OPENHUNTING.IO

THREAT HUNTING MALWARE INFRASTRUCTURE

A Method for Threat Hunting & Intelligence Team to identifying Malware infrastructure using Search Engine

THREAT HUNTING MALWARE INFRASTRUCTURE

Release Date

Sunday, 3 December 2023

Threat Intelligence Analyst

Rizqy Rionaldy, CTIA, CEH, CHFI, ECIH

Security Researcher @openhunting.io

CONTENTS

INTRODUCTION

Proactive methods for dealing with cyber threats are growing along with the complexity of malware. Malware has an infrastructure that supports its operation. This infrastructure includes servers, domains, IP addresses, and other components that allow malware to communicate and carry out malicious activities. Malware infrastructure analysis is key to understanding and combating these threats. Malware Infrastructure Analysis investigates these elements to dissect anatomy, uncover hidden threats, strengthen defenses, and ultimately protect systems from attack. In the current era of threat development, threat actors continue to improve technically, it is also important as a cyber threat to carry out threat hunting strategies to stay one step away from attackers. This article will discuss malware infrastructure analysis methods using infrastructure search engines to obtain a list of infrastructure used by malware.

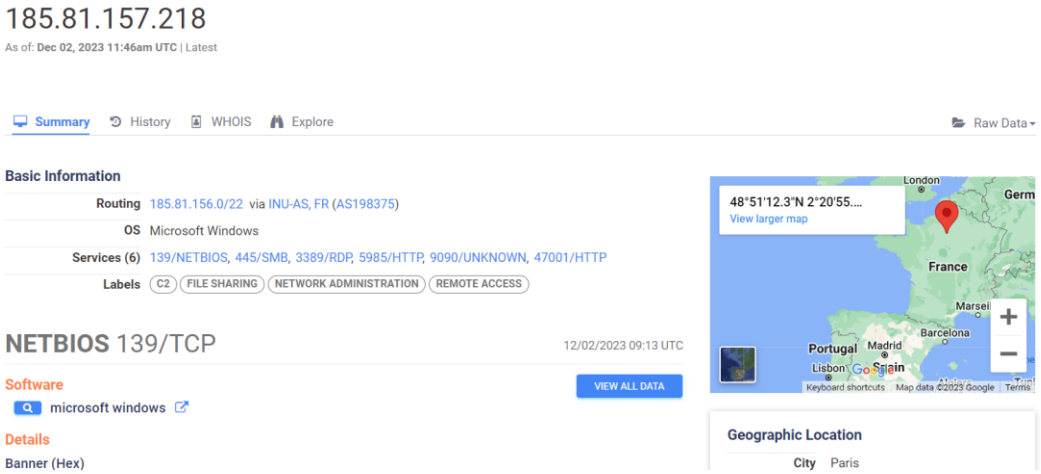
As a final part, I would like to thank the very interesting article from @MichalKoczwara and @Matthew. This article was inspired by the thoughts and ideas they shared. A collaborative spirit in the world of cybersecurity is the key to building a resilient and adaptive defense.

INFRASTRUCTURE ANALYSIS WITH SEARCH ENGINE

In the initial section, we will delve into understanding malware infrastructure analysis methods by leveraging outcomes from the **Censys Search Engine**. In this instance, we will conduct an example search using **AsyncRAT malware**.

AsyncRAT malware identified Indicators of Compromise (IoC) linked to the C2 IP of the malware through an analysis of the IP 185.81.157[.]218. In practice, acquiring the C2 IP of malware can be accomplished through diverse methods, including Malware Sample Analysis, Twitter, Threat Intelligence Reports, and Threatfox, among

others. We searched the IP Address **185.81.157[.]218** using Censys and obtained the following results.



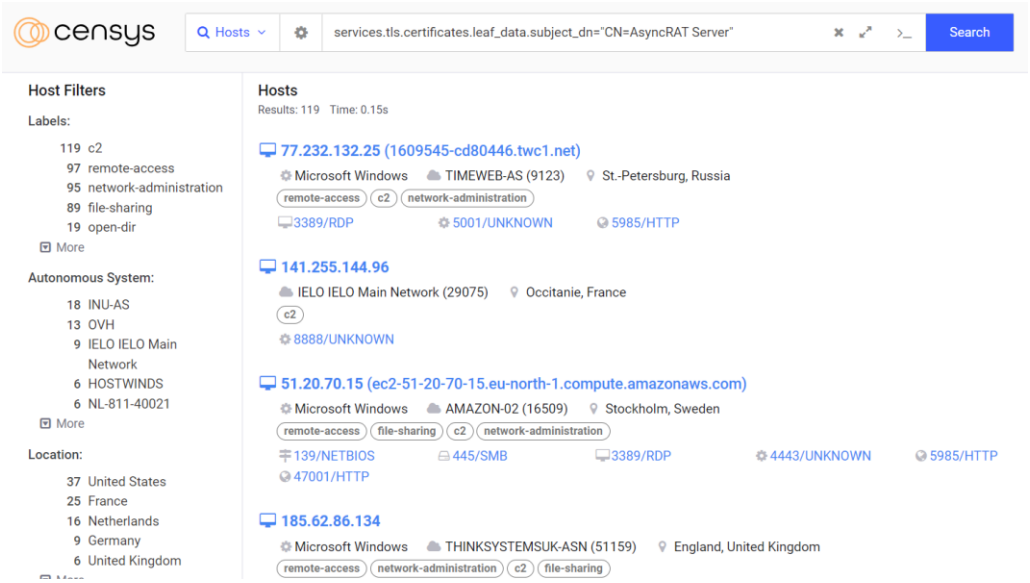
Afterward, an in-depth analysis was conducted to examine the details of the infrastructure used.

