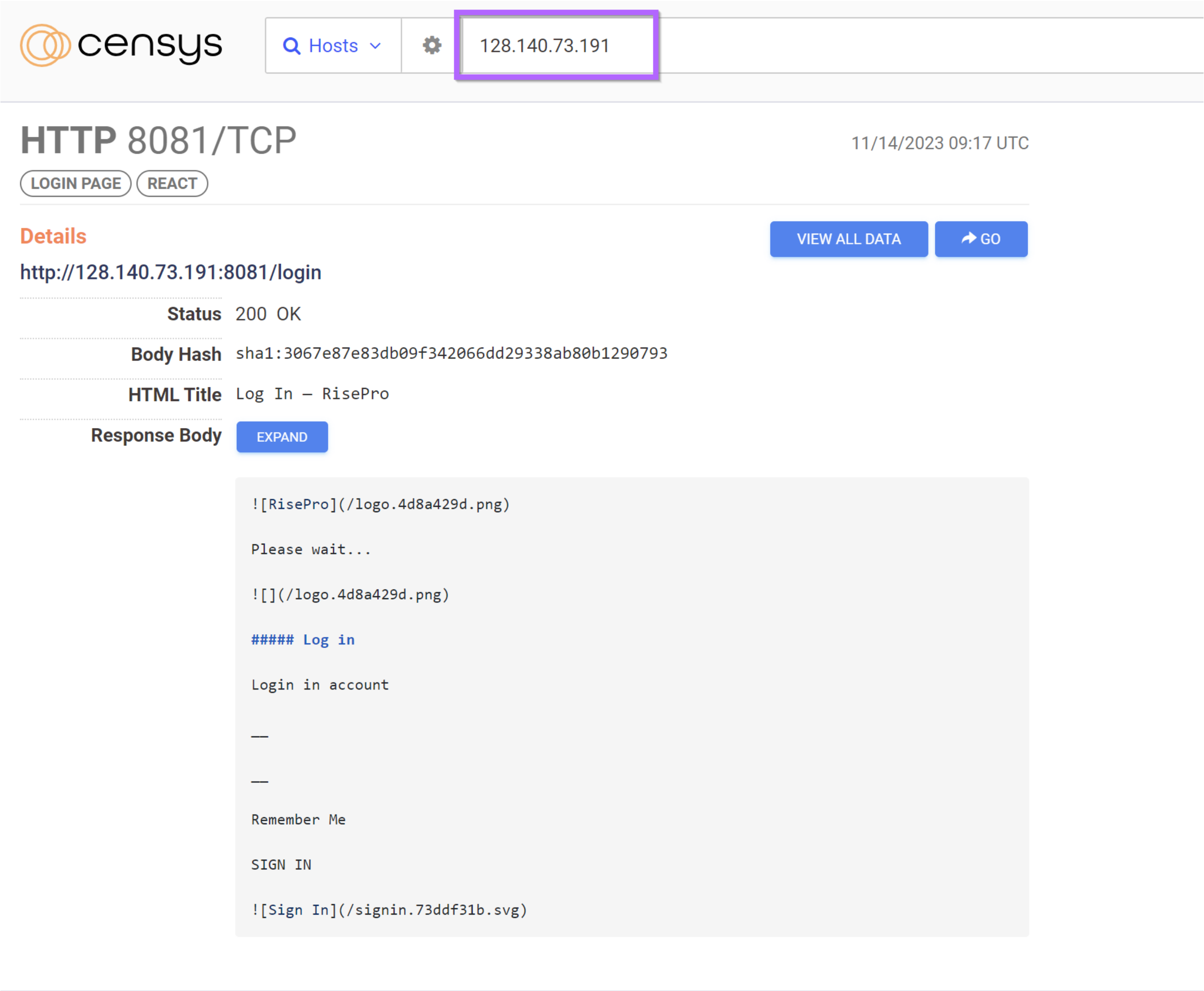
Activity related to DCRAT, PRIVATELOADER - according to source Cluster25 - 1 day ago

↳ This IPV4 is used as a CnC by DCRAT, PRIVATELOADER. DCRat, a commercial .NET malware available since 2018, is sold in Russian underground forums for an affordable price (starting from less than $6.00, depending on license duration). The primary goal of DCRat is data exfiltration, supporting keylogging and theft of confidential information like credentials from web browsers and FTP clients. Its functions include keylogging, screenshot capture, stealing cookies, passwords, form contents, FTP client credentials, clipboard contents, and machine information. The collected data is sent to a C2 server. PrivateLoader is a malware with a modulat structure that has the capability is to download and execute one or several payloads.

