Lab 2: Exploratory Data Analysis of IP

Elaborated by:
Leandro Delgado
114416241

Tatiana Outkina
CYT-250/Threat Investigation

CYT250 Lab2. Exploratory Data Analysis of IP – 4%

Part 1. Read the Chapter 4 materials and answer the following questions – 2%

Scope of reading: Chapter 4, Section "Dissecting the IP address" (Representing IP Addresses, Converting IP Addresses to/from, Segmenting and Grouping IP Addresses, Testing IPv4 Address Membership in a CIDR block, Locating IP Addresses).

The questions:

1. **Why would you need to convert dotted-decimal presentation of IP address to integer form?**
   According to the text, by doing the conversion of an IP address helps to make the comparisons and calculation easier. For example, if I need to check the two ip address belong to a common range, it is much easier and faster to specify the number of range than must deal with the dotted decimal number. It allows to get the calculations much faster and simplex.
2. **Why would you need to do segmenting, or grouping, of IP addresses?**
   Because helps to organize Ip address, especially in larger networks. The grouping could have server at one place and users' devices at another. As a result, it makes easier to manage traffic and improve security and routing. So, that information travels safely and efficiently through the network.
3. **Explain CIDR prefix format.**
   It is called classless Interdomain Routing, that means of expressing IP address. It shows how many bites are being utilized for the Address network part. For example, if I consider an IP address 192.168.1.0/24 denotes that the first 24 bits are representing the network while the second part are used for individual devices. In fact, CIDR, allows for much flexibility than the previous model of dividing addresses into a hard-set class for usage allowing to get more efficient use of those IP addresses.
4. **Explain what is AS and ASN. How it can be useful for segmenting or grouping task?**
   Autonomous System (AS), consisting of a group of IP networks and routers that are under the control of a single entity. Autonomous system Number (ASN), is a unique identifier assigned to each AS. In fact, they are used while grouping Ip address, which allows for their organization and management on the basic of ownership or hierarchal control. For example, if I consider the identification of malicious traffic originating from a certain Autonomous System (SA) can assist in the network security as it can be indicative of corrupt systems or overall problem network.
5. **Play with https://www.maxmind.com/en/home. Describe the value of the services and data provided (you are not supposed to buy anything there, just go through description)**

According to the web MaxMind, it provides a range of services that can support businesses to improve their security and customer experience. Between the services mentioned are:

1. **Fraud Prevention:** It can help you spot and stop fraudulent activity in real time if you are running online services. Also, they provide risk scores that help you identify potentially suspicious transactions, saving you from dealing with fraudulent orders.
2. **IP Geolocation:** if any business is looking to personalize their website experience for visitors, it is the best option. With IP geolocation, you can serve content based on the user's location, whether it's showing region-specific offers, ads, or ensuring you're compliant with local laws.
3. **Proxy Detection:** it detects if someone is hiding their real IP behind a VPN or proxy. This is important for businesses that want to make sure only legitimate users are accessing their services.

Part 2. Implement the following Use Case – 2%

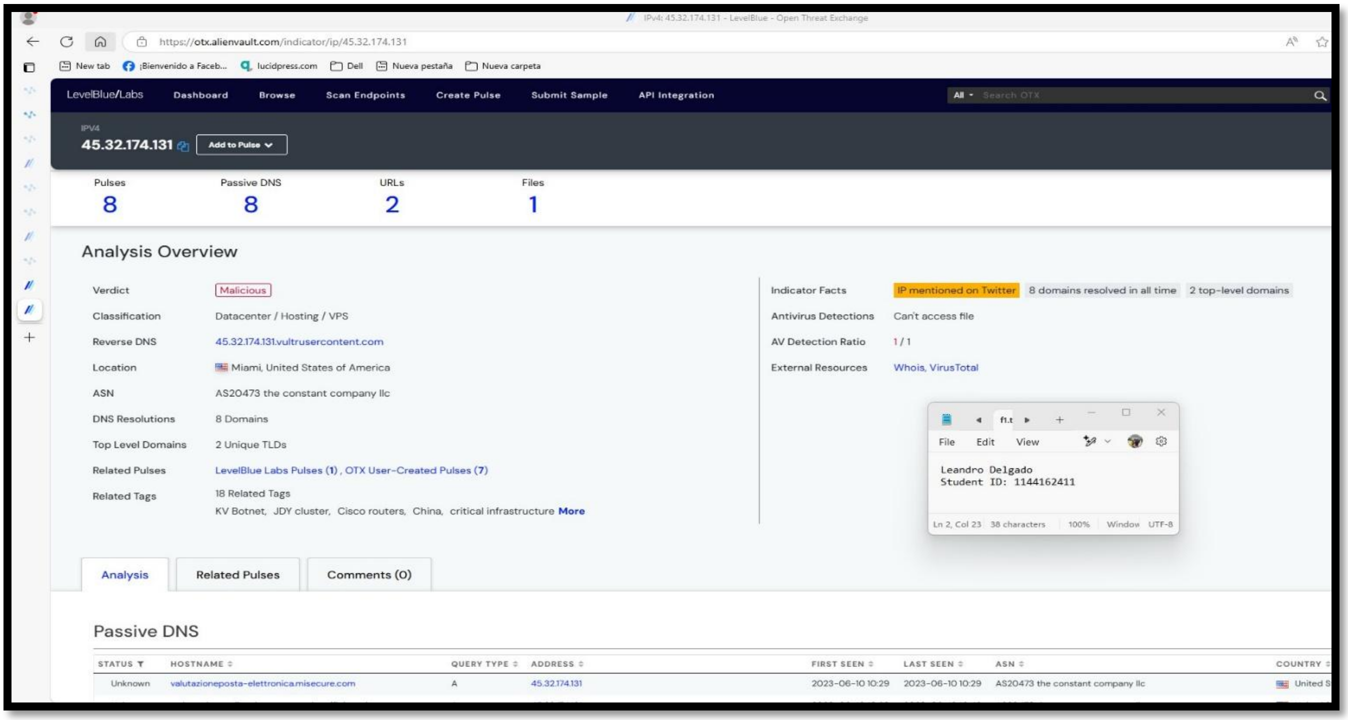
You are a security analyst of the AAA company, and you are given the task of investigating a group of IP addresses.