services.service_name	UNKNOWN	
services.software.uniform_resource_identifier	cpe:2.3:a:asyncrat:asyncrat:*:*:*:*:*:*:*:*	
services.software.part	a	
services.software.vendor	AsyncRAT	
services.software.product	AsyncRAT	
services.software.other.device	C2	
services.software.source	OSI_APPLICATION_LAYER	
services.source_ip	167.94.138.36	
services.tls.version_selected	TLSv1_0	
services.tls.cipher_selected	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	
services.tls.certificates.leaf_fp_sha_256	9931aa2da55225079f51aa1f1f1477ead3c4cd9c142fe3ca59a7b30f475f8b4c	
services.tls.certificates.leaf_data.subject_dn	CN=AsyncRAT Server	
services.tls.certificates.leaf_data.issuer_dn	CN=AsyncRAT Server	
services.tls.certificates.leaf_data.pubkey_bit_size	4096	
services.tls.certificates.leaf_data.pubkey_algorithm	RSA	
services.tls.certificates.leaf_data.tbs_fingerprint	e85a82295ede91e4dc9e959b277375f14ae054119d29691714f9f171e2804d06	

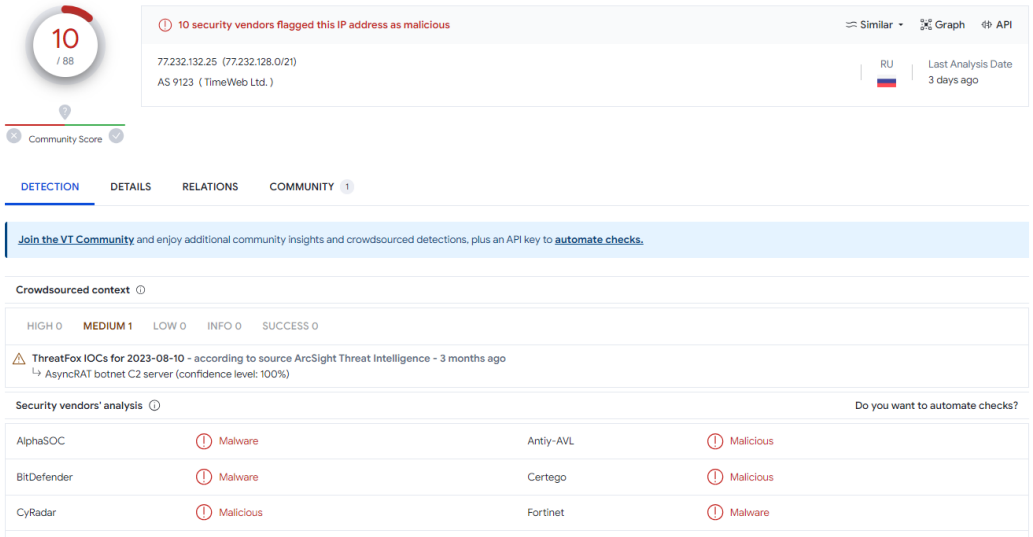
In the detailed information we discovered, several columns contain attributes with unique values that have drawn our attention.

Attribute	Value
services.software.vendor	AsyncRAT
services.software.product	AsyncRAT
services.tls.certificates.leaf_data.subject_dn	CN=AsyncRAT Server
services.tls.certificates.leaf_data.issuer_dn	CN=AsyncRAT Server
services.tls.certificates.leaf_data.issuer.common_name	AsyncRAT Server
services.tls.certificates.leaf_data.subject.common_name	AsyncRAT Server

Based on the data we obtained, we then tested our hypothesis by searching for one of the attributes used. Utilizing this attribute, we formulated a keyword query: services.tls.certificates.leaf_data.subject_dn="CN=AsyncRAT Server". The associated Censys Link unveiled a total of **119 relevant hosts**.



Following the search, the keyword query produced multiple lists of hosts. Subsequent validation through a VirusTotal search revealed the following results.



Search results are conclusively validated, as the IP hosts we obtained are recognized by VirusTotal as part of the AsyncRAT Botnet malware. While conducting Threat Hunting for the AsyncRAT malware on the Censys search engine, utilizing the IoC IP C2 **185.81.157[.]218**, we

unearthed several attribute values linked to the malware. These attributes offer valuable insights into the characteristics and behavior of the identified malware.

```
services.software.vendor=”AsyncRAT”
services.software.product=”AsyncRAT”
services.tls.certificates.leaf_data.subject_dn    =”CN=AsyncRAT
Server”
services.tls.certificates.leaf_data.issuer_dn=”CN=AsyncRAT Server”
services.tls.certificates.leaf_data.issuer.common_name=”AsyncRAT
Server”
services.tls.certificates.leaf_data.subject.common_name=”AsyncRAT
Server”
```

Identifying the attributes that define the characteristic features of malware infrastructure is not always a straightforward process. In the case of **AsyncRat**, we were fortunate as the malware directly provided information related to these attributes. However, it's crucial to acknowledge that certain malware may not overtly disclose distinctive attribute values. The following section will delve into methods for identifying and utilizing attributes in such scenarios.

EXAMPLE QUERY FOR ATTRIBUTE INFORMATION

After explaining how this method works in the first section, I will now share the query results obtained from an article by @Matthew, which I read on embee-research.ghost.io. These query results can be used as a reference for conducting Threat Hunting for Malware Infrastructure.

