

# 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.



The screenshot shows the Microsoft Sentinel Logs interface. The top navigation bar includes 'Logs' and 'Selected workspace: 'sentinellogspace''. On the left, a sidebar lists 'General', 'Threat management', 'Content management', and 'Configuration'. The main area is titled 'New Query 1\*' with a 'Run' button, a time range of 'Last 24 hours', and a result count of '1000 results'. A KQL code editor shows the following query:

```
union *  
[f]
```

Below the code editor, there are tabs for 'Results' (selected), 'Chart', and 'Add bookmark'.

- 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.

**Authenticate for API access** | If you are experiencing issues with receiving data from abuse.ch platforms via API, please ensure your requests are authenticated.  
[Read here for more info](#)

**THREAT** fox  
from ABUSE.ch 

 [Browse IOCs](#)  [Share IOCs](#)  [IOC Requests](#)  [Access Data](#)  [FAQ](#)  [About](#)  [Login](#)

# ThreatFox IOC Database

You are browsing the Indicator Of Compromise (IOC) database of ThreatFox. If you would like to contribute IOCs to the corpuse, you can do so through either the [web form](#) or the [API](#).



Using the form below, you can search for malware samples by a hash (MD5, SHA256, SHA1), imphash, tish hash, ClamAV signature, tag or malware family.

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

Show	entries	Search:		
Date (UTC)	IOC	Malware	Tags	Reporter
2025-10-05 09:26	n0.4-j722.ru	ClearFake	ClearFake	Anonymous
2025-10-05 08:58	e1.4-j722.ru	ClearFake	ClearFake	Anonymous
2025-10-05 08:48	59.35.57.83:47041	DeimosC2	Deimos drb-ra	abuse_ch
2025-10-05 08:48	52.222.17.56:443	DeimosC2	Deimos drb-ra	abuse_ch
2025-10-05 08:48	52.223.63.97:443	DeimosC2	Deimos drb-ra	abuse_ch
2025-10-05 08:48	45.87.43.249:50540	DeimosC2	Deimos drb-ra	abuse_ch
2025-10-05 08:32	qk2.4-j722.ru	ClearFake	ClearFake	Anonymous
2025-10-05 08:32	5f.4-j722.ru	ClearFake	ClearFake	Anonymous

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

IOC ID:	1607517
IOC:	59.35.57.83:47041
IOC Type ⓘ:	ip:port
Threat Type ⓘ:	botnet_cc
Malware:	DeimosC2
Confidence Level ⓘ:	的信心等级已提升至75% 的信心等级已提升至75%
ASN:	AS140308 CHINATELECOM-GUANGDONG-ZHUHAI-5G-NETWORK
Country:	CN
First seen:	2025-10-05 08:48:32 UTC
Last seen:	2025-10-05 09:49:03 UTC
UUID:	12ac6a7e-a1c8-11f0-894e-42010aa4000a
Reporter ⓘ	abuse_ch
Reward ⓘ	5 credits from ThreatFox

- 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.

The screenshot shows the THREATfox interface. At the top, there's a navigation bar with links for 'Browse IOCs', 'IOC Requests', 'Share IOCs', 'Request IOCs', 'Data', 'FAQ', and 'About'. Below the navigation is a section titled 'Database Entry' for 'DeimosC2'. This section contains a table with the following data:

Malware:	<b>DeimosC2</b>
First seen:	2023-10-09 16:06:39 UTC
Last seen:	2025-10-05 08:48:32 UTC
Number of IOCs:	1'418
Malpedia:	<a href="https://malpedia.caad.fkie.fraunhofer.de/details/win.deimos_c2">https://malpedia.caad.fkie.fraunhofer.de/details/win.deimos_c2</a>

Below the table is a horizontal bar with a blue progress indicator labeled '# of IOCs' ranging from 100 to 120, with a value of approximately 118 indicated by a blue triangle.

- 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.

The screenshot shows the VirusTotal analysis page for the IP address 59.35.57.83. The main summary indicates that 2/95 security vendors flagged the IP as malicious. The IP is identified as 59.35.57.83 (59.35.0.0/18) and AS 140308 (CHINATELECOM Guangdong province Zhuhai 5G network). The last analysis date was 39 minutes ago. The 'DETECTION' tab is selected, showing the following vendor analysis:

Security vendor	Detection	Action
BitDefender	Malware	Malware
Gridinsoft	Suspicious	Suspicious
G-Data		
SOCRadar		

## 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**.

```

New Query 1* ... +
Save Share ... Queries hub
Run Time range : Last 24 hours Show : 1000 results
KQL mode
1 SecurityEvent
2 | where ipAddress in ("59.35.57.83")
...
```

Results Chart

No results found from the last 24 hours  
Try selecting another time range

- 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.

## Database Entry

Actions ▾	
IOC ID:	1607521
IOC:	n0.4-j722.ru
IOC Type ⓘ:	domain
Threat Type ⓘ:	payload_delivery
Malware:	<a href="#">ClearFake</a>
Confidence Level ⓘ:	Confidence level is high (100%)
ASN:	AS13335 CLOUDFLARENET
Country:	US
..	

