Introduction

In today's evolving cybersecurity landscape, organizations face a continuous stream of threats ranging from phishing campaigns and malware infections to targeted attacks by advanced adversaries. Traditional security measures such as firewalls and antivirus software are no longer sufficient on their own. To effectively defend against sophisticated attacks, organizations must combine **threat intelligence** with **proactive threat hunting** — enabling them to detect, investigate, and respond to potential threats before they cause significant harm.

The objective of this project was to **gather Indicators of Compromise (IOCs)** from open-source threat intelligence platforms and then **conduct a threat hunt** using those IOCs within a simulated enterprise environment through **Azure Sentinel**. By doing so, the project demonstrates how threat intelligence can be operationalized to enhance detection capabilities and improve an organization's overall security posture.

This project involved three core components:

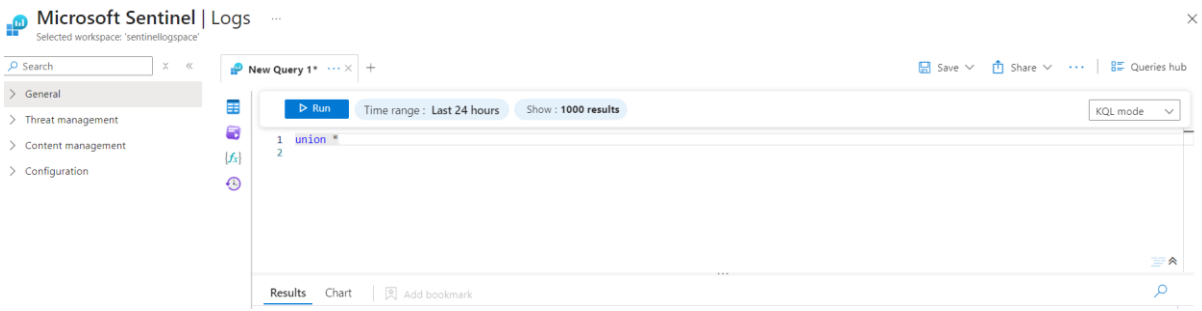
1. **Threat Intelligence Gathering** – Collecting IOCs such as malicious IP addresses, domains, file hashes, and URLs from reputable open-source platforms.
2. **Threat Hunting with KQL** – Using Kusto Query Language (KQL) in Azure Sentinel to search for these IOCs in the **SecurityEvents** log data.
3. **Analysis and Investigation** – Examining the results of the queries to identify suspicious activity, understand the context of potential threats, and determine appropriate response actions.

Through this exercise, I gained practical experience in **integrating threat intelligence into SOC workflows**, **writing KQL queries for proactive hunting**, and **analyzing real-world indicators** to uncover potential malicious activity in an environment.

Steps that I took:

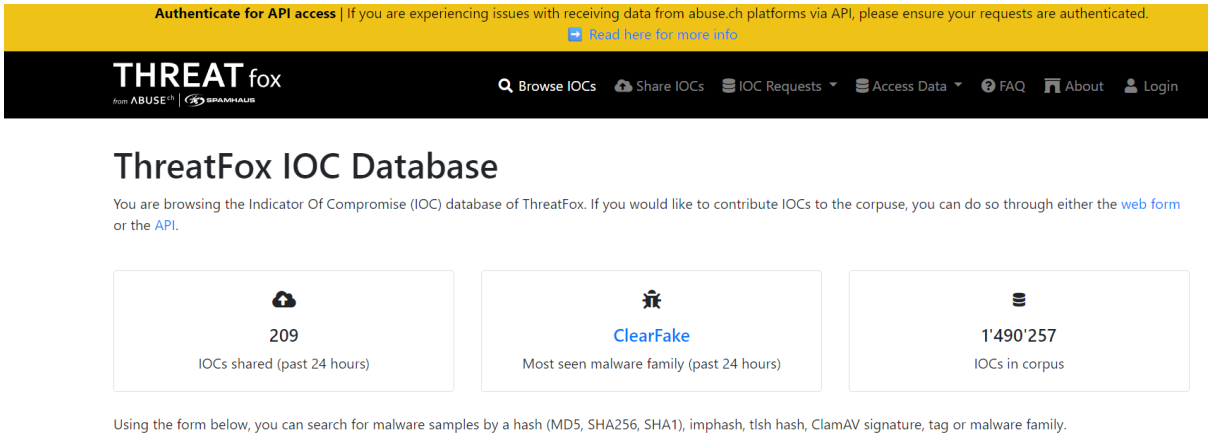
Step 1: Threat Intelligence Gathering and IOC Collection