No	Malware	Query
1	**AsyncRAT** **Censys Link**	services.tls.certificates.leaf_data.subject.common_name:"AsyncRAT Server" or services.tls.certificates.leaf_data.issuer.common_name:"AsyncRAT Server"
2	**Solarmarker/ Jupyter** **Censys Link**	services:(ssh.server_host_key.fingerprint_sha256 = "c655bae831ca57a857b26d76a7c98a56a65d00fdab7d234a64addf8166e3cd09" and port = 22) and services:(service_name:HTTP and port:80) and not services.port:993

3	**Qakbot (Possibly Pikabot)** Censys Link	not dns.reverse_dns.names:* and services.http.response.html_title:"Slack is your productivity platform | Slack"
4	**Cobalt Strike** Censys Link	services.tls.certificates.leaf_data.issuer.common_name="Major Cobalt Strike"
5	**Cobalt Strike** Censys Link	services.tls.certificates.leaf_data.issuer.organization="cobaltstrike "
6	**Cobalt Strike** Censys Link	services.tls.certificates.leaf_data.issuer.organizational_unit="AdvancedPenTesting"
7	**Cobalt Strike** Censys Link	services.tls.certificates.leaf_data.subject.province="Cyberspace" and services.tls.certificates.leaf_data.subject.country="Earth"
8	**Quasar RAT** Censys Link	services.tls.certificates.leaf_data.subject.common_name: "Quasar Server CA"
9	**Laplas Clipper** Censys Link	services.tls.certificates.leaf_data.subject.common_name:"Laplas.app" or services.tls.certificates.leaf_data.issuer.common_name:"Laplas.app"
10	**Sliver C2** Censys Link	services:(tls.certificates.leaf_data.subject.common_name:multiplayer and tls.certificates.leaf_data.issuer.common_name:operators)
11	**Mythic C2** Censys Link	(services.http.response.html_title="Mythic") or services.http.response.favicons.md5_hash="6be63470c32ef458926abb198356006c" or services.tls.certificates.leaf_data.subject.common_name="Mythic"
12	**Remote Access Hosting MZ Files** Censys Link	labels: `remote-access` and services.http.response.body:"This program cannot be run in DOS mode"
13	**Possible Balada Malware** Censys Link	services:(http.response.body="404 Not Found" and port:443 and tls.certificates.leaf_data.subject.common_name="*.*.com" and tls.certificates.leaf_data.issuer.organization="Let's Encrypt" and not tls.certificates.leaf_data.subject.common_name="www.*.com" and http.response.headers: (key: `Server` and value.headers: `nginx`)) and services:(port:80 and http.response.headers: (key: `Server` and value.headers: `nginx`)) and not services.port:[1000 to 65000] and services.port:22 and not services.http.response.html_title:* and not dns.reverse_dns.names:* and dns.names:*.*.com

14	**NJRat/Xworm Botnet Servers** Censys Link	service_count:[200 to 2000] and dns.names:*.ngrok.* and services.banner:Gstreamer
15	**Redline Stealer C2** Censys Link	services.dns.server_type="FORWARDING" and dns.reverse_dns.names:*.ru and services.extended_service_name="VALVE" and service_count:3
16	**XTreme RAT** Censys Link	services.banner_hashes="sha256:22adaf058a2cb668b15cb4c1f30e7cc720bbe38c146544169db35fbf630389c4" and services.port:10001
17	**SuperShell BotNet** Censys Link	services.http.response.html_title:"Supershell" or services.http.response.favicons.md5_hash="cb183a53ebfc2b61b3968c9d4aa4b14a"

Based on the list of malware infrastructure queries, we extracted queries to examine the utilized attributes. The table below presents attributes that can be reviewed by Threat Hunters for escalation in determining search queries. The employed attributes encompass various types of value variations, including exact matches, numerical ranges, wildcards such as *.ru and *.id, and the use of Regex (available only for premium accounts).

No	Attribute	Description
1	autonomous_system.asn	Match
2	banner_hashes	Match
3	jarm.fingerprint	Match
4	labels	Match
5	service.banner_hashes	Match
6	service.tls.certificates.leaf_data.issuer_dn	Match
7	services.dns.server_type	Match
8	services.http.response.body	Match
9	services.http.response.body_hash	Match
10	services.http.response.favicons.md5_hash	Match
11	services.http.response.headers	Match
12	services.http.response.headers.content_disposition	Match
13	services.http.response.html_title	Match
14	services.port	Match
15	services.ssh.server_host_key.fingerprint_sha256	Match
16	services.tls.certificates.leaf_data.issuer.common_name	Match
17	services.tls.certificates.leaf_data.issuer.organization	Match

18	services.tls.certificates.leaf_data.issuer.organizational_unit	Match
19	services.tls.certificates.leaf_data.issuer_dn	Match
20	services.tls.certificates.leaf_data.subject.province	Match
21	services.tls.certificates.leaf_data.subject_dn	Match
22	services.tls.ja3s	Match
23	ssl.cert.issuer.cn	Match
24	ssl.cert.subject.cn	Match
25	tls.ja3s	Match
26	services.http.response.body_size	Range
27	service.tls.certificates.leaf_data.subject_dn	Match
28	services.tls.certificates.leaf_data.names	Match
29	dns.reverse_dns.names	Wildcard
30	services.tls.certificates.leaf_data.subject.common_name	Wildcard

