
OSINT
INVESTIGATION
Tracking
Cybercriminal Alias:
DarkWebX

Table of Contents

1. Introduction 03

2. Methodology 04

2.1 Tools & Techniques Used 04
2.2 Investigation Process 04

3. Findings 05

3.1 Social Media & Online Accounts 05
3.2 Associated Emails 07
3.3 Leaked Credentials 08
3.4 IP Addresses 09

4. MITRE ATT&CK Mapping 10

5. Conclusion 11

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

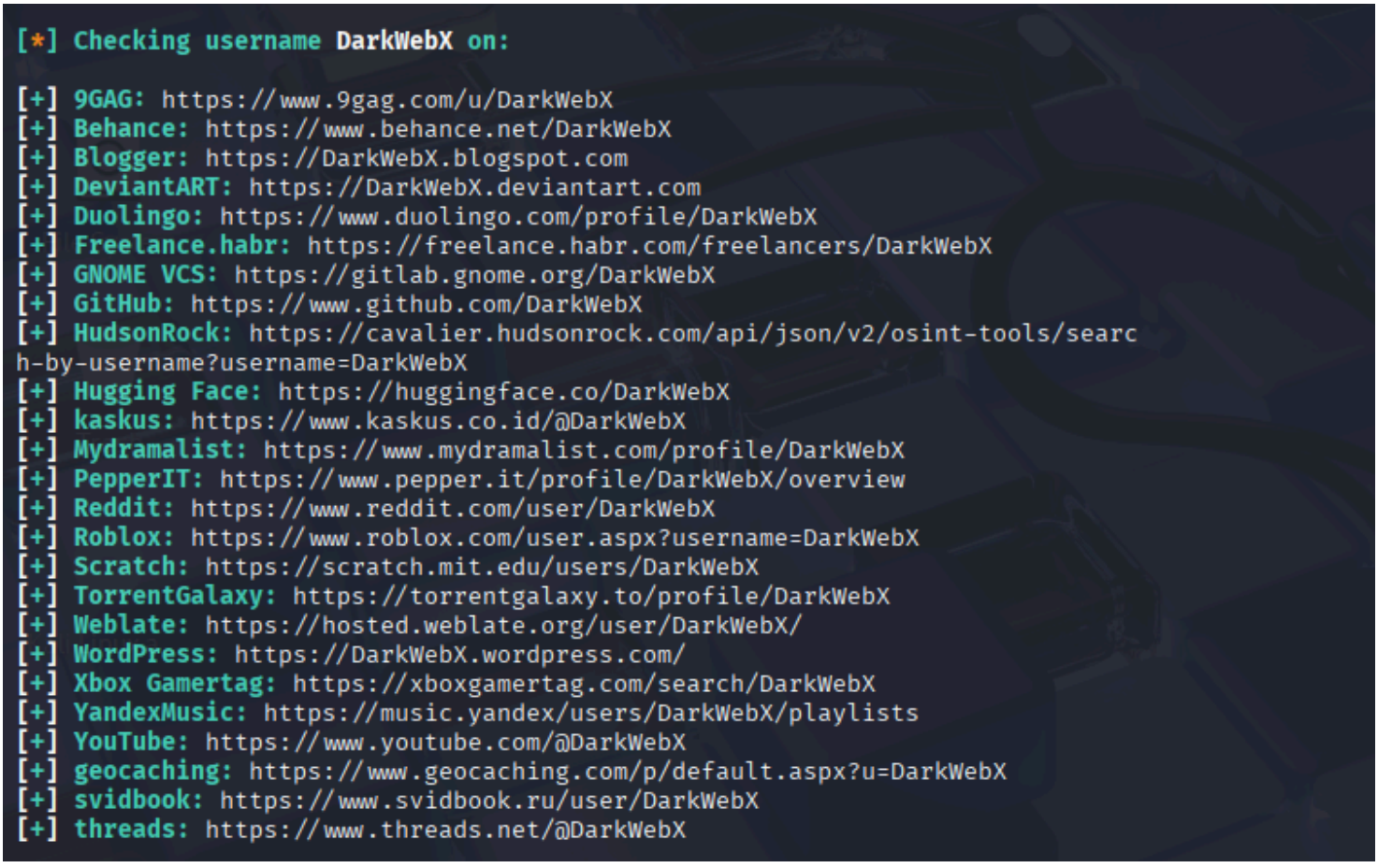
Social Media & Online Accounts

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