- Before starting the project, I configured **Microsoft Sentinel** in the Azure portal and ensured that my device was successfully sending security event logs to the **SecurityEvents** table for analysis.

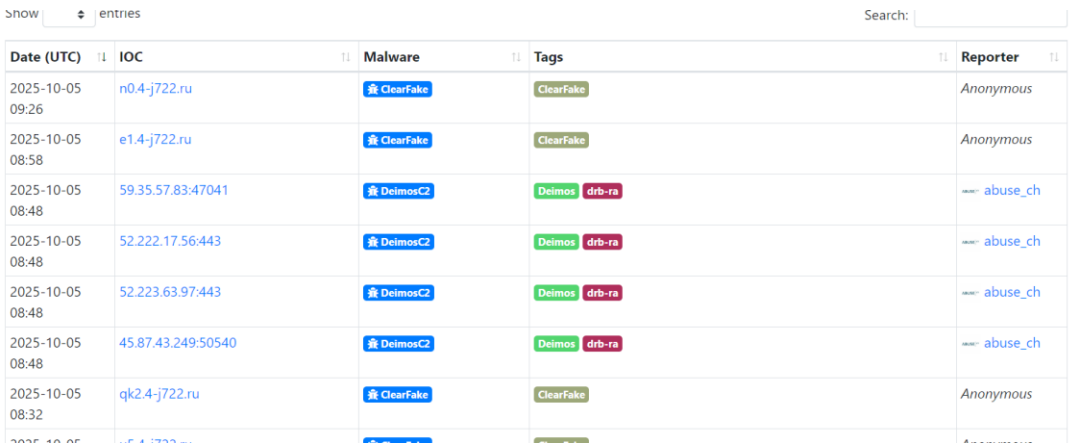


- I accessed **ThreatFox** and explored the dashboard showing IOCs shared within the last 24 hours.

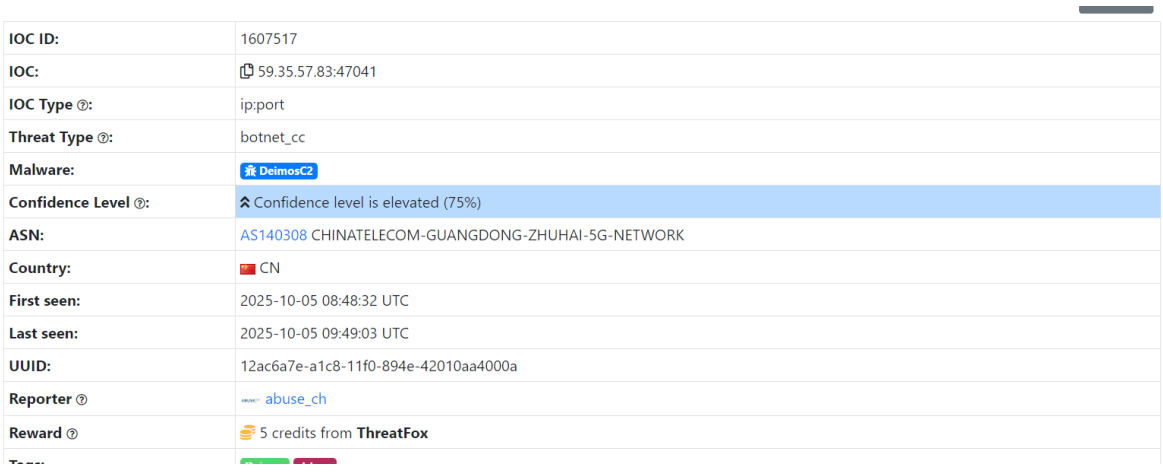
- One of the most recent threats I identified was **ClearFake**, a known malware family.