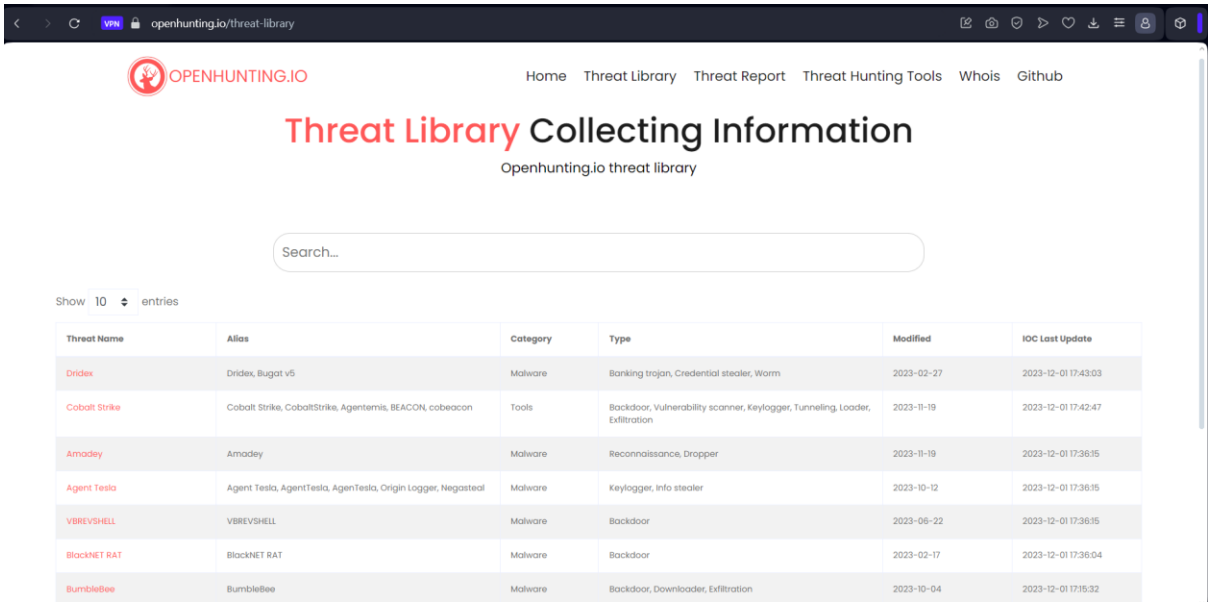
The provided attributes can assist analysts in identifying patterns of similarity within malware infrastructure.

CREATING MALWARE INFRASTRUCTURE QUERY SEARCH

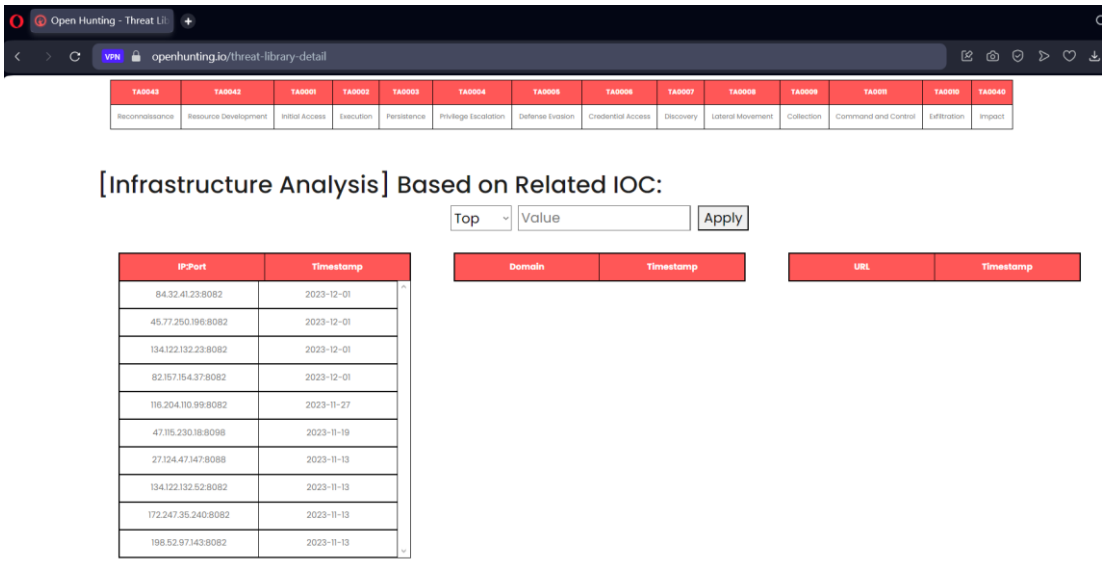
In this section, we will explain how to create a Search Query for exploring malware infrastructure. This aims to further enhance the reader's understanding of how the query search process can be conducted.

Exploring the Initial Vector

Numerous information sources can be utilized to search for the latest Malware IP Addresses. Readers can employ platforms such as Twitter, Threatfox, Threat Intelligence Reports, and other websites. We will utilize the Threat Library menu on Openhunting.io to acquire a Threat Name List with the latest IoC updates.



Next, we will conduct a search based on the Threat Name. For example, let's say we want to explore the Threat **VBREVSHELL**.