Your actions:

Step1. Connect to AlienVault site and retrieve network indicators:

https://otx.alienvault.com/pulse/678a92bdb1203066894a3c50?utm_userid=tato12344&utm_medium=InProduct&utm_source=OTX&utm_content=Email&utm_campaign=new_pulse_from_following

a) Is this IP address malicious? YE



IPV4
45.32.174.131

Pulses	Passive DNS	URLs	Files
8	8	2	1

Analysis Overview

Verdict	Malicious
Classification	Datacenter / Hosting / VPS
Reverse DNS	45.32.174.131.vultrusercontent.com
Location	Miami, United States of America
ASN	AS20473 the constant company llc
DNS Resolutions	8 Domains
Top Level Domains	2 Unique TLDs
Related Pulses	LevelBlue Labs Pulses (1) , OTX User-Created Pulses (7)
Related Tags	18 Related Tags KV Botnet, JDY cluster, Cisco routers, China, critical infrastructure More

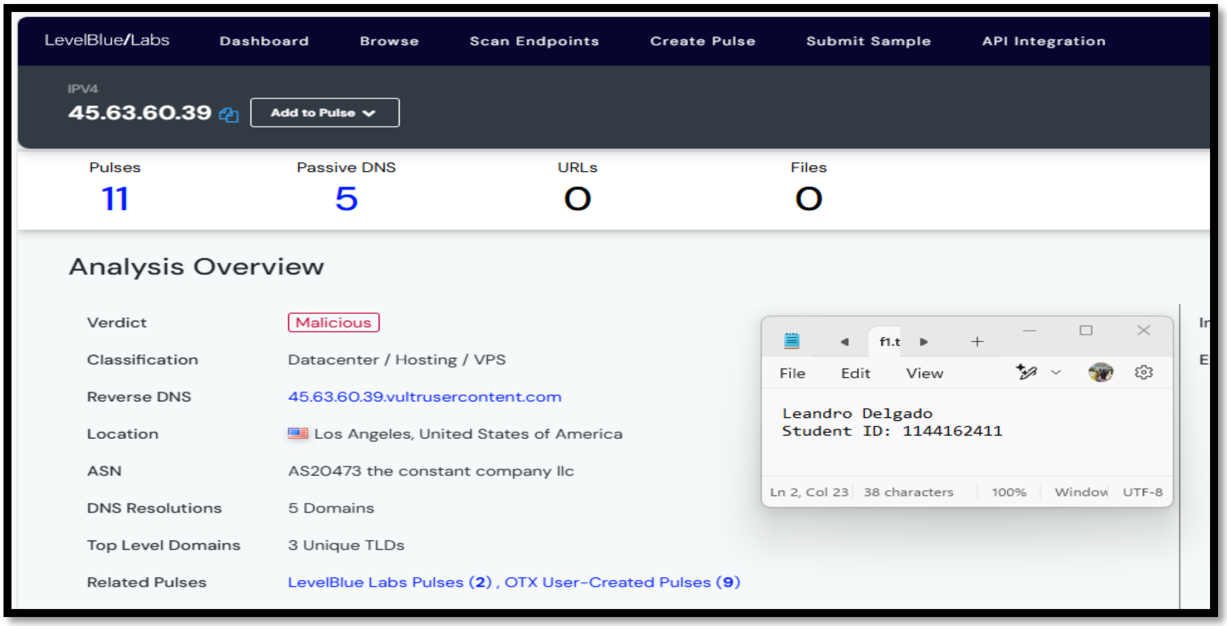
Indicator Facts	IP mentioned on Twitter · 8 domains resolved in all time · 2 top-level domains
Antivirus Detections	Can't access file
AV Detection Ratio	1 / 1
External Resources	Whois, VirusTotal

```
Leandro Delgado
Student ID: 1144162411
```

Passive DNS

STATUS	HOSTNAME	QUERY TYPE	ADDRESS	FIRST SEEN	LAST SEEN	ASN	COUNTRY
Unknown	valutazioneposta-elettronica.misecure.com	A	45.32.174.131	2023-06-10 10:29	2023-06-10 10:29	AS20473 the constant company llc	United S

