



THREAT HUNTING MALWARE INFRASTRUCTURE

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

<https://t.me/learningnets>

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.....	2
INFRASTRUCTURE ANALYSIS WITH SEARCH ENGINE	2
EXAMPLE QUERY FOR ATTRIBUTE INFORMATION.....	5
CREATING MALWARE INFRASTRUCTURE QUERY SEARCH	8
MALWARE INFRASTRUCTURE SEARCH QUERY	13
EXTRACTION IOC FROM SEARCH QUERY	14
APPENDIX 1.....	16
REFERENCE	19



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**.

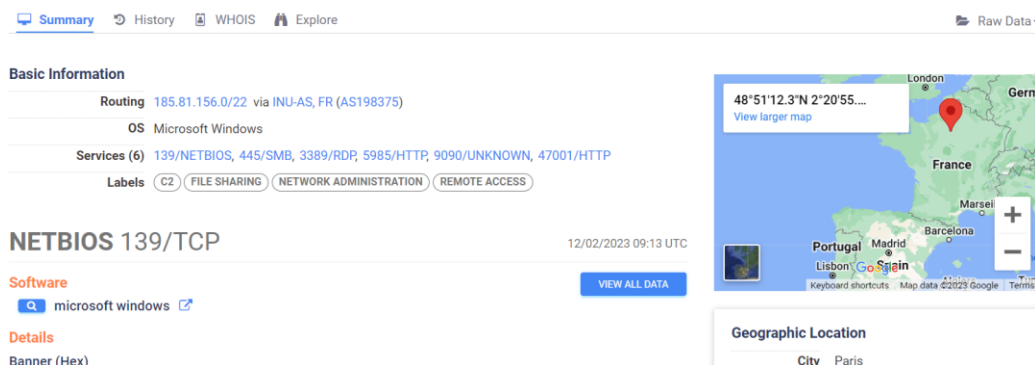
AsyncRAT malware identified Indicators of Compromise (IoC) linked to the C2 IP of the malware through an analysis of the IP 185.81.157[.]218. In practice, acquiring the C2 IP of malware can be accomplished through diverse methods, including Malware Sample Analysis, Twitter, Threat Intelligence Reports,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



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

185.81.157.218

As of: Dec 02, 2023 11:46am UTC | Latest



Basic Information

- Routing: 185.81.156.0/22 via INU-AS, FR (AS198375)
- OS: Microsoft Windows
- Services (6): 139/NETBIOS, 445/SMB, 3389/RDP, 5985/HTTP, 9090/UNKNOWN, 47001/HTTP
- Labels: C2, FILE SHARING, NETWORK ADMINISTRATION, REMOTE ACCESS

NETBIOS 139/TCP 12/02/2023 09:13 UTC

Software

- microsoft windows

Geographic Location

City: Paris

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

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

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**.

Host Filters

Labels:

- 119 c2
- 97 remote-access
- 95 network-administration
- 89 file-sharing
- 19 open-dir
- More

Autonomous System:

- 18 INU-AS
- 13 OVH
- 9 IELO IELO Main Network
- 6 HOSTWINDS
- 6 NL-811-40021
- More

Location:

- 37 United States
- 25 France
- 16 Netherlands
- 9 Germany
- 6 United Kingdom
- More

Hosts

Results: 119 Time: 0.15s

77.232.132.25 (1609545-cd80446.twc1.net)

- Microsoft Windows TIMEWEB-AS (9123) St.-Petersburg, Russia
- remote-access c2 network-administration
- 3389/RDP 5001/UNKNOWN 5985/HTTP

141.255.144.96

- IELO IELO Main Network (29075) Occitanie, France
- c2
- 8888/UNKNOWN

51.20.70.15 (ec2-51-20-70-15.eu-north-1.compute.amazonaws.com)

- Microsoft Windows AMAZON-02 (16509) Stockholm, Sweden
- remote-access file-sharing c2 network-administration
- 139/NETBIOS 445/SMB 3389/RDP 4443/UNKNOWN 5985/HTTP
- 47001/HTTP

185.62.86.134

- Microsoft Windows THINKSYSTEMSUK-ASN (51159) England, United Kingdom
- remote-access network-administration c2 file-sharing

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

10 / 88

10 security vendors flagged this IP address as malicious

77.232.132.25 (77.232.128.0/21)
AS 9123 (TimeWeb Ltd.)