https://openhunting.io/threat-library-detail?data=vbrevshell

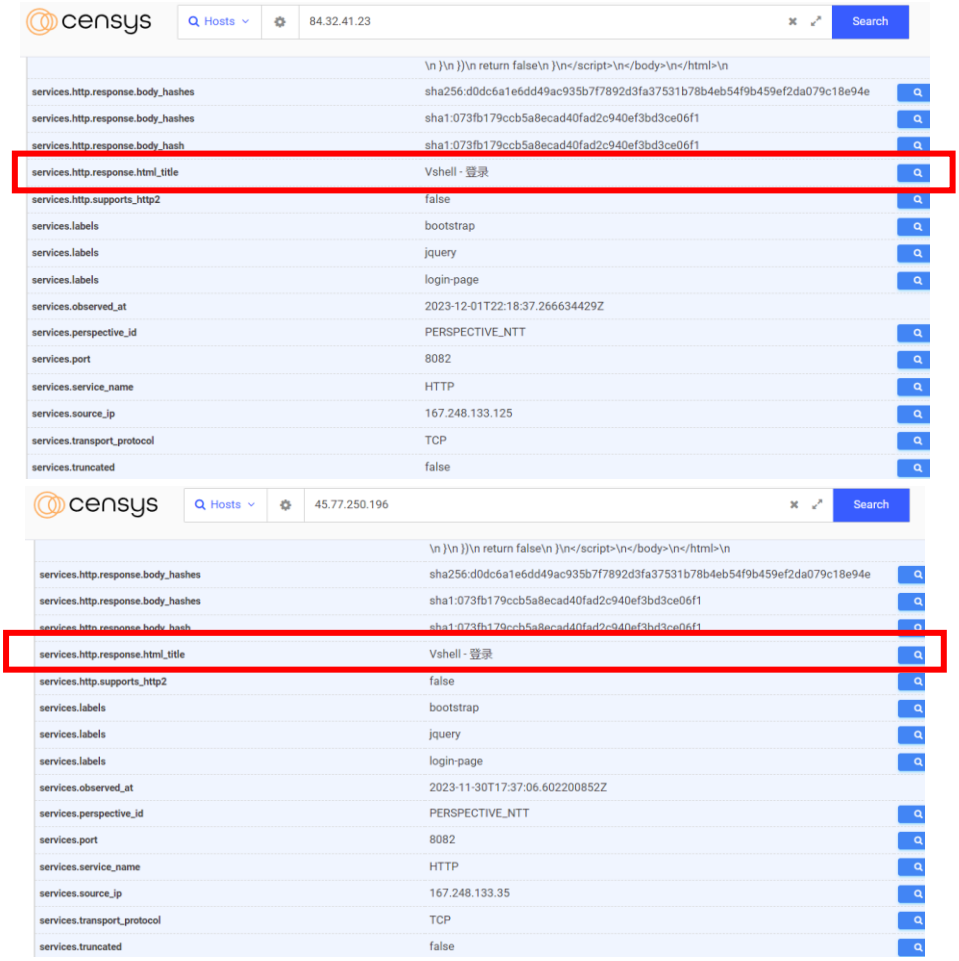
Based on the Infrastructure Analysis, 10 IP Addresses associated with the VBREVSHELL Threat were identified. Subsequently, two IP Addresses were sampled for further analysis:

84.32.41[.]23:8082

45.77.250[.]196:8082

Manual Analysis

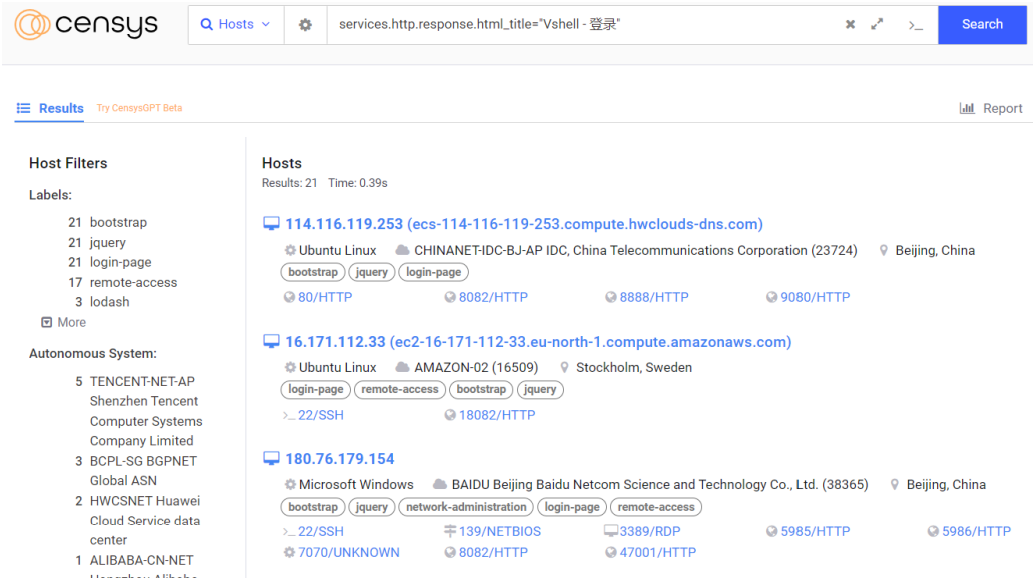
We then conducted a manual analysis based on the Attribute Table in the previous section for the sampled IP Addresses. In this stage, analysis is essential to compare the values obtained from the search results for two or more of the acquired IP addresses.