b) What company does it belong to?
AS20473 the constant company llc



IPV4
45.63.60.39

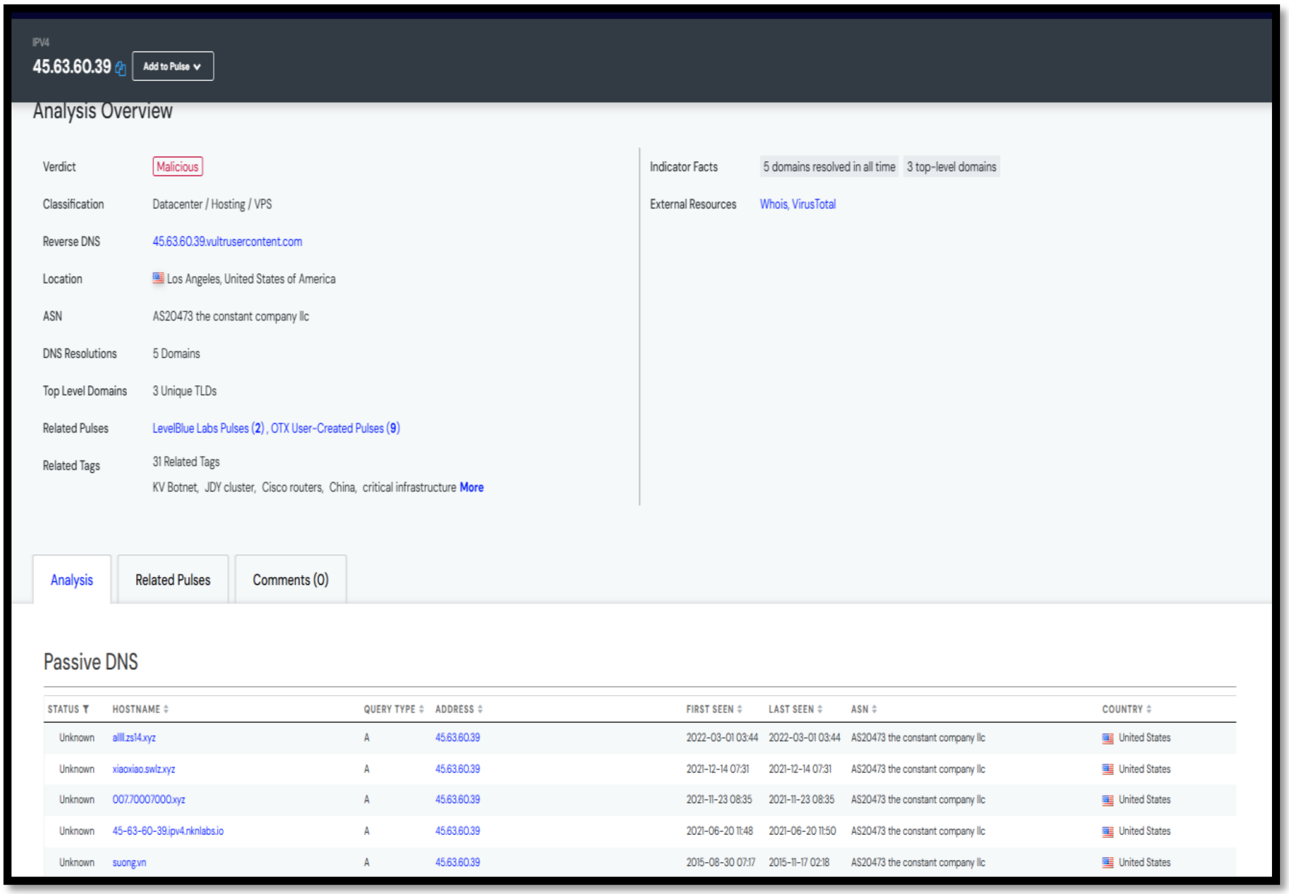
Pulses	Passive DNS	URLs	Files
11	5	0	0

Analysis Overview

Verdict	Malicious
Classification	Datacenter / Hosting / VPS
Reverse DNS	45.63.60.39.vultrusercontent.com
Location	Los Angeles, United States of America
ASN	AS20473 the constant company llc
DNS Resolutions	5 Domains
Top Level Domains	3 Unique TLDs
Related Pulses	LevelBlue Labs Pulses (2) , OTX User-Created Pulses (9)

Leandro Delgado
Student ID: 1144162411

c) Is it a part of an Autonomous System (AS) group of IP addresses? YES



IPV4
45.63.60.39

Analysis Overview

Verdict	Malicious
Classification	Datacenter / Hosting / VPS
Reverse DNS	45.63.60.39.vultrusercontent.com
Location	Los Angeles, United States of America
ASN	AS20473 the constant company llc
DNS Resolutions	5 Domains
Top Level Domains	3 Unique TLDs
Related Pulses	LevelBlue Labs Pulses (2) , OTX User-Created Pulses (9)
Related Tags	31 Related Tags KV Botnet, JDY cluster, Cisco routers, China, critical infrastructure More

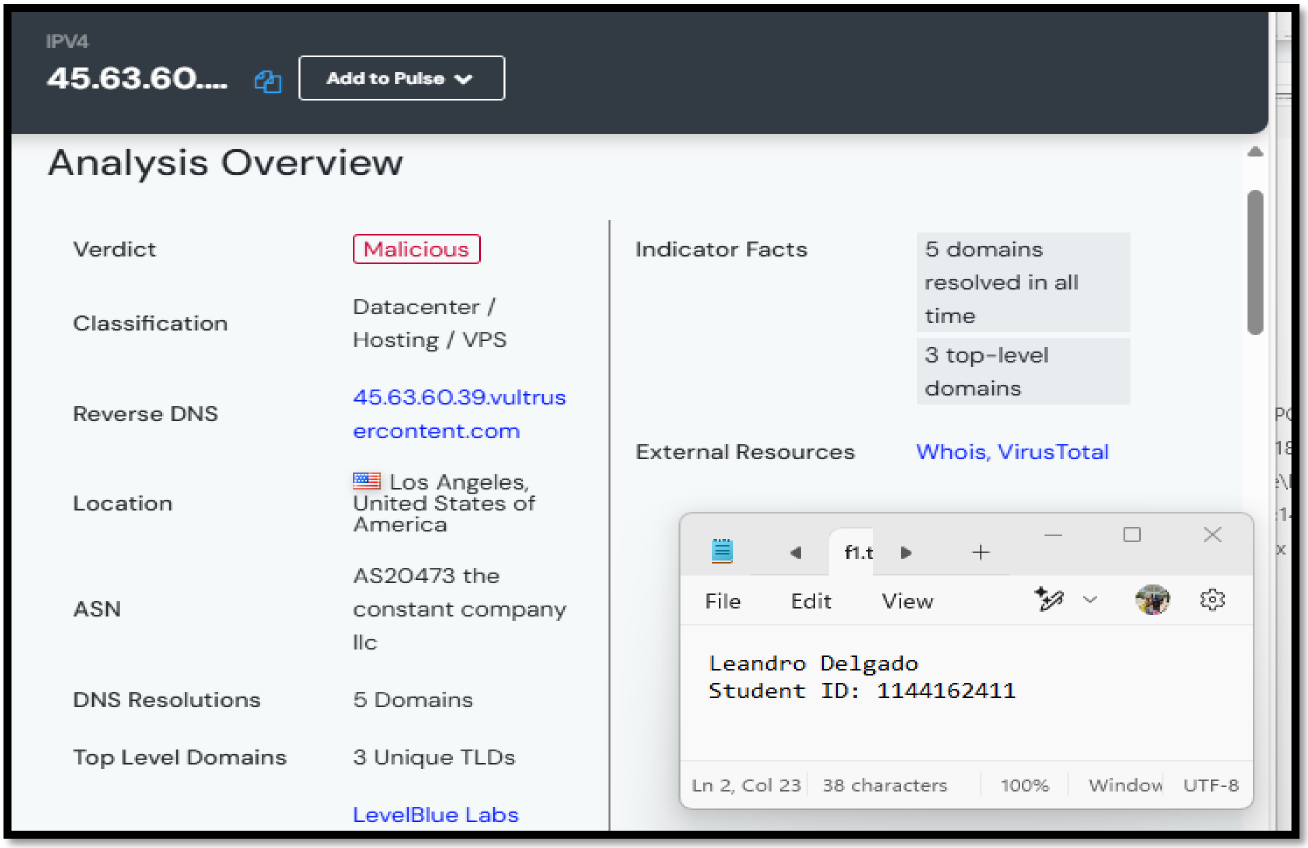
Indicator Facts	5 domains resolved in all time 3 top-level domains
External Resources	Whois, VirusTotal

Passive DNS

STATUS	HOSTNAME	QUERY TYPE	ADDRESS	FIRST SEEN	LAST SEEN	ASN	COUNTRY
Unknown	alll.zs14.xyz	A	45.63.60.39	2022-03-01 03:44	2022-03-01 03:44	AS20473 the constant company llc	United States
Unknown	xiaoxiao.swlz.xyz	A	45.63.60.39	2021-12-14 07:31	2021-12-14 07:31	AS20473 the constant company llc	United States
Unknown	007.70007000.xyz	A	45.63.60.39	2021-11-23 08:35	2021-11-23 08:35	AS20473 the constant company llc	United States
Unknown	45-63-60-39.ipv4.nknlabs.io	A	45.63.60.39	2021-06-20 11:48	2021-06-20 11:50	AS20473 the constant company llc	United States
Unknown	suong.vn	A	45.63.60.39	2015-08-30 07:17	2015-11-17 02:18	AS20473 the constant company llc	United States

d) What is its ASN?