RU Last Analysis Date 3 days ago

Community Score

DETECTION DETAILS RELATIONS COMMUNITY 1

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

Crowdsourced context

HIGH 0 MEDIUM 1 LOW 0 INFO 0 SUCCESS 0

ThreatFox IOCs for 2023-08-10 - according to source ArcSight Threat Intelligence - 3 months ago
↳ AsyncRAT botnet C2 server (confidence level: 100%)

Security vendors' analysis

Vendor	Detection	Category	Confidence
AlphaSOC	Malware	Anti-AVL	Malicious
BitDefender	Malware	Certego	Malicious
CyRadar	Malicious	Fortinet	Malware

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 = "c655bae831ca57a857b26d76a7c98a56a65d00fdab7d234a64addf 8166e3cd09" 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](https://openhunting.io) to acquire a Threat Name List with the latest IoC updates.



The screenshot shows the OpenHunting.io Threat Library interface. At the top, there is a navigation bar with links for Home, Threat Library, Threat Report, Threat Hunting Tools, Whois, and Github. The main heading is "Threat Library Collecting Information" with the subtitle "Openhunting.io threat library". Below this is a search bar and a "Show 10 entries" dropdown. The main content is a table listing various threats.

Threat Name	Alias	Category	Type	Modified	IOC Last Update
Dridex	Dridex, Bugat v5	Malware	Banking trojan, Credential stealer, Worm	2023-02-27	2023-12-01 17:43:03
Cobalt Strike	Cobalt Strike, CobaltStrike, Agentemis, BEACON, cobbeacon	Tools	Backdoor, Vulnerability scanner, Keylogger, Tunneling, Loader, Exfiltration	2023-11-19	2023-12-01 17:42:47
Amadey	Amadey	Malware	Reconnaissance, Dropper	2023-11-19	2023-12-01 17:36:15
Agent Tesla	Agent Tesla, AgentTesla, AgenTesla, Origin Logger, Negastcal	Malware	Keylogger, Info stealer	2023-10-12	2023-12-01 17:36:15
VBREVSHELL	VBREVSHELL	Malware	Backdoor	2023-06-22	2023-12-01 17:36:15
BlackNET RAT	BlackNET RAT	Malware	Backdoor	2023-02-17	2023-12-01 17:36:04
BumbleBee	BumbleBee	Malware	Backdoor, Downloader, Exfiltration	2023-10-04	2023-12-01 17:15:32

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

The screenshot shows the detail page for the VBREVSHELL threat. At the top, there is a navigation bar with links for various threat categories: TA0043, TA0042, TA0001, TA0002, TA0003, TA0004, TA0005, TA0006, TA0007, TA0008, TA0009, TA0010, TA0011, TA0012, TA0013, and TA0014. Below this is a table with 14 columns representing different threat categories and their descriptions.

TA0043	TA0042	TA0001	TA0002	TA0003	TA0004	TA0005	TA0006	TA0007	TA0008	TA0009	TA0010	TA0011	TA0012	TA0013	TA0014
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact		

[Infrastructure Analysis] Based on Related IOC:

The screenshot shows the Infrastructure Analysis section for the VBREVSHELL threat. It includes a dropdown menu set to "Top" and a search bar with the value "Value". Below this is a table with two columns: "IP:Port" and "Timestamp".

IP:Port	Timestamp
84.32.41.23:8082	2023-12-01
45.77.250.196:8082	2023-12-01
134.122.132.23:8082	2023-12-01
82.167.164.37:8082	2023-12-01
116.204.110.99:8082	2023-11-27
47.115.230.18:8098	2023-11-19
27.124.47.147:8088	2023-11-13
134.122.132.52:8082	2023-11-13
172.247.35.240:8082	2023-11-13
198.52.97.143:8082	2023-11-13

<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.

The image displays two screenshots of the Censys Hosts interface, showing attribute tables for two different IP addresses. The first screenshot is for IP 84.32.41.23, and the second is for IP 45.77.250.196. Both tables list various attributes and their values. The attribute 'services.http.response.html_title' is highlighted with a red box in both screenshots, showing the value 'Vshell - 登录'.