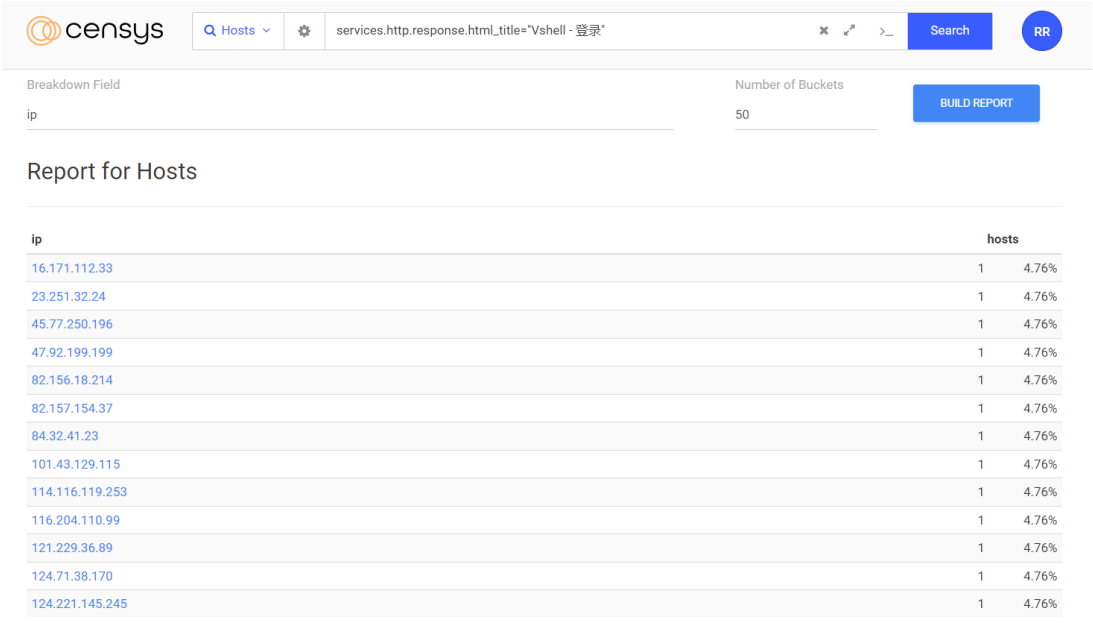
Test Query

Based on the search results, it was observed that there is an attribute with the same value, namely:

services.http.response.html_title="Vshell - 登录"

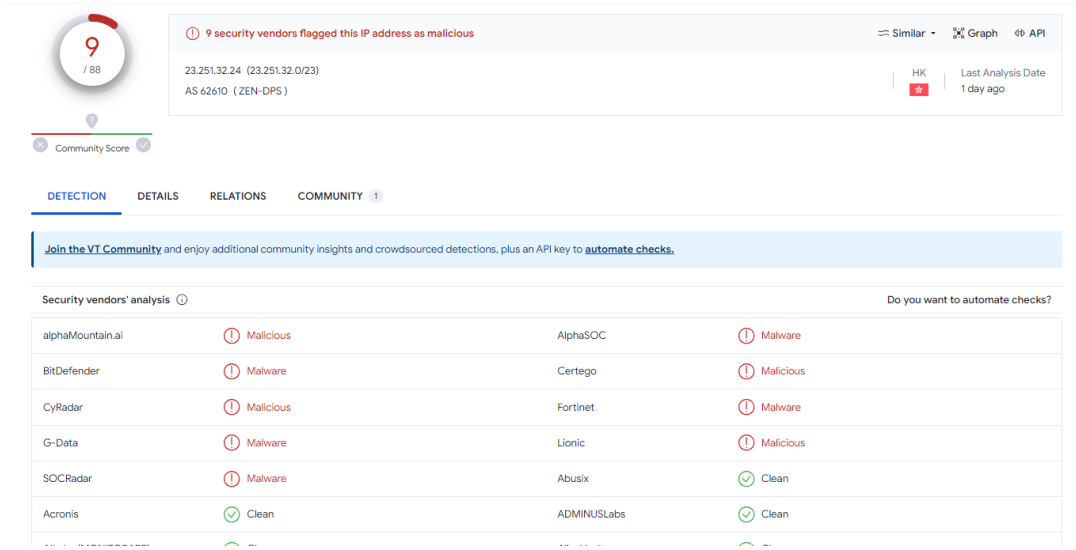


From the search results, it was determined that the keyword query produced results associated with 21 hosts. Following this, we extracted IP addresses using the Report feature.

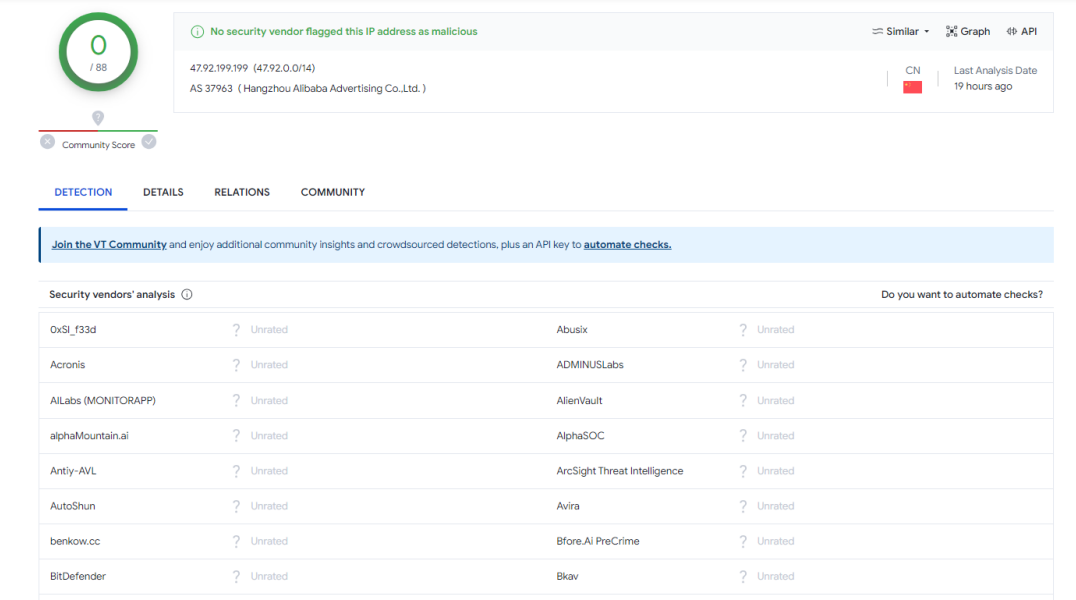


Validation Process

As part of the analysis process, we subsequently validated our findings to ensure the accuracy of the IP addresses obtained from the query. The IP address 23.251.32[.]24, in particular, has a reputation score of 9/88.



However, there are also IP addresses like 16.171.112[.]33 that have not been checked by VirusTotal.