AS20473 the constant company llc



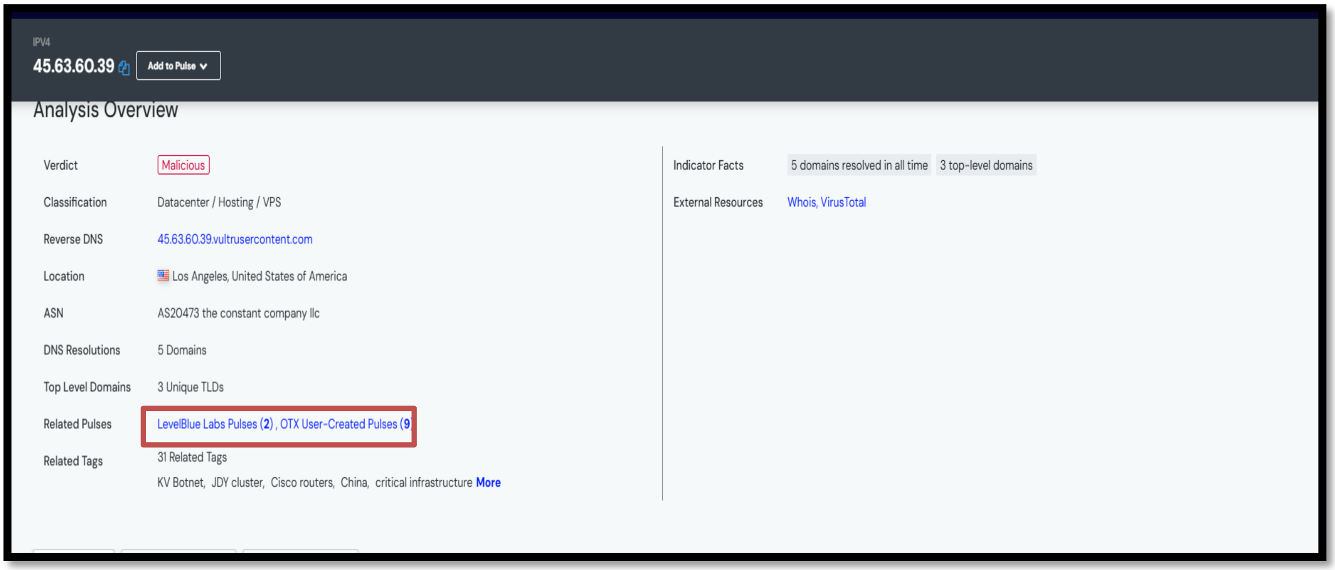
Analysis Overview

Verdict	Malicious
Classification	Datacenter / Hosting / VPS
Reverse DNS	45.63.60.39.vultrusercontent.com
Location	Los Angeles, United States of America
ASN	AS20473 the constant company llc
DNS Resolutions	5 Domains
Top Level Domains	3 Unique TLDs
	LevelBlue Labs

Indicator Facts	5 domains resolved in all time 3 top-level domains
External Resources	Whois, VirusTotal

Leandro Delgado
Student ID: 1144162411

e) What is potential danger associated with this AS?

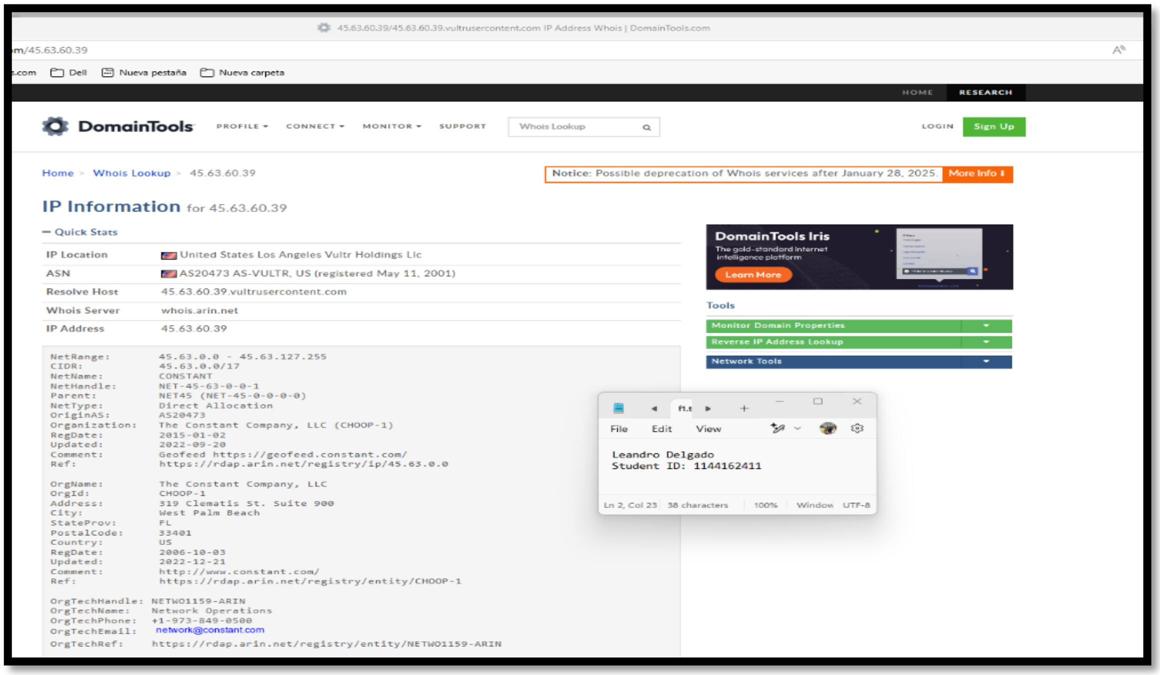


Analysis Overview

Verdict	Malicious
Classification	Datacenter / Hosting / VPS
Reverse DNS	45.63.60.39.vultrusercontent.com
Location	Los Angeles, United States of America
ASN	AS20473 the constant company llc
DNS Resolutions	5 Domains
Top Level Domains	3 Unique TLDs
Related Pulses	LevelBlue Labs Pulses (2) , OTX User-Created Pulses (9
Related Tags	31 Related Tags KV Botnet, JDY cluster, Cisco routers, China, critical infrastructure More

Indicator Facts	5 domains resolved in all time 3 top-level domains
External Resources	Whois, VirusTotal

f) You see the links to other sources of information (Whois, VirusTotal). What other sources of information say about this IP?



