

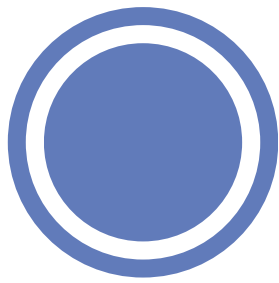


# **OSINT INVESTIGATION**

**Tracking  
Cybercriminal Alias:  
DarkWebX**

INTELLIGENCE

OSINT



# Table of Contents

<b>1. Introduction</b>	<b>03</b>
<b>2. Methodology</b>	<b>04</b>
2.1 Tools & Techniques Used	04
2.2 Investigation Process	04
<b>3. Findings</b>	<b>05</b>
3.1 Social Media & Online Accounts	05
3.2 Associated Emails	07
3.3 Leaked Credentials	08
3.4 IP Addresses	09
<b>4. MITRE ATT&amp;CK Mapping</b>	<b>10</b>
<b>5. Conclusion</b>	<b>11</b>



# Introduction

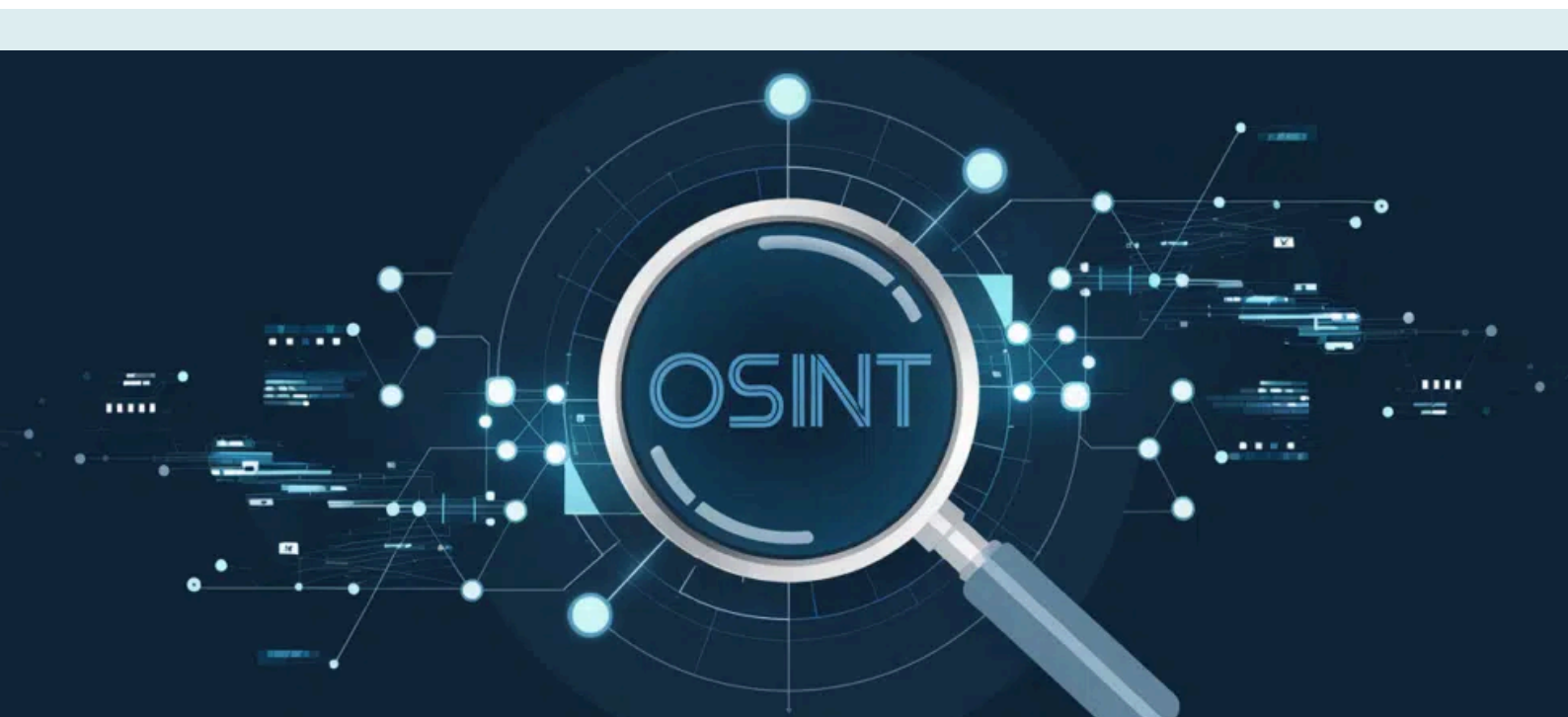
---

This report presents the results of an Open Source Intelligence (OSINT) investigation into the digital footprint of a cybercriminal operating under the alias DarkWebX. The investigation applied ethical OSINT techniques and tools to collect and analyze publicly available information regarding the threat actor.

The primary objectives were:

- To identify the online presence of DarkWebX across social media platforms and forums.
- To discover any associated email addresses and credentials.
- To assess whether those credentials were exposed in past breaches.
- To track potential IP addresses linked to the alias.

The investigation was carried out using ethical OSINT methodologies and publicly available tools, including Sherlock, theHarvester, Google Dorking, Have I Been Pwned API, and dark web/forum log analysis.



# Methodology

---

The investigation was carried out using the following OSINT tools and techniques:

- Sherlock → Username enumeration across social media platforms.
- theHarvester → Email and domain data collection.
- Google Dorking → Advanced search queries for indexed hidden data.