Security vendors' analysis

Do you want to automate checks?

Another server `128.140.73[.]191` contains the same C2 panel and has 0/88 detections.



HTTP 8081/TCP

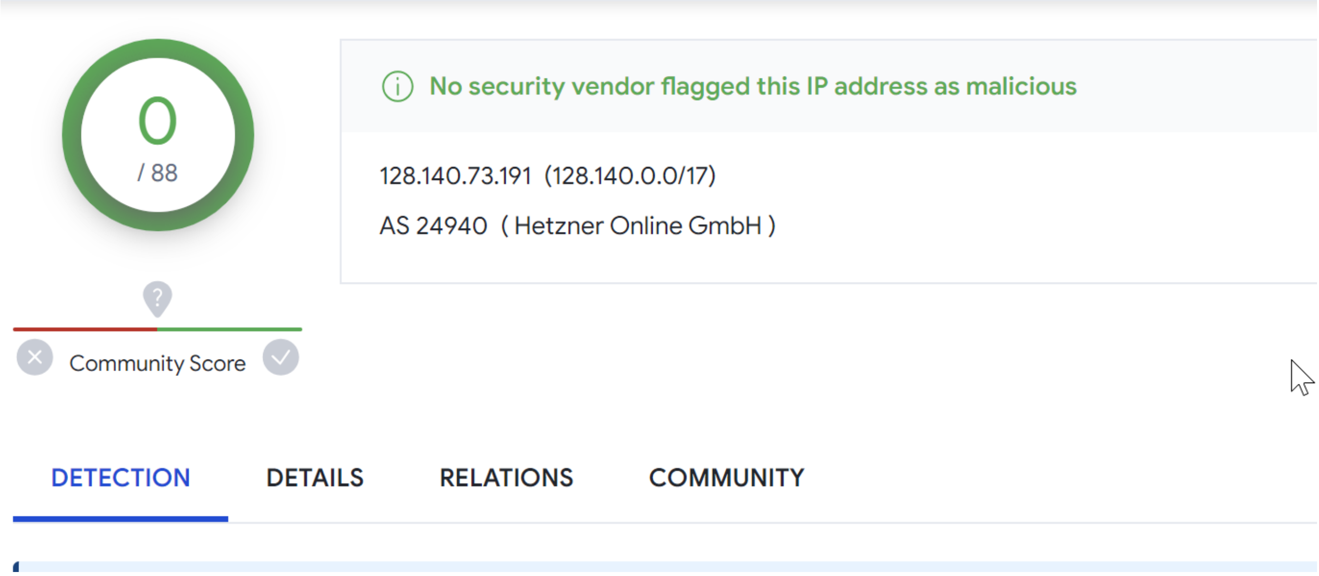
11/14/2023 09:17 UTC

Details

http://128.140.73.191:8081/login

Status	200 OK
Body Hash	sha1:3067e87e83db09f342066dd29338ab80b1290793
HTML Title	Log In — RisePro
Response Body	EXPAND

```
![RisePro](/logo.4d8a429d.png)

Please wait...

![](/logo.4d8a429d.png)

##### Log in

Login in account

—

—

Remember Me

SIGN IN

![Sign In](/signin.73ddf31b.svg)
```