IP Information for 45.63.60.39

IP Location	United States Los Angeles Vultr Holdings Llc
ASN	AS20473 AS-VULTR, US (registered May 11, 2001)
Resolve Host	45.63.60.39.vultrusercontent.com
Whois Server	whois.arin.net
IP Address	45.63.60.39

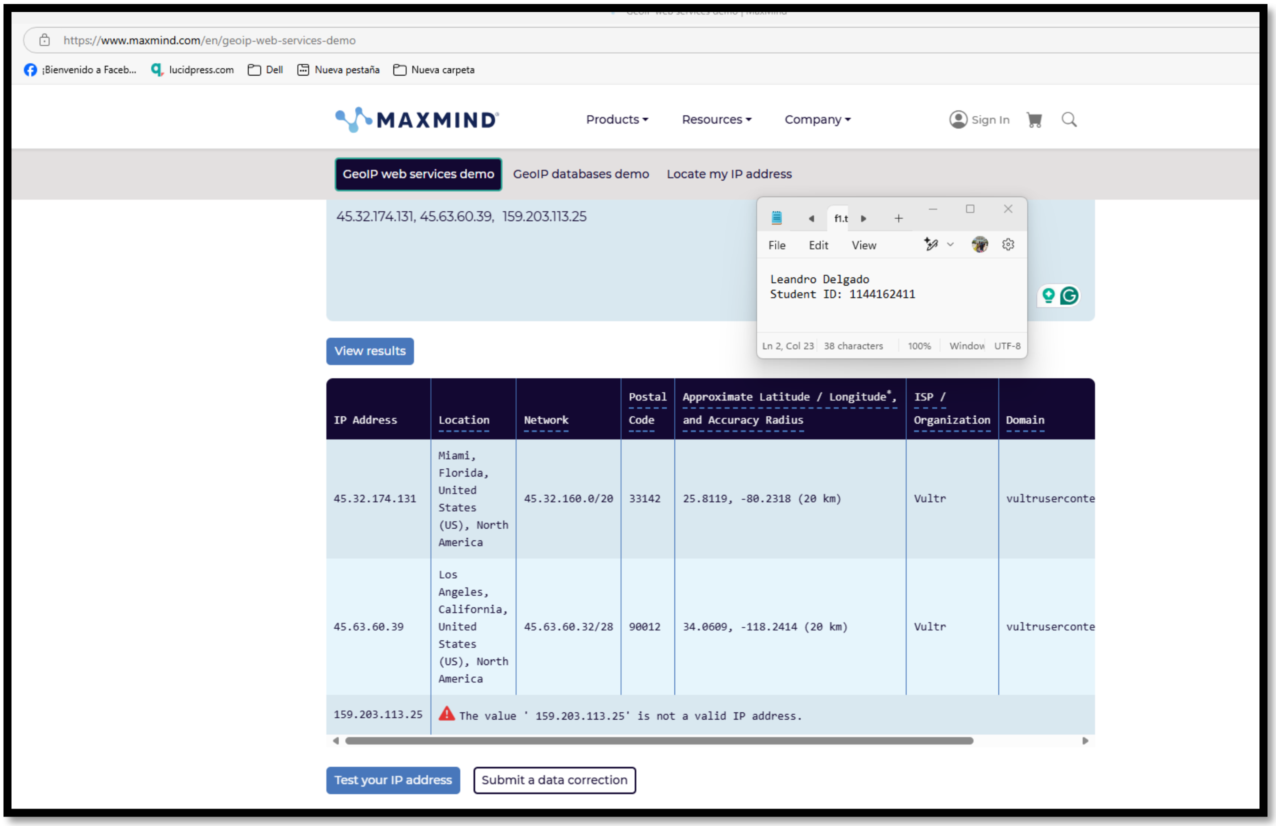
```
NetRange:       45.63.0.0 - 45.63.127.255
CIDR:           45.63.0.0/17
NetName:        CONSTANT
NetHandle:      NET-45-63-0-0-1
Parent:         NET45 (NET-45-0-0-0-0)
NetType:        Direct Allocation
OriginAS:       AS20473
Organization:   The Constant Company, LLC (CHOOP-1)
RegDate:        2015-01-02
Updated:        2022-09-20
Comment:        Geofeed https://geofeed.constant.com/
Ref:            https://rdap.arin.net/registry/ip/45.63.0.0

OrgName:        The Constant Company, LLC
OrgId:          CHOOP-1
Address:        319 Clematis St. Suite 900
City:           West Palm Beach
StateProv:      FL
PostalCode:     33401
Country:        US
RegDate:        2006-10-03
Updated:        2022-12-21
Comment:        http://www.constant.com/
Ref:            https://rdap.arin.net/registry/entity/CHOOP-1

OrgTechHandle: NETWO1159-ARIN
OrgTechName:   Network Operations
OrgTechPhone:  +1-973-849-0500
OrgTechEmail:  network@constant.com
OrgTechRef:    https://rdap.arin.net/registry/entity/NETWO1159-ARIN
```

Leandro Delgado
Student ID: 1144162411

45.63.60.39/45.63.60.39.vultrusercontent.com IP Address Whois | DomainTools.com
m/45.63.60.39
.com Dell Nueva pestaña Nueva carpeta
HOME RESEARCH
DomainTools
PROFILE
CONNECT
MONITOR
SUPPORT
Whois Lookup
LOGIN
Sign Up
Home > Whois Lookup > 45.63.60.39
Notice: Possible deprecation of Whois services after January 28, 2025. More Info
Quick Stats
DomainTools Iris
The gold-standard internet intelligence platform
Learn More
Tools
Monitor Domain Properties
Reverse IP Address Lookup
Network Tools
f1.t
File Edit View
Ln 2, Col 23 38 characters 100% Window UTF-8

Step2. Obtain IP geolocation via Maxmind service

- [GeoIP2 Web Service Demo | MaxMind](https://www.maxmind.com/en/geoip-web-services-demo)
- Just copy/paste IPs to Maxmind service. Observe the result.