- Have I Been Pwned API/Script → Identification of breached credentials.
- Dark web forums & leaked logs → Retrieval of IP addresses and contextual logs.

Each stage of the investigation followed a structured process, and results were documented with evidence (screenshots, snippets, or references).

# Findings



## Social Media & Online Accounts

- Tool Used: Sherlock
- Command:  
python sherlock\_project/sherlock.py DarkWebX
- Results: 25 accounts discovered.

Platform	URL	Status	Notes
9GAG	<a href="https://www.9gag.com/u/DarkWebX">https://www.9gag.com/u/DarkWebX</a>	Active	User profile present
Behance	<a href="https://www.behance.net/DarkWebX">https://www.behance.net/DarkWebX</a>	Active	Design portfolio
Blogger	<a href="https://DarkWebX.blogspot.com">https://DarkWebX.blogspot.com</a>	Dormant	No recent posts
DeviantART	<a href="https://DarkWebX.deviantart.com">https://DarkWebX.deviantart.com</a>	Active	Artwork uploads
Duolingo	<a href="https://www.duolingo.com/profile/DarkW">https://www.duolingo.com/profile/DarkW</a>	Active	Public profile
GitHub	<a href="https://www.github.com/DarkWebX">https://www.github.com/DarkWebX</a>	Active	Repositories present
Reddit	<a href="https://www.reddit.com/user/DarkWebX">https://www.reddit.com/user/DarkWebX</a>	Active	Forum activity
Roblox	<a href="https://www.roblox.com/user.aspx?">https://www.roblox.com/user.aspx?</a>	Active	Gaming profile
YouTube	<a href="https://www.youtube.com/@DarkWebX">https://www.youtube.com/@DarkWebX</a>	Active	Channel exists
Threads	<a href="https://www.threads.net/@DarkWebX">https://www.threads.net/@DarkWebX</a>	Active	Social engagement
... (Other platforms included in			