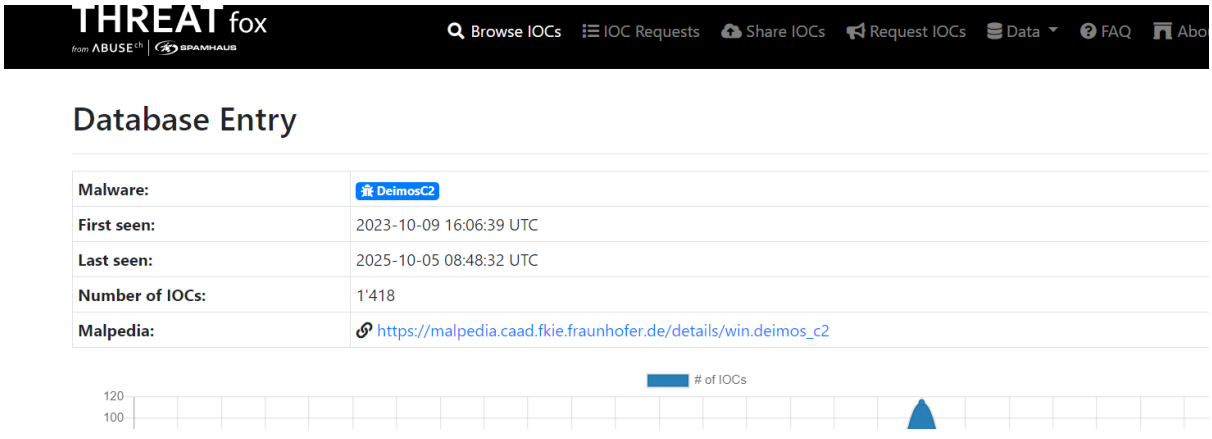
- While browsing the list of IOCs, I selected the **DimosC2** family to focus on for further analysis.



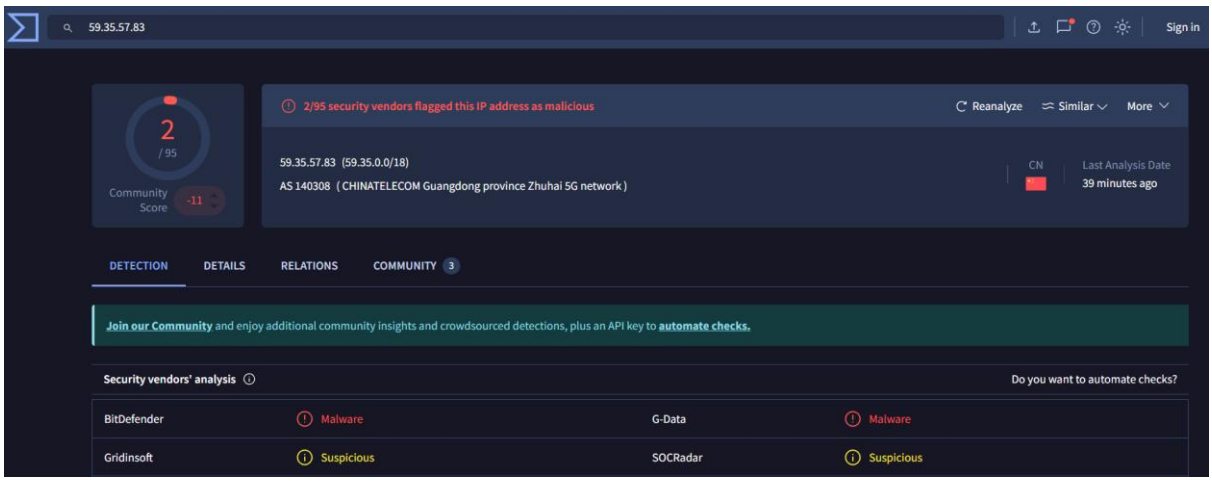
- This IOC contained detailed information, including its **ID, type, threat type, malware family name, origin, first seen, and last seen**.