45.32.174.131, 45.63.60.39, 159.203.113.25

IP Address	Location	Network	Postal Code	Approximate Latitude / Longitude*, and Accuracy Radius	ISP / Organization	Domain
45.32.174.131	Miami, Florida, United States (US), North America	45.32.160.0/20	33142	25.8119, -80.2318 (20 km)	Vultr	vultruserconte
45.63.60.39	Los Angeles, California, United States (US), North America	45.63.60.32/28	90012	34.0609, -118.2414 (20 km)	Vultr	vultruserconte
159.203.113.25	The value ' 159.203.113.25' is not a valid IP address.					

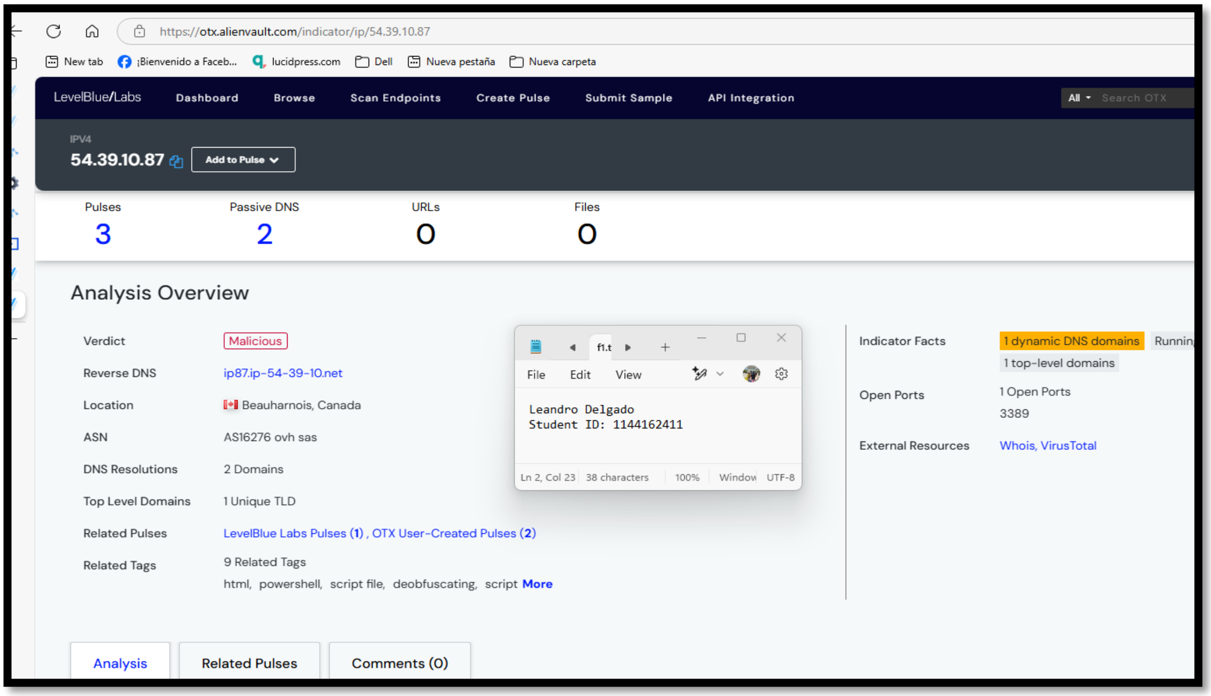
Leandro Delgado
Student ID: 1144162411

When checking the IP addresses, they point to various locations. For example, one of the IP addresses is linked to Miami, Florida.

Step3. Proceed with review

a) Note that first network IOC is marked as scanning host.

b) Open more detailed information. You notice the location of this IP is Canada.



IPV4
54.39.10.87

Pulses	Passive DNS	URLs	Files
3	2	0	0

Analysis Overview

Verdict	Malicious
Reverse DNS	ip87.ip-54-39-10.net
Location	Beauharnois, Canada
ASN	AS16276 ovh sas
DNS Resolutions	2 Domains
Top Level Domains	1 Unique TLD
Related Pulses	LevelBlue Labs Pulses (1) , OTX User-Created Pulses (2)
Related Tags	9 Related Tags html, powershell, script file, deobfuscating, script More

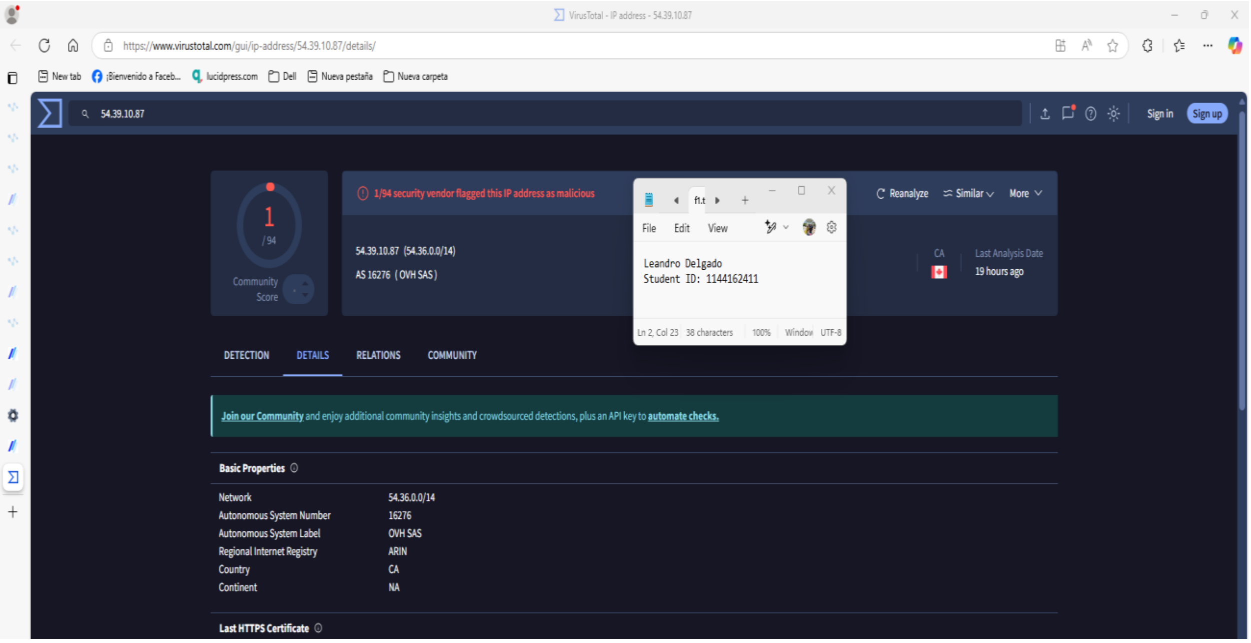
Indicator Facts	1 dynamic DNS domains Runnin 1 top-level domains
Open Ports	1 Open Ports 3389
External Resources	Whois, VirusTotal

```
Leandro Delgado
Student ID: 1144162411
```