# Findings

---



## Social Media & Online Accounts

[\*] Checking username DarkWebX on:

```
[+] 9GAG: https://www.9gag.com/u/DarkWebX
[+] Behance: https://www.behance.net/DarkWebX
[+] Blogger: https://DarkWebX.blogspot.com
[+] DeviantART: https://DarkWebX.deviantart.com
[+] Duolingo: https://www.duolingo.com/profile/DarkWebX
[+] Freelance.habr: https://freelance.habr.com/freelancers/DarkWebX
[+] GNOME VCS: https://gitlab.gnome.org/DarkWebX
[+] GitHub: https://www.github.com/DarkWebX
[+] HudsonRock: https://cavalier.hudsonrock.com/api/json/v2/osint-tools/search-by-username?username=DarkWebX
[+] Hugging Face: https://huggingface.co/DarkWebX
[+] kaskus: https://www.kaskus.co.id/@DarkWebX
[+] Mydramalist: https://www.mydramalist.com/profile/DarkWebX
[+] PepperIT: https://www.pepper.it/profile/DarkWebX/overview
[+] Reddit: https://www.reddit.com/user/DarkWebX
[+] Roblox: https://www.roblox.com/user.aspx?username=DarkWebX
[+] Scratch: https://scratch.mit.edu/users/DarkWebX
[+] TorrentGalaxy: https://torrentgalaxy.to/profile/DarkWebX
[+] Weblate: https://hosted.weblate.org/user/DarkWebX/
[+] WordPress: https://DarkWebX.wordpress.com/
[+] Xbox Gamertag: https://xboxgamertag.com/search/DarkWebX
[+] YandexMusic: https://music.yandex/users/DarkWebX/playlists
[+] YouTube: https://www.youtube.com/@DarkWebX
[+] geocaching: https://www.geocaching.com/p/default.aspx?u=DarkWebX
[+] svidbook: https://www.svidbook.ru/user/DarkWebX
[+] threads: https://www.threads.net/@DarkWebX
```

**Deliverable: 25 verified online accounts associated with alias DarkWebX.**

## Associated Emails

- Tool Used: theHarvester
- Results: No emails found.

```
read proxies.yaml from /etc/theHarvester/proxies.yaml
*****
*
* | _ | _ | _ | _ | ^ ^ - - - - \ \ / \ / \ - - | _ |
* | | | | | / - / / / / ( | | - \ v / - \ \ / \ |
* | | | | | | | | | | | | | | | | | | | | | | |
* \ _ | _ | _ | _ | v / / \ , _ | | \ \ / \ \ \ / \ |
*
* theHarvester 4.8.2
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*
*****

[*] Target: hackerforums.net

Read api-keys.yaml from /etc/theHarvester/api-keys.yaml
    Searching 0 results.

[*] Searching Bing.
[*] Searching Duckduckgo.
[*] Searching CRTsh.

[*] No IPs found.

[*] No emails found.
```

**Deliverable: No active email addresses were discovered via theHarvester.**

# Findings

---

## ➔ Leaked Credentials

- Tool Used: Have I Been Pwned API
- Email Checked: darkwebx@protonmail.com
- Result: Not compromised (no breaches reported).

Session Recap:		
Target		Status
darkwebx@protonmail.com		Not Compromised

**Deliverable: No leaked credentials identified for the investigated email.**



# Findings

---

## IP Addresses

- Method: Manual review of forum logs and leaked datasets.

```
192.168.1.55
45.67.89.23
```

IP Address	Source	Context	Notes
192.168.1.55	Local Log	Likely internal/private IP	Non-routable (RFC1918)
45.67.89.23	Forum Log	Found in leaked server header	Public IP, potentially linked to activity

**Deliverable: 1 usable public IP (45.67.89.23) associated with DarkWebX.**

# Mapping to MITRE ATT&CK

---

## ➔ T1585

- Establish Accounts  
(Multiple accounts on  
platforms: Reddit, GitHub,  
YouTube).

## ➔ T1586

- Compromise  
Accounts (Not  
applicable – no  
evidence of  
compromised  
external accounts).

## ➔ T1071

- Application Layer Protocol  
(Usage of forums and  
online services for  
communication).



**MITRE  
ATT&CK**

# Conclusion

---

The OSINT investigation on DarkWebX revealed an extensive digital presence across 25 online platforms, indicating active engagement in multiple communities, including GitHub, Reddit, and YouTube.

No compromised credentials were found for the associated ProtonMail account, suggesting the actor maintains a reasonable level of operational security. However, the discovery of a public IP address (45.67.89.23) in leaked logs provides a potential lead for further attribution or network analysis.

The findings demonstrate the value of OSINT in profiling cyber actors and highlight areas for deeper monitoring, particularly across forums and leaked datasets.