- I clicked on the **blue icon** next to the malware family name, which redirected me to a detailed page about the **DimosC2** family.
- This page provided comprehensive information such as when the malware family **first appeared**, when it was **last seen**, and a complete **list of all IOCs** associated with that family.



- Next, I copied the IOC IP address **59.35.57.83** and checked it on **VirusTotal** to analyze its reputation and risk level.
- The IP showed a **detection score of 2**, with a **community score of -11**, and while some vendors flagged it as **malicious**, others did not, indicating mixed results.

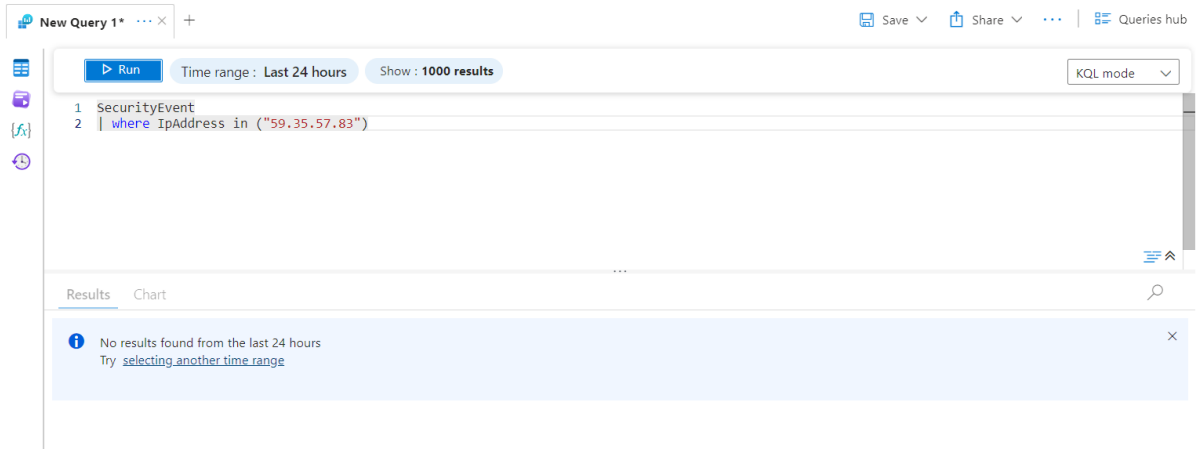


Step 2: Threat Hunting with KQL Queries

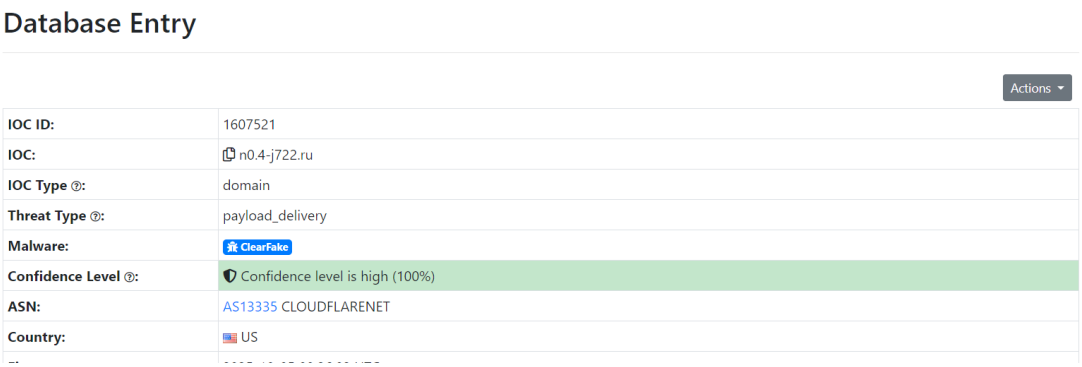
- I used the following **KQL query** in Microsoft Sentinel to search for the IP address in my logs:

```
SecurityEvent
| where IpAddress in ("59.35.57.83")
```