Ln 2, Col 23 | 38 characters | 100% | Window | UTF-8

c) Proceed with the tab "External Resources":

a. Virus total: what is said there about location? What are ASN data? The location is Canadas



1 /94 Community Score

1/94 security vendor flagged this IP address as malicious

54.39.10.87 (54.36.0.0/14)
AS 16276 (OVH SAS)

CA

Last Analysis Date 19 hours ago

```
Leandro Delgado
Student ID: 1144162411
```

Ln 2, Col 23 | 38 characters | 100% | Window | UTF-8

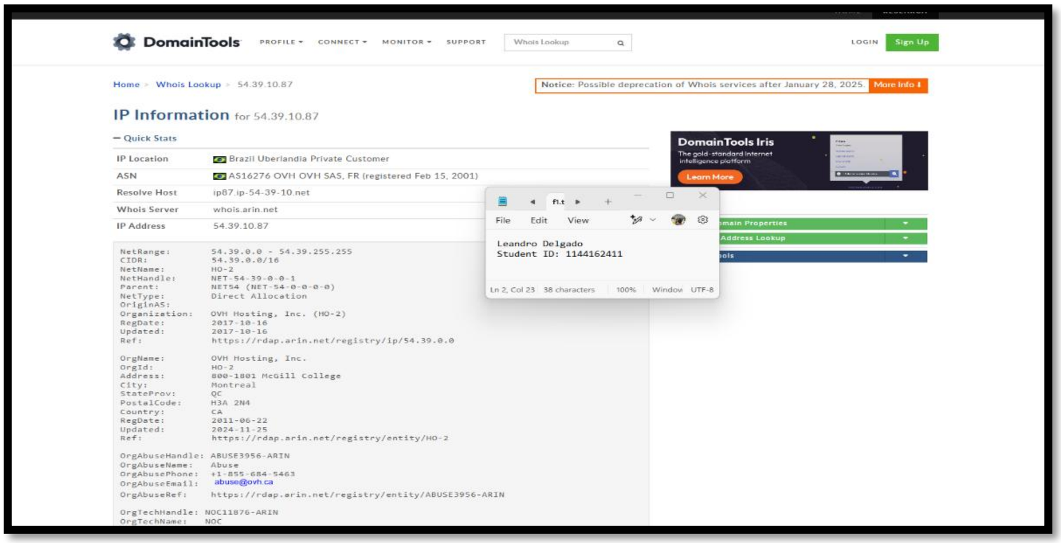
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Basic Properties

Network	54.36.0.0/14
Autonomous System Number	16276
Autonomous System Label	OVH SAS
Regional Internet Registry	ARIN
Country	CA
Continent	NA

Last HTTPS Certificate

b. Whois: what is said about location? What is CIDR?



Notice: Possible deprecation of Whois services after January 28, 2025.

IP Information for 54.39.10.87

— Quick Stats

IP Location	Brazil Uberlandia Private Customer
ASN	AS16276 OVH OVH SAS, FR (registered Feb 15, 2001)
Resolve Host	ip87.ip-54-39-10.net
Whois Server	whois.arin.net
IP Address	54.39.10.87

```
NetRange:       54.39.0.0 - 54.39.255.255
CIDR:           54.39.0.0/16
NetName:        HO-2
NetHandle:      NET-54-39-0-0-1
Parent:         NET54 (NET-54-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   OVH Hosting, Inc. (HO-2)
RegDate:        2017-10-16
Updated:        2017-10-16
Ref:            https://rdap.arin.net/registry/ip/54.39.0.0

OrgName:        OVH Hosting, Inc.
OrgId:          HO-2
Address:        800-1801 McGill College
City:           Montreal
StateProv:      QC
PostalCode:     H3A 2N4
Country:        CA
RegDate:        2011-06-22
Updated:        2024-11-25
Ref:            https://rdap.arin.net/registry/entity/HO-2

OrgAbuseHandle: ABUSE3956-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-855-684-5463
OrgAbuseEmail:  abuse@ovh.ca
OrgAbuseRef:    https://rdap.arin.net/registry/entity/ABUSE3956-ARIN

OrgTechHandle: NOC11876-ARIN
OrgTechName:   NOC
```

```
Leandro Delgado
Student ID: 1144162411
```

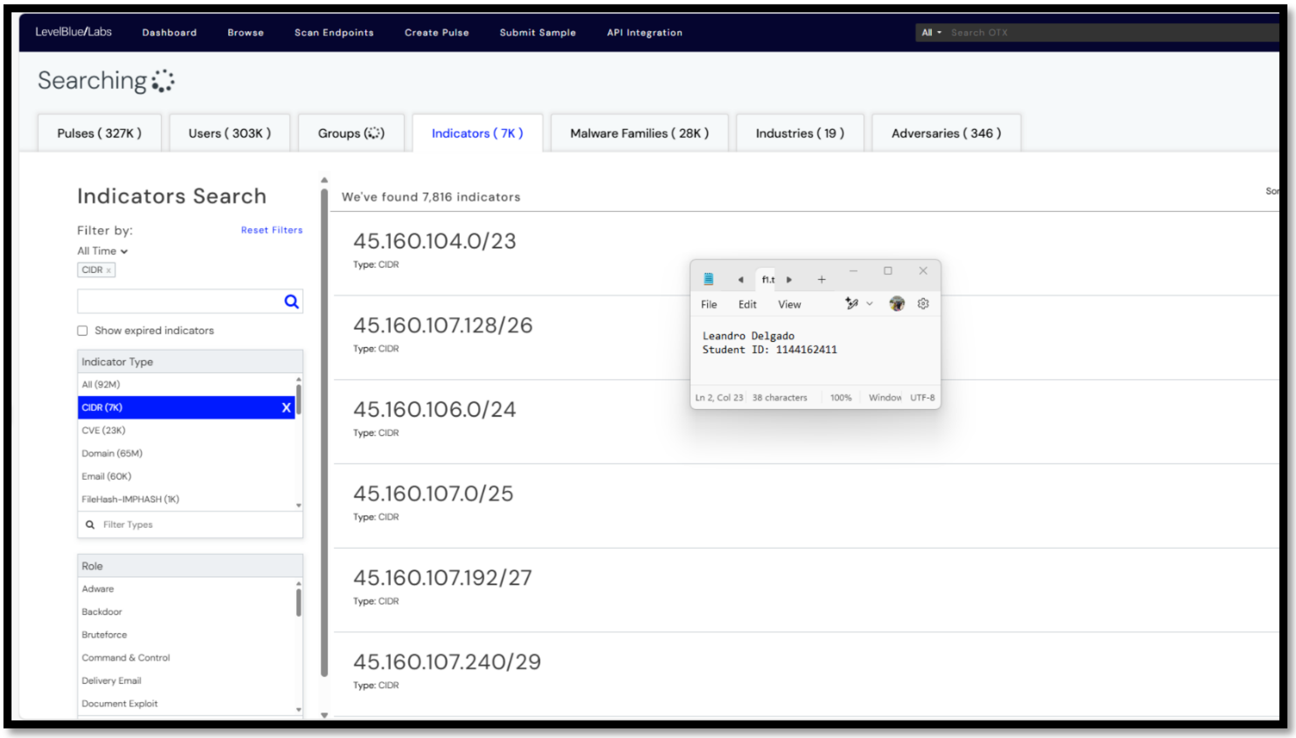
The location is Brazil and CIDR is 54.390.0/16