- 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**.

SPAMHAUS PROJECT

4-j722.ru

IP AND DOMAIN REPUTATION CHECKER 1

4-j722.ru has 1 listing

Please don't be alarmed! We understand finding your IP address, domain, URL or ASN on a blocklist can be worrying. This website will give you information about why you are listed and what you can do to ensure you don't get listed again.

Where it is possible to request removal, we will help you through the process. However, if your IP is listed on the Spamhaus Blocklist (SBL), removal can only be requested by your Internet Service Provider (ISP).

Close

Domain Blocklist (DBL) - Why is this domain listed?

This listing may be caused by poor sending reputation, or the domain or website may have been hijacked by cybercriminals.

As a result, this domain is listed in the [Domain Blocklist \(DBL\)](#).

- 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.

The screenshot shows the VirusTotal analysis interface for the URL <http://n0.4-j722.ru/>. The main summary indicates that 4/98 security vendors flagged the URL as malicious. Below this, a detailed breakdown shows BitDefender and Sophos both flagged it as Malware, while G-Data and Webroot flagged it as Malicious. The URL is identified as a 404 text/html file from a moment ago.

- 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**.

The screenshot shows the Microsoft Sentinel KQL query editor. A new query named "New Query 1" is running, with the command `SecurityEvent | where CommandLine has_any ("4-j722.ru")`. The results pane indicates that no results were found from the last 24 hours, suggesting the URL was not present in the environment during that time.

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

TYPES OF INDICATORS

Show 10 entries Search:

TYPE	INDICATOR	ROLE	TITLE	ADDED	ACTIVE	RELATED PULSES
hostname	src.sandcastlesmagazine.com			Dec 2, 2014, 4:26:17 PM		6
Description:						
Role:			Expiration: Related Pulses: 6			
hostname	img.lakeforestparkhome.info			Dec 2, 2014, 4:26:17 PM		6
hostname	cdn.jameswardmusic.com			Dec 2, 2014, 4:26:17 PM		6
hostname	cdn2.movetoclarksville.com			Dec 2, 2014, 4:26:17 PM		6
hostname	cdn.movetoclarksville.com			Dec 2, 2014, 4:26:17 PM		6
hostname	img.greenwoodhouse.info			Dec 2, 2014, 4:26:17 PM		6

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

src.sandcastlesmagazine.com

3/95 security vendors flagged this domain as malicious

src.sandcastlesmagazine.com  
sandcastlesmagazine.com  
Malicious (alphaMountain.ai)

Registrar: GoDaddy.com, LLC | Creation Date: 13 years ago | Last Analysis Date: 2 months ago

Community Score: 3 / 95

DETECTION DETAILS RELATIONS COMMUNITY

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

- 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.

The Hacker News

Followed by 5.20+ million

SECURING AI AGENTS 101 A Quick Intro for Security Teams

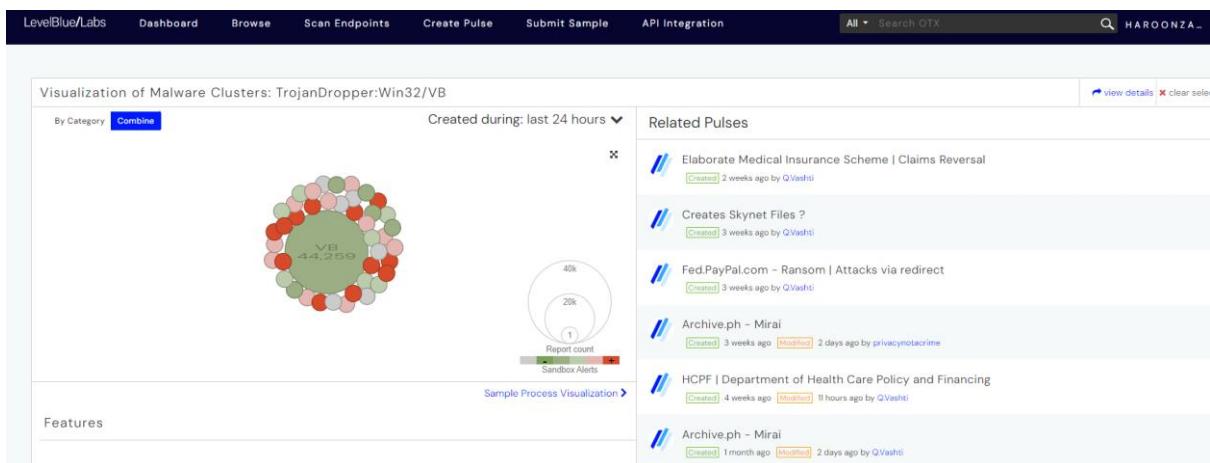
CometJacking: One Click Can Turn Perplexity's Comet AI Browser Into a Data Thief

Scanning Activity on Palo Alto Networks Portals Jump 500% in One Day

corelight NDR DEFENDING THE WORLD'S MOST SENSITIVE NETWORKS (WE CAN'T SAY WHO, BUT YOU'RE HAPPY WE DO) LEARN THE SECRET OF ELITE SOCS >

- 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.