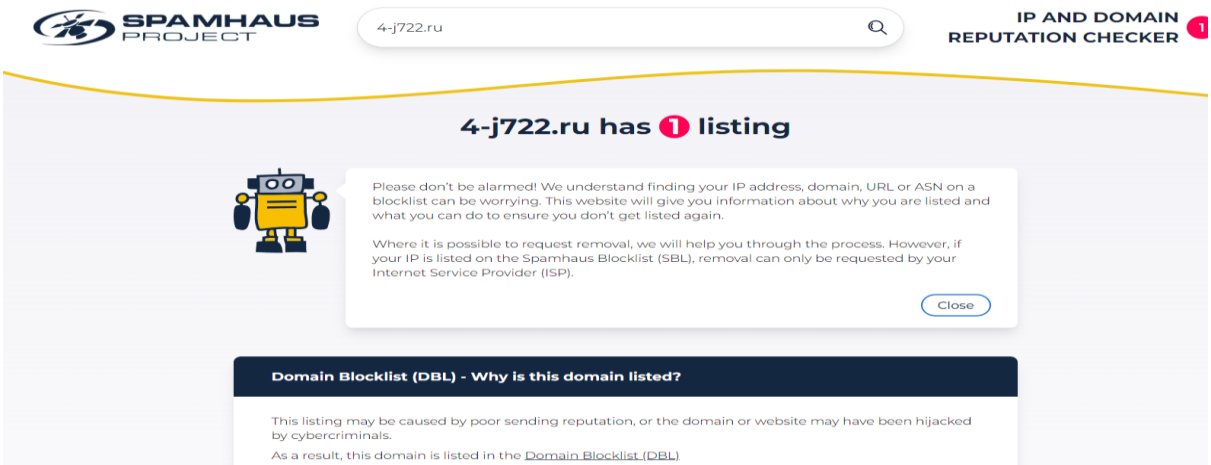
- This query helped me verify whether the malicious IP had appeared in my environment. Since the query returned **no matches**, it indicated that the IP was **not present** in my logs and my system remained **secure**.



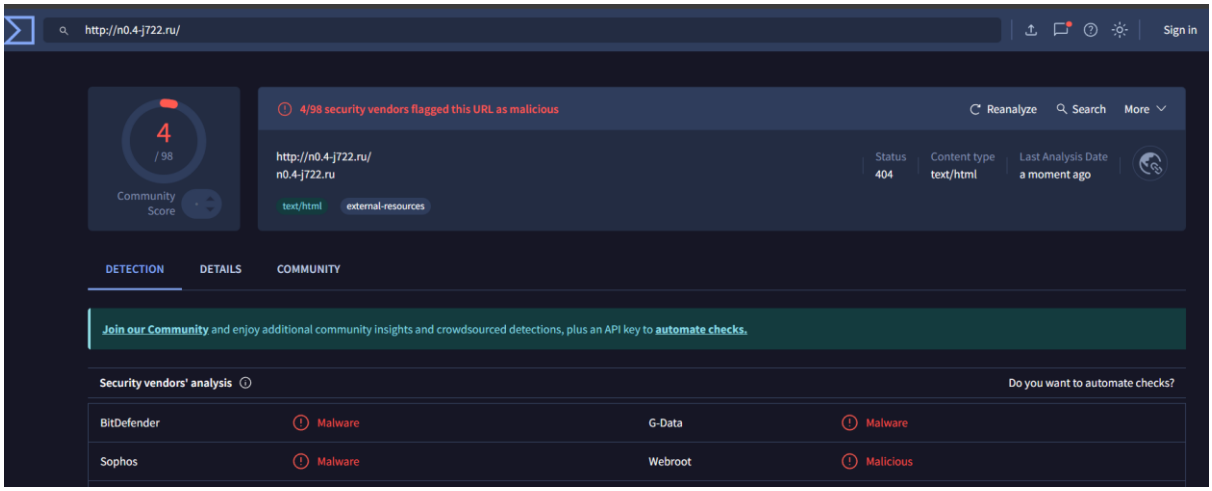
- Next, I returned to **ThreatFox** and selected the **ClearFake** malware family.
- I then copied the **IOC**, which in this case was a **malicious URL link**, for further investigation.