Step4. Proceed to

- AlienVault - Open Threat Exchange

Step5. Summarize your observations

The image shows a list of IP ranges (CIDR blocks) that might be linked to security threats. The platform helps organize and filter these indicators, making it easier to track and analyze potential issues in network security.



Indicators Search

Filter by: All Time ▾ CIDR ×

We've found 7,816 indicators

45.160.104.0/23
Type: CIDR

45.160.107.128/26
Type: CIDR

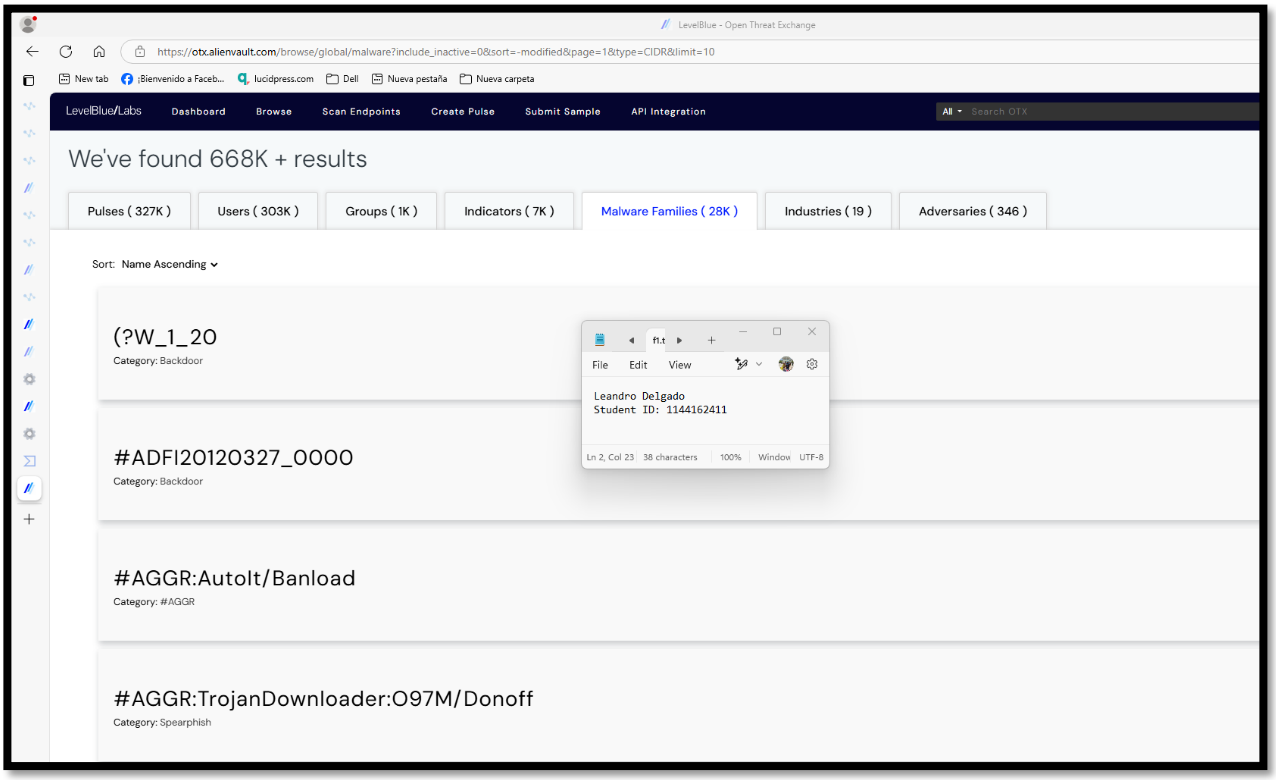
45.160.106.0/24
Type: CIDR

45.160.107.0/25
Type: CIDR

45.160.107.192/27
Type: CIDR

45.160.107.240/29
Type: CIDR

```
Leandro Delgado
Student ID: 1144162411
```



We've found 668K + results

Pulses (327K) | Users (303K) | Groups (1K) | Indicators (7K) | Malware Families (28K) | Industries (19) | Adversaries (346)

Sort: Name Ascending

(?W_1_20
Category: Backdoor

#ADFI20120327_0000
Category: Backdoor

#AGGR:AutoIt/Banload
Category: #AGGR

#AGGR:TrojanDownloader:O97M/Donoff
Category: Spearphish

```
Leandro Delgado
Student ID: 1144162411
```

What IOC/group do you work on?

I focus on analyzing IP address indicators (CIDR blocks), which helps identify suspicious IP ranges that might be linked to cybersecurity threats. By looking at these IP ranges, I can track potential security risks like unauthorized access or breaches.

What threats are associated with it?

These IP indicators are usually connected to threats like adware, backdoor access, and brute force attacks. These types of activities are often carried out by cybercriminals trying to exploit weaknesses in a system.

What details have you found important?

I paid attention to the IP ranges, the ASN numbers (which show who owns the IP), and the geolocation of the IPs. These details are key to understanding where the threats are coming from and whether they're genuinely malicious or not.

What sources of information have you examined?

To get reliable data, I used platforms like MaxMind, DomainTools, VirusTotal, and LevelBlueLabs.

What can you say about consistency of data?

The data from these platforms is generally consistent, but sometimes there are small differences because each platform updates their data at different times.