OSINT Investigation Report

Target Alias: DarkWebX
Prepared by: Kareem Omran
Date: 28/9/2025

4. Introduction

This report documents the open-source intelligence (OSINT) investigation into the digital footprint of the cybercriminal alias 'DarkWebX.' Only publicly available information was used.

2. Objectives

- Investigate the digital footprint of DarkWebX.
- Identify and verify social media accounts.
- Discover associated emails.
- Check for leaked credentials.
- Trace any IP addresses in publicly available logs or posts.

3. Methodology

Describe the tools and methods you used. For example:

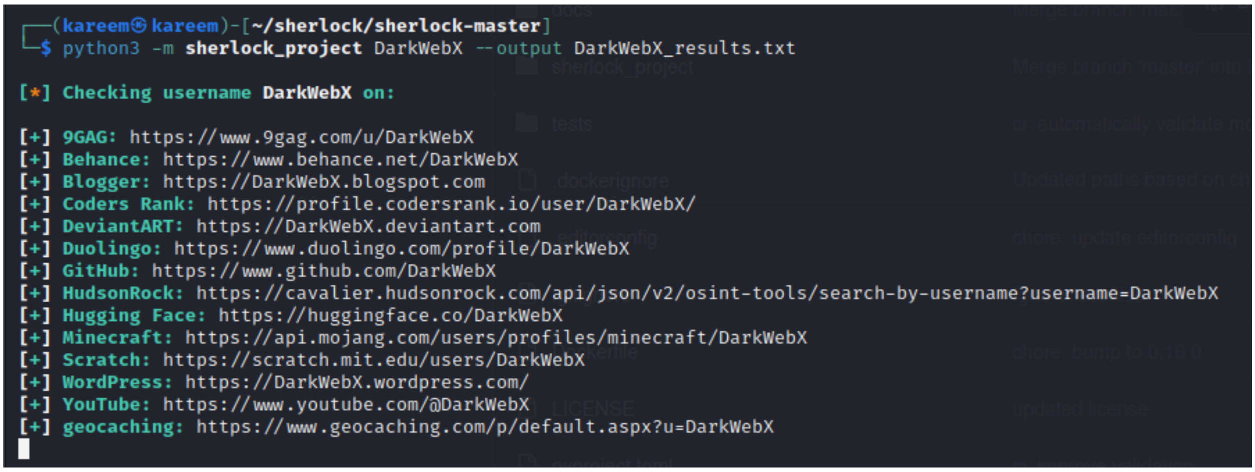
- Sherlock (social media account discovery)
- theHarvester (email and domain data)
- Google Dorking (advanced search queries)
- HaveIBeenPwned (breach and credential checks)
- Forum/Log Analysis (public IP traces)

4. Findings

4.1 Social Media Accounts

Platform/Service	URL	Notes / Status
9GAG	https://www.9gag.com/u/DarkWebX	Found via Sherlock
Behance	https://www.behance.net/DarkWebX	Found via Sherlock
Blogger	https://DarkWebX.blogspot.com	Found via Sherlock (active blog)
Coders Rank	https://profile.codersrank.io/user/DarkWebX/	Found via Sherlock
DeviantART	https://DarkWebX.deviantart.com	Found via Sherlock
Duolingo	https://www.duolingo.com/profile/DarkWebX	Found via Sherlock
GitHub	https://www.github.com/DarkWebX	Found via Sherlock
HudsonRock API	https://cavalier.hudsonrock.com/api/json/v2/osint-tools/search-by-username?username=DarkWebX	Found via Sherlock
Hugging Face	https://huggingface.co/DarkWebX	Found via Sherlock
Minecraft API	https://api.mojang.com/users/profiles/minecraft/DarkWebX	Found via Sherlock
Scratch	https://scratch.mit.edu/users/DarkWebX	Found via Sherlock
WordPress	https://DarkWebX.wordpress.com	Found via Sherlock
YouTube (username)	https://www.youtube.com/@DarkWebX	Found via Sherlock
Geocaching	https://www.geocaching.com/p/default.aspx?u=DarkWebX	Found via Sherlock

Sherlock findings