- After copying the URL IOC, I visited the **Spamhaus Project** to check the reputation and threat status of the link.
- The URL check on **Spamhaus** returned a **DBL (Domain Block List)** result, indicating that the link was associated with **malicious or phishing activity**.



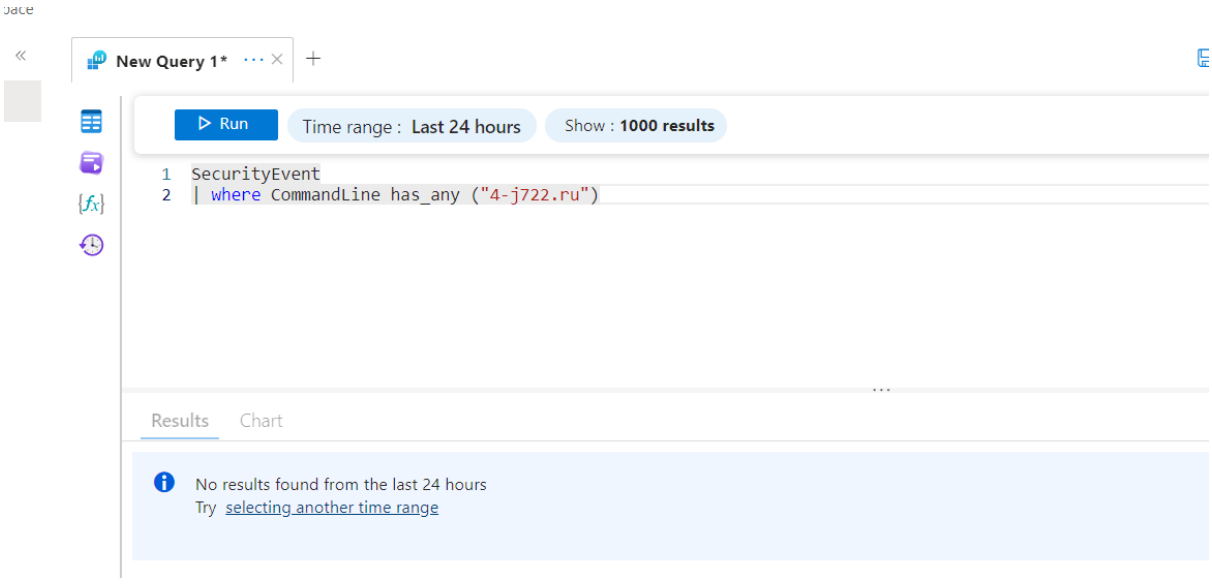
- I then used **VirusTotal** to further analyze the URL IOC, checking its detection status and reputation across multiple security vendors.
- The VirusTotal scan of the URL returned a **detection score of 4/98**, indicating that only a few vendors flagged it as malicious.