The process of querying for malware infrastructure may potentially produce lists of IP addresses that could be false positives. To enhance protective measures, I recommend blocking those IP addresses within the Network Security Engineer's domain until it is confirmed that there is a legitimate need for users to access them.

MALWARE INFRASTRUCTURE SEARCH QUERY

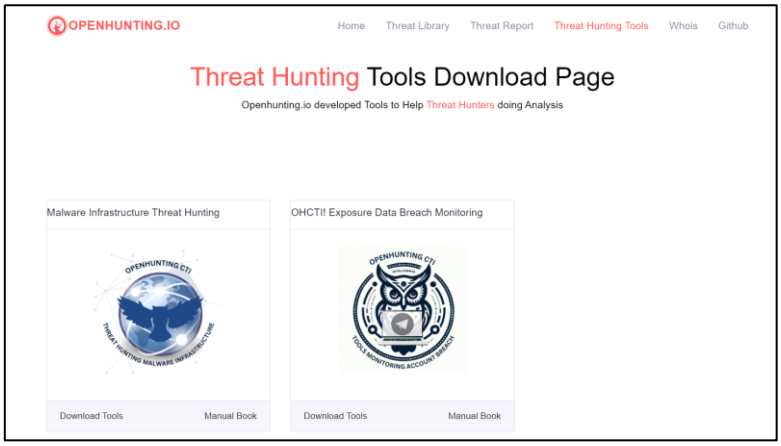
In this section, we will present the findings of our Search Query to update the existing queries. We aim to escalate the search results from the already established Query created by @Matthew read on the embee-research.ghost.io. This is intended to expand the sources of search queries available for Threat Hunting. Our search yielded a total of 15 additional Malware Search Queries. We hope that after reading this you will be able to create your search queries to retrieve IPs associated with malware and then share the results to community.

No	Malware	Query
1	**VBREVSHELL** Censys Link	services.http.response.html_title="Vshell - 登录"
2	**DarkCrystal RAT** Censys Link	services.tls.certificates.leaf_data.subject_dn="CN=DcRat*"
3	**NanoCore RAT** Censys Link	service_count:[200 to 2000] and dns.names:*.ngrok.* and services.banner="SSH-2.0-OpenSSH_7.4p1 Debian-10+deb9u7"
4	**DarkComet** Censys Link	(services.banner_hashes="sha256:adbb6e5879d006b5aa2b6f047ed00b7e38d87055cfc9a0f2274e77a25e1edfb0")
5	**PlugX** Censys Link	(services.banner="HTTP/1.1 404 Not Found\r\nAccept-Ranges: bytes\r\nContent-Type: text/html\r\nContent-Length: 80\r\nConnection: close\r\nCache: no-cache\r\nServer: Apache 1.3.27\r\n" and (services.port=`443` and services.port=`80` and services.port=`53`))
6	**Orcus RAT** Censys Link	services.tls.certificates.leaf_data.subject_dn:"CN=Orcus*"
7	**Mythic C2** Censys Link	services.tls.certificates.leaf_data.subject_dn:"O=Mythic*"
8	**Supershell** Censys Link	services.http.response.html_tags="<title>Supershell - 登录</title>"
9	**VenomRat (AsyncRAT)** Censys Link	services.tls.certificates.leaf_data.subject_dn:"CN=VenomRAT"
10	**Covenant** Censys Link	services.tls.certificates.leaf_data.subject_dn:"CN=Covenant"

11	**RisePro** **Censys Link**	services.banner="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"
12	**HookBot** **Censys Link**	services.http.response.html_tags="<title>HOOKBOT PANEL</title>"
13	**Viper RAT** **Censys Link**	(services.http.response.html_title="VIPER") and services.port=`60000`
14	**Havoc** **Censys Link**	services.banner="HTTP/1.1 404 Not Found\r\nContent-Type: text/html\r\nServer: nginx\r\nX-Havoc: true\r\nDate: <REDACTED>\r\nContent-Length: 146\r\n"
15	**ShadowPad** **Censys Link**	service_count:[10 to 20] and services.tls.certificates.leaf_data.subject_dn="C=CN, ST=myprovince, L=mycity, O=myorganization, OU=mygroup, CN=myCA"

EXTRACTION IOC FROM SEARCH QUERY

After discovering the Search Query as a pattern to find malware IP addresses, the next step is to perform automated extraction on the obtained IP addresses. Openhunting.io has provided a script for automated extraction on Censys based on the collected Search Queries; you can also add the Search Query results you find.



Source: https://openhunting.io/threat-tools

1. Get Repository

```
git clone https://github.com/openhunting-io/ohcti-malwareinfra.git
cd ohcti-malwareinfra
mv .env.example .env
```

2. Install Requirement

```
python3 -m pip install -r requirement.txt
```

3. Setting API Censys pada file **.env**

```
CENSYS_API_ID=YOUR_API_ID
CENSYS_API_SECRET=YOUR_API_SECRET
```

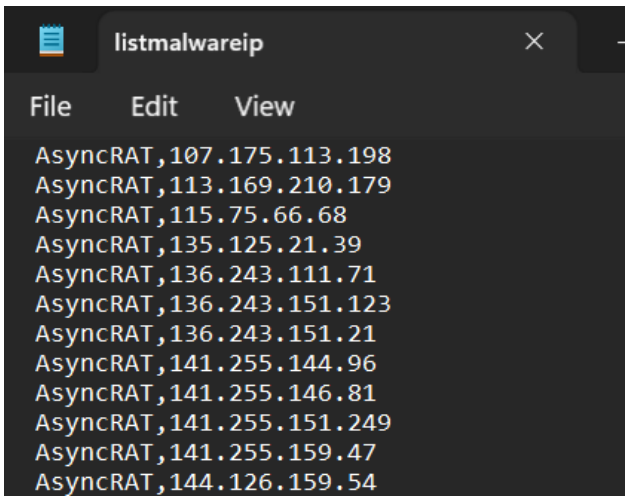
4. **(Optional)** Modify the source of your search queries.

```
{
    "threats": [
    {
        "name": "XTreme RAT",
        "search":
"services.banner_hashes=\"sha256:22adaf058a2cb668b15cb4c1f30e7cc72
0bbe38c146544169db35fbf630389c4\" and services.port:10001"
      },
      //insert your Search Query in Here
}
```