Attribute	Value
services.http.response.body_hashes	sha256:d0dc6a1e6dd49ac935b7f7892d3fa37531b78b4eb54f9b459ef2da079c18e94e
services.http.response.body_hashes	sha1:073fb179ccb5a8ecad40fad2c940ef3bd3ce06f1
services.http.response.body_hash	sha1:073fb179ccb5a8ecad40fad2c940ef3bd3ce06f1
services.http.response.html_title	Vshell - 登录
services.http.supports_http2	false
services.labels	bootstrap
services.labels	jquery
services.labels	login-page
services.observed_at	2023-12-01T22:18:37.266634429Z
services.perspective_id	PERSPECTIVE_NTT
services.port	8082
services.service_name	HTTP
services.source_ip	167.248.133.125
services.transport_protocol	TCP
services.truncated	false

Attribute	Value
services.http.response.body_hashes	sha256:d0dc6a1e6dd49ac935b7f7892d3fa37531b78b4eb54f9b459ef2da079c18e94e
services.http.response.body_hashes	sha1:073fb179ccb5a8ecad40fad2c940ef3bd3ce06f1
services.http.response.body_hash	sha1:073fb179ccb5a8ecad40fad2c940ef3bd3ce06f1
services.http.response.html_title	Vshell - 登录
services.http.supports_http2	false
services.labels	bootstrap
services.labels	jquery
services.labels	login-page
services.observed_at	2023-11-30T17:37:06.602200852Z
services.perspective_id	PERSPECTIVE_NTT
services.port	8082
services.service_name	HTTP
services.source_ip	167.248.133.35
services.transport_protocol	TCP
services.truncated	false

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"



Host Filters

Labels:

- 21 bootstrap
- 21 jquery
- 21 login-page
- 17 remote-access
- 3 lodash
- More

Autonomous System:

- 5 TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited
- 3 BCPL-SG BGPNET Global ASN
- 2 HWCSNET Huawei Cloud Service data center
- 1 ALIBABA-CN-NET

Hosts
Results: 21 Time: 0.39s

114.116.119.253 (ecs-114-116-119-253.compute.hwclouds-dns.com)
 Ubuntu Linux CHINANET-IDC-BJ-AP IDC, China Telecommunications Corporation (23724) Beijing, China
 bootstrap jquery login-page
 80/HTTP 8082/HTTP 8888/HTTP 9080/HTTP

16.171.112.33 (ec2-16-171-112-33.eu-north-1.compute.amazonaws.com)
 Ubuntu Linux AMAZON-02 (16509) Stockholm, Sweden
 login-page remote-access bootstrap jquery
 22/SSH 18082/HTTP

180.76.179.154
 Microsoft Windows BAIDU Beijing Baidu Netcom Science and Technology Co., Ltd. (38365) Beijing, China
 bootstrap jquery network-administration login-page remote-access
 22/SSH 139/NETBIOS 3389/RDP 5985/HTTP 5986/HTTP
 7070/UNKNOWN 8082/HTTP 47001/HTTP

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.

Breakdown Field: ip Number of Buckets: 50 BUILD REPORT

Report for Hosts

ip	hosts
16.171.112.33	1 4.76%
23.251.32.24	1 4.76%
45.77.250.196	1 4.76%
47.92.199.199	1 4.76%
82.156.18.214	1 4.76%
82.157.154.37	1 4.76%
84.32.41.23	1 4.76%
101.43.129.115	1 4.76%
114.116.119.253	1 4.76%
116.204.110.99	1 4.76%
121.229.36.89	1 4.76%
124.71.38.170	1 4.76%
124.221.145.245	1 4.76%

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.



9 security vendors flagged this IP address as malicious

23.251.32.24 (23.251.32.0/23)
AS 62610 (ZEN-DPS)

Similar Graph API

HK Last Analysis Date 1 day ago

Community Score

DETECTION DETAILS RELATIONS COMMUNITY 1

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

Security vendors' analysis Do you want to automate checks?

alphaMountain.ai	Malicious	AlphaSOC	Malware
BitDefender	Malware	Certego	Malicious
CyRadAr	Malicious	Fortinet	Malware
G-Data	Malware	Lionic	Malicious
SOCRadAr	Malware	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean

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

No security vendor flagged this IP address as malicious

47.92.199.199 (47.92.0.0/14)
AS 37963 (Hangzhou Alibaba Advertising Co.,Ltd.)