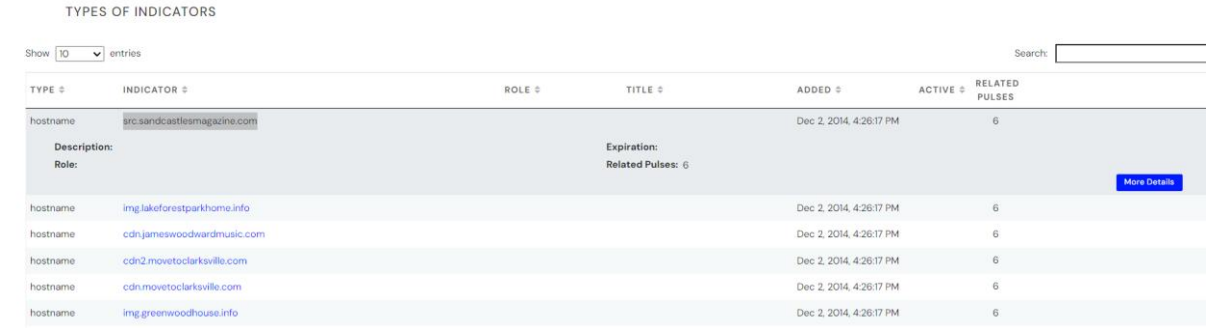
- I copied the URL IOC and ran a **KQL query** in Microsoft Sentinel to check if it appeared in my logs:

```
SecurityEvent
| where CommandLine has_any ("4-j722.ru")
```

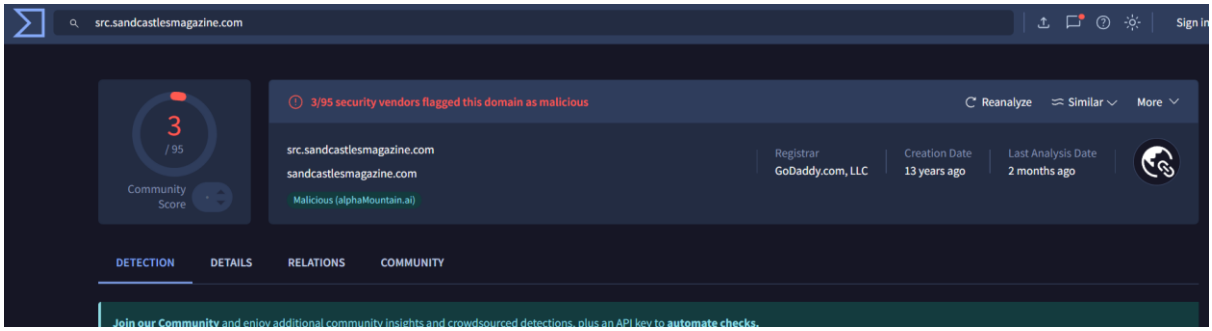
- This allowed me to verify whether the malicious URL had been accessed or executed in my environment.
- The query returned **no results**, indicating that the URL **was not present** in my environment and there was **no associated threat**.



- Next, I visited **AlienVault OTX** and clicked on **“Browse”**, which directed me to a page displaying a **list of available IOCs** for analysis.

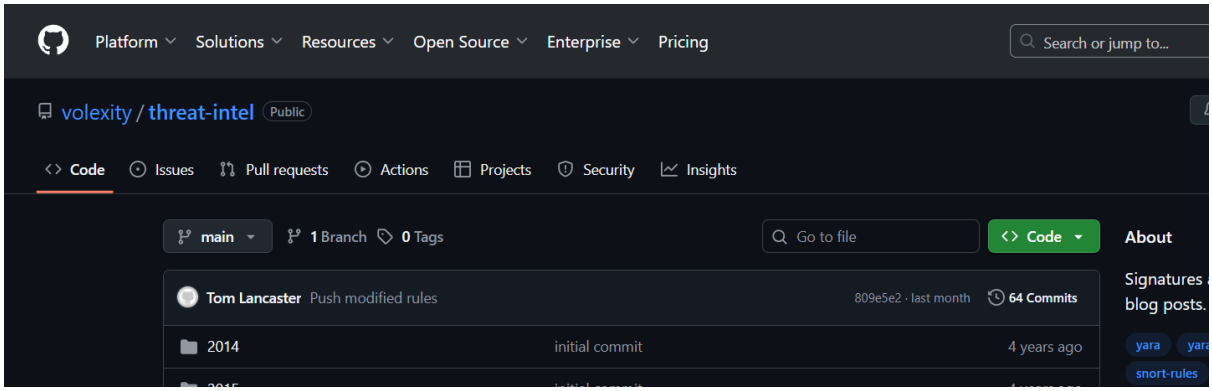


- I then copied one of the **malicious links** from AlienVault and checked it on **VirusTotal** to analyze its detection score and reputation.