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

Findings

Social Media & Online Accounts

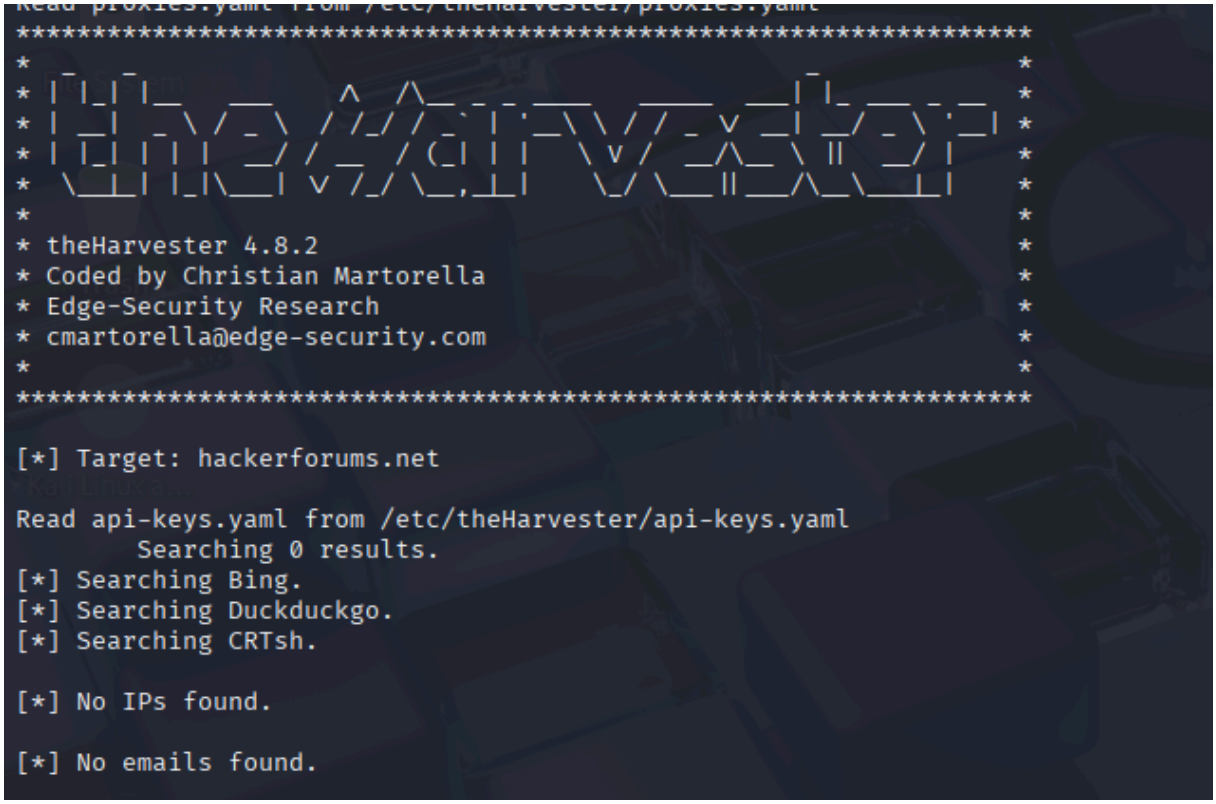


Deliverable: 25 verified online accounts associated with alias DarkWebX.

Findings

Associated Emails

- Tool Used: theHarvester
- Results: 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).

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).

T1071

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

T1586

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

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.