5. Running Threat Hunting Malware Infrastructure Script

```
python3 ohcti-malwareinfra.py
```

6. Get result in file **listmalwareip.txt**



APPENDIX 1

Malware Infrastructure Search Query Table

No	Malware	Query
1	**VBREVSHELL** Censys Link	services.http.response.html_title="Vshell - 登录"
2	**DarkCrystal RAT** Censys Link	services.tls.certificates.leaf_data.subject_dn="CN=DcRat*"
3	**NanoCore RAT** Censys Link	service_count:[200 to 2000] and dns.names:*.ngrok.* and services.banner="SSH-2.0-OpenSSH_7.4p1 Debian-10+deb9u7"
4	**DarkComet** Censys Link	(services.banner_hashes="sha256:adbb6e5879d006b5aa2b6f047ed00b7e38d87055cfc9a0f2274e77a25e1edfb0")
5	**PlugX** Censys Link	(services.banner="HTTP/1.1 404 Not Found\r\nAccept-Ranges: bytes\r\nContent-Type: text/html\r\nContent-Length: 80\r\nConnection: close\r\nCache: no-cache\r\nServer: Apache 1.3.27\r\n" and (services.port=`443` and services.port=`80` and services.port=`53`))
6	**Orcus RAT** Censys Link	services.tls.certificates.leaf_data.subject_dn:"CN=Orcus*"
7	**Mythic C2** Censys Link	services.tls.certificates.leaf_data.subject_dn:"O=Mythic*"
8	**Supershell** Censys Link	services.http.response.html_tags="<title>Supershell - 登录</title>"
9	**VenomRat (AsyncRAT)** Censys Link	services.tls.certificates.leaf_data.subject_dn:"CN=VenomRAT"
10	**Covenant** Censys Link	services.tls.certificates.leaf_data.subject_dn:"CN=Covenant"
11	**RisePro** Censys Link	services.banner="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"
12	**HookBot** Censys Link	services.http.response.html_tags="<title>HOOKBOT PANEL</title>"
13	**Viper RAT** Censys Link	(services.http.response.html_title="VIPER") and services.port=`60000`

14	**Havoc** Censys Link	services.banner="HTTP/1.1 404 Not Found\r\nContent-Type: text/html\r\nServer: nginx\r\nX-Havoc: true\r\nDate: <REDACTED>\r\nContent-Length: 146\r\n"
15	**ShadowPad** Censys Link	service_count:[10 to 20] and services.tls.certificates.leaf_data.subject_dn="C=CN, ST=myprovince, L=mycity, O=myorganization, OU=mygroup, CN=myCA"
16	**VBREVSHELL** Censys Link	services.http.response.html_title="Vshell - 登录"
17	**DarkCrystal RAT** Censys Link	services.tls.certificates.leaf_data.subject_dn="CN=DcRat*"
18	**NanoCore RAT** Censys Link	service_count:[200 to 2000] and dns.names:*.ngrok.* and services.banner="SSH-2.0-OpenSSH_7.4p1 Debian-10+deb9u7"
19	**DarkComet** Censys Link	(services.banner_hashes="sha256:adbb6e5879d006b5aa2b6f047ed00b7e38d87055cfc9a0f2274e77a25e1edfb0")
20	**PlugX** Censys Link	(services.banner="HTTP/1.1 404 Not Found\r\nAccept-Ranges: bytes\r\nContent-Type: text/html\r\nContent-Length: 80\r\nConnection: close\r\nCache: no-cache\r\nServer: Apache 1.3.27\r\n" and (services.port=`443` and services.port=`80` and services.port=`53`))
21	**Orcus RAT** Censys Link	services.tls.certificates.leaf_data.subject_dn:"CN=Orcus*"
22	**Mythic C2** Censys Link	services.tls.certificates.leaf_data.subject_dn:"O=Mythic*"
23	**Supershell** Censys Link	services.http.response.html_tags="<title>Supershell - 登录</title>"
24	**VenomRat (AsyncRAT)** Censys Link	services.tls.certificates.leaf_data.subject_dn:"CN=VenomRAT"
25	**Covenant** Censys Link	services.tls.certificates.leaf_data.subject_dn:"CN=Covenant"
26	**RisePro** Censys Link	services.banner="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"
27	**HookBot** Censys Link	services.http.response.html_tags="<title>HOOKBOT PANEL</title>"
28	**Viper RAT** Censys Link	(services.http.response.html_title="VIPER") and services.port=`60000`

29	**Havoc** **Censys Link**	services.banner="HTTP/1.1 404 Not Found\r\nContent-Type: text/html\r\nServer: nginx\r\nX-Havoc: true\r\nDate: <REDACTED>\r\nContent-Length: 146\r\n"
30	**ShadowPad** **Censys Link**	service_count:[10 to 20] and services.tls.certificates.leaf_data.subject_dn="C=CN, ST=myprovince, L=mycity, O=myorganization, OU=mygroup, CN=myCA"

REFERENCE

https://embee-research.ghost.io/shodan-censys-queries/
https://openhunting.io/threat-library
https://search.censys.io/

OPENHUNTING.IO

Project To Make Threat Hunting and Intelligence Information &

Tools Available for Every One.