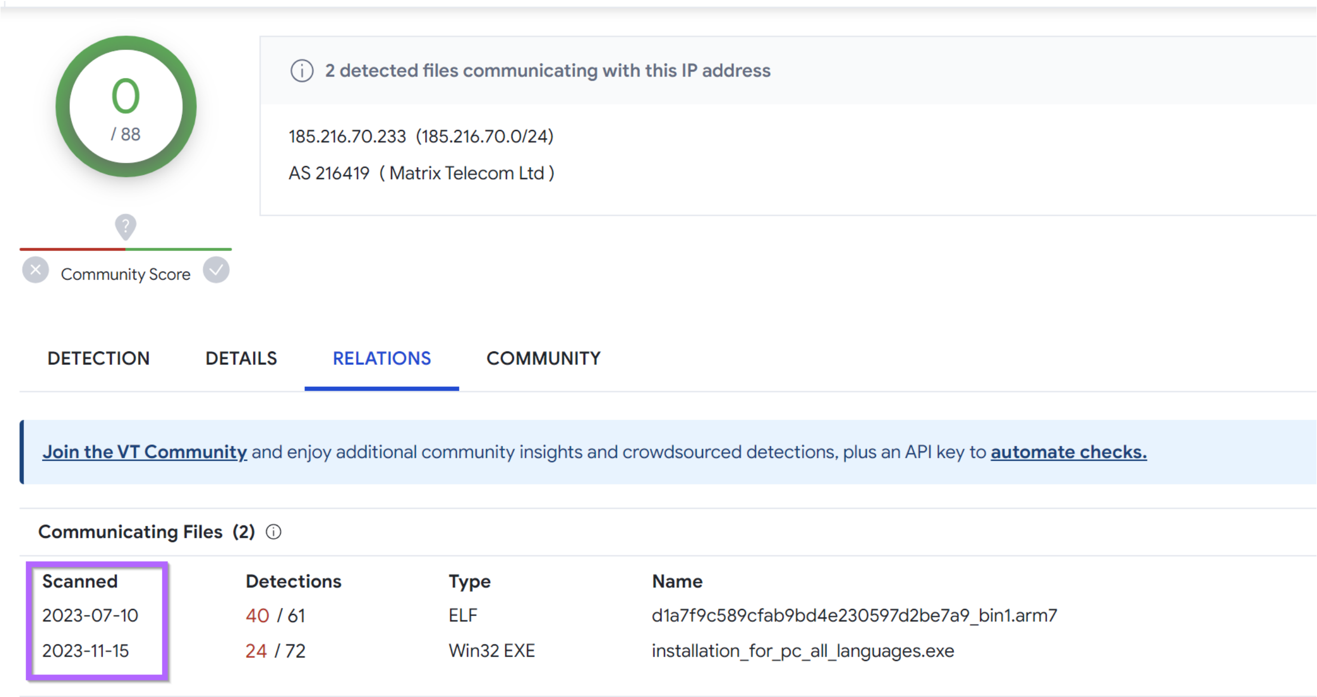


No security vendor flagged this IP address as malicious

128.140.73.191 (128.140.0.0/17)

AS 24940 (Hetzner Online GmbH)

Another server 185.216.70[.]233 has 0/88 detections, with malicious files communicating as far back as July 2023.



2 detected files communicating with this IP address

185.216.70.233 (185.216.70.0/24)
AS 216419 (Matrix Telecom Ltd)

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

Communicating Files (2)

Scanned	Detections	Type	Name
2023-07-10	40 / 61	ELF	d1a7f9c589cfab9bd4e230597d2be7a9_bin1.arm7
2023-11-15	24 / 72	Win32 EXE	installation_for_pc_all_languages.exe

The rest of the servers were largely repeats of those already mentioned. A full list of the results can be found below.

List of Returned C2's

```
#RisePro Server List - VT Detections as of 2023/11/15

5.42.92[.]51 - 12/88
37.27.22[.]139 - 2/88
45.15.156[.]137 - 1/88
85.209.11[.]247 -  7/88
91.103.253[.]146 - 1/88
109.107.182[.]9 - 1/88
128.140.73[.]191 - 0/88
152.89.198[.]49 -  1/88
185.216.70[.]222 - 1/88
185.216.70[.]233 - 0/88
185.216.70[.]238 - 13/88
194.49.94[.]41 - 1/88
194.169.175[.]113 - 1/88
194.169.175[.]122 - 1/88
194.169.175[.]123 - 1/88
194.169.175[.]128 - 20/88
```