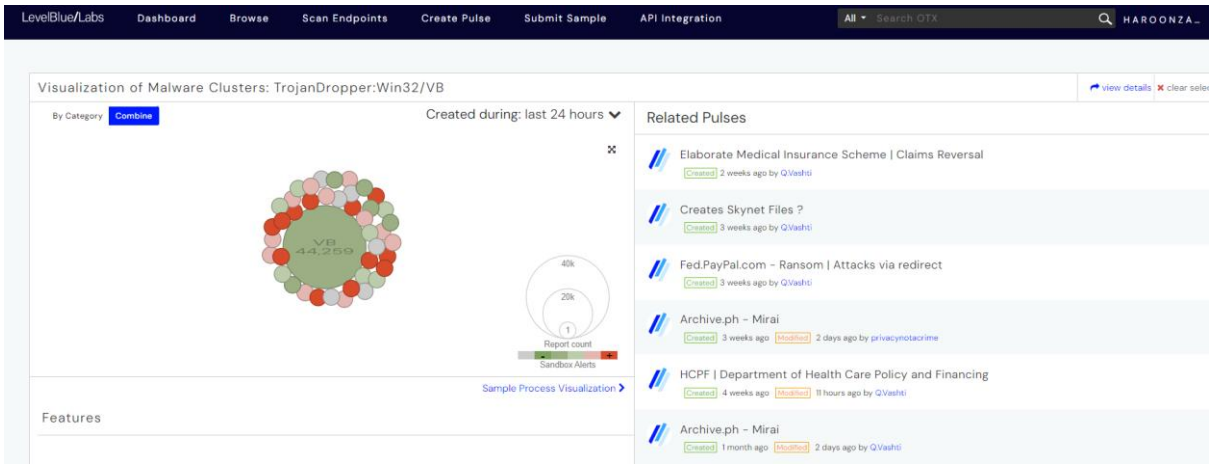


- Additionally, I referred to **Hacker News blogs** to find **fresh updates on new IOCs**, including detailed information on what each IOC does and how it operates.

- I also explored **GitHub**, where many security researchers and creators regularly **post new IOCs** for public use and analysis.



- On the **AlienVault dashboard**, I viewed the IOCs in a **graphical format**, where each IOC is represented as a circle. The **size of the circle** corresponds to the **count of that IOC**, which represents how many times that indicator has been **observed or reported** across the AlienVault community and integrated threat feeds.



Conclusion

Through this project, I gained practical experience in combining **threat intelligence gathering** with **proactive threat hunting** using Microsoft Sentinel. I explored multiple **open-source threat intelligence platforms** including ThreatFox, AlienVault OTX, Spamhaus, VirusTotal, and GitHub to collect **Indicators of Compromise (IOCs)** such as malicious IPs, URLs, domains, and malware families.

I then applied **Kusto Query Language (KQL)** to search the **SecurityEvents** table in Azure Sentinel for these IOCs, allowing me to identify potential threats within the environment. Queries against IP addresses and URLs confirmed whether any of the collected IOCs were present in my logs, helping me assess risk and validate system security.

This exercise enhanced my understanding of:

- **Threat intelligence workflows** and IOC analysis
- **Proactive threat hunting techniques** in a SIEM environment
- **KQL query construction** and log investigation

- **Interpreting threat scores and community feedback** from multiple security vendors

Overall, the project demonstrated how threat intelligence can be effectively operationalized to detect and investigate potential threats, strengthening the overall **security posture** of an organization.