Cybersecurity

Activity File

Module 12 Day 3: 06 Investigation, Analysis, and Escalation

In this activity, you will continue in your role as an SOC analyst for the California DMV.

- Although IDS alerts indicate an attack, they typically lead to more questions than answers. Security administrators must expand their investigation by performing deep packet analysis using thousands of data points.
- As a junior analyst working in an SOC with multiple tiers of analysts, you need to perform the initial triage of alerts and then escalate these events to senior incident responders.
- You will use Security Onion and Kibana to investigate, analyze, and escalate indicators of attack.

Instructions

Using the following credentials, launch an instance of the Security Onion VM in Azure:

- Username: `sysadmin`
- Password: `cybersecurity`

Investigation and Analysis

Using Security Onion Alert Dashboard, answer the following questions:

Adjust the time interval to go back to the year 2010 until the end of the current day.

1. Group By Source IP, Name tab, what is the top source IP?
2. Group By Destination IP, Name, what is the top destination IP?
3. Group By Sensor, Source IP/Port, Destination IP/Port, Name exclude events with an event severity label of `low`, answer the following questions:
    - What is the top source/destination IP pair? 192.168.10.124 and 110.40.0.103
    - What is the rule name? GPL SNMP public access udp

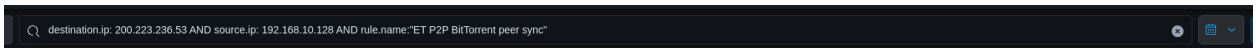
- What is the event severity label? medium

Investigation and Escalation

Using Security Onion, find and select on the following alert:

- Source IP address: `192.168.10.128`.
- Destination IP address: `200.223.236.53`.
- Event message: `ET P2P BitTorrent peer sync`.

Go to Hunt by clicking on it in the left column of Security Onion, and enter the following query `destination.ip: 200.223.236.53 AND source.ip: 192.168.10.128 AND rule.name:"ET P2P BitTorrent peer sync"`.



Click on the destination IP in the results, and select Clipboard and `Copy this value only`.

- Then click `Kibana` in the left column
- Filter using **destination.ip: **. Paste the IP from the clipboard.
- Make sure that you are viewing the last year of data.

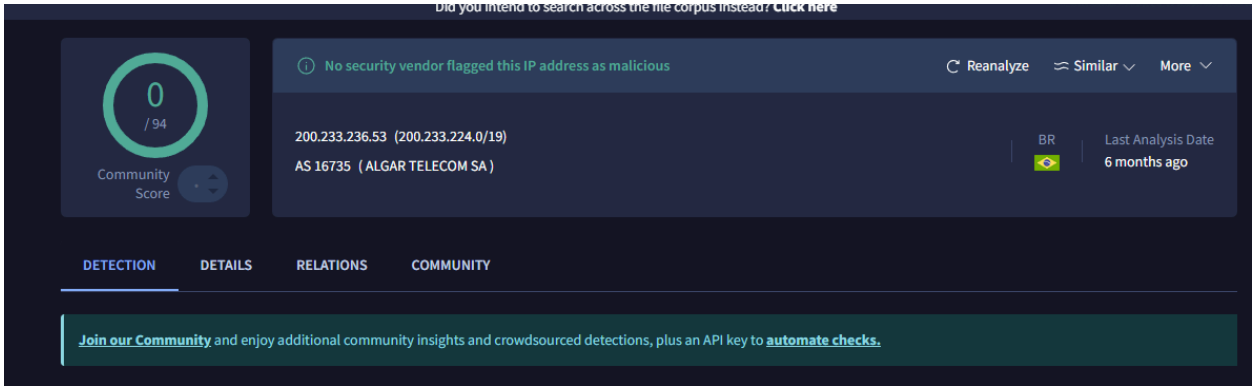
Answer the following questions:

1. What is the event count shown under `Security Onion - All Logs`? 31
2. What is the destination port? 51,275

Go back to Security Onion Hunt.

Using the same alert click on the destination IP and go to Actions, VirusTotal to lookup if the IP address has been flagged as malicious.

3. Was the IP address considered malicious? No



Continue to review the event fields in the Hunt Dashboard and answer the following questions

4. What is the rule category that triggered the alert? Potential Corporate Privacy Violation
5. What is the country name for the destination IP? Brazil

Now that you have gathered all the information needed to fully determine the scope of this particular incident, you're ready to engage your incident response team.