Similar Graph API

CN Last Analysis Date 19 hours ago

Community Score

DETECTION DETAILS RELATIONS COMMUNITY

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

Security vendors' analysis Do you want to automate checks?

0xSI_f33d	Unrated	Abusix	Unrated
Acronis	Unrated	ADMINUSLabs	Unrated
AllLabs (MONITORAPP)	Unrated	AlienVault	Unrated
alphaMountain.ai	Unrated	AlphaSOC	Unrated
Antiy-AVL	Unrated	ArcSight Threat Intelligence	Unrated
AutoShun	Unrated	Avira	Unrated
benkow.cc	Unrated	Bfore.AI PreCrime	Unrated
BitDefender	Unrated	Bkav	Unrated

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.

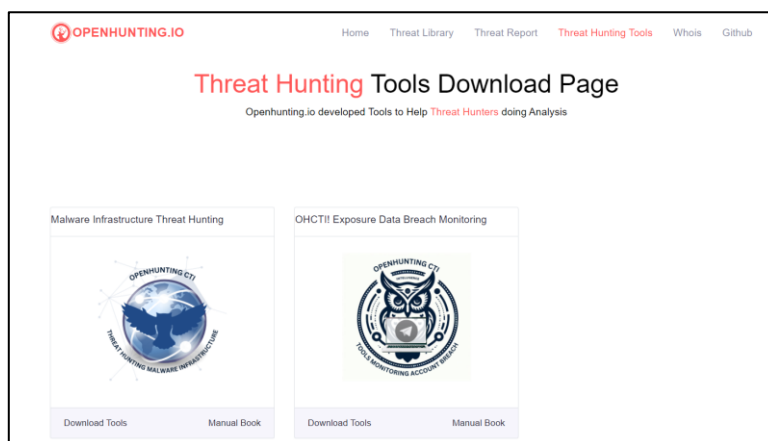
No	Malware	Query
1	VBREVSHELL Censys Link	services.http.response.html_title="Vshell - 登录"
2	DarkCrystal RAT Censys Link	services.tls.certificates.leaf_data.subject_dn="CN=DcRat*"
3	NanoCore RAT Censys Link	service_count:[200 to 2000] and dns.names:*.ngrok.* and services.banner="SSH-2.0-OpenSSH_7.4p1 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
```

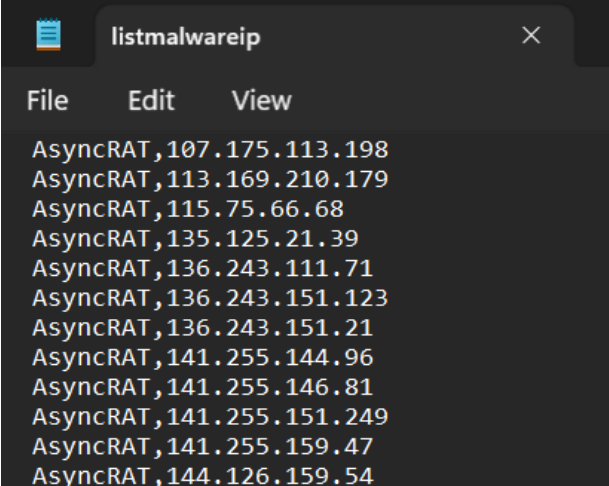
4. (Optional) Modify the source of your search queries.

```
{  
  "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



```
listmalwareip  
File Edit View  
AsyncRAT,107.175.113.198  
AsyncRAT,113.169.210.179  
AsyncRAT,115.75.66.68  
AsyncRAT,135.125.21.39  
AsyncRAT,136.243.111.71  
AsyncRAT,136.243.151.123  
AsyncRAT,136.243.151.21  
AsyncRAT,141.255.144.96  
AsyncRAT,141.255.146.81  
AsyncRAT,141.255.151.249  
AsyncRAT,141.255.159.47  
AsyncRAT,144.126.159.54
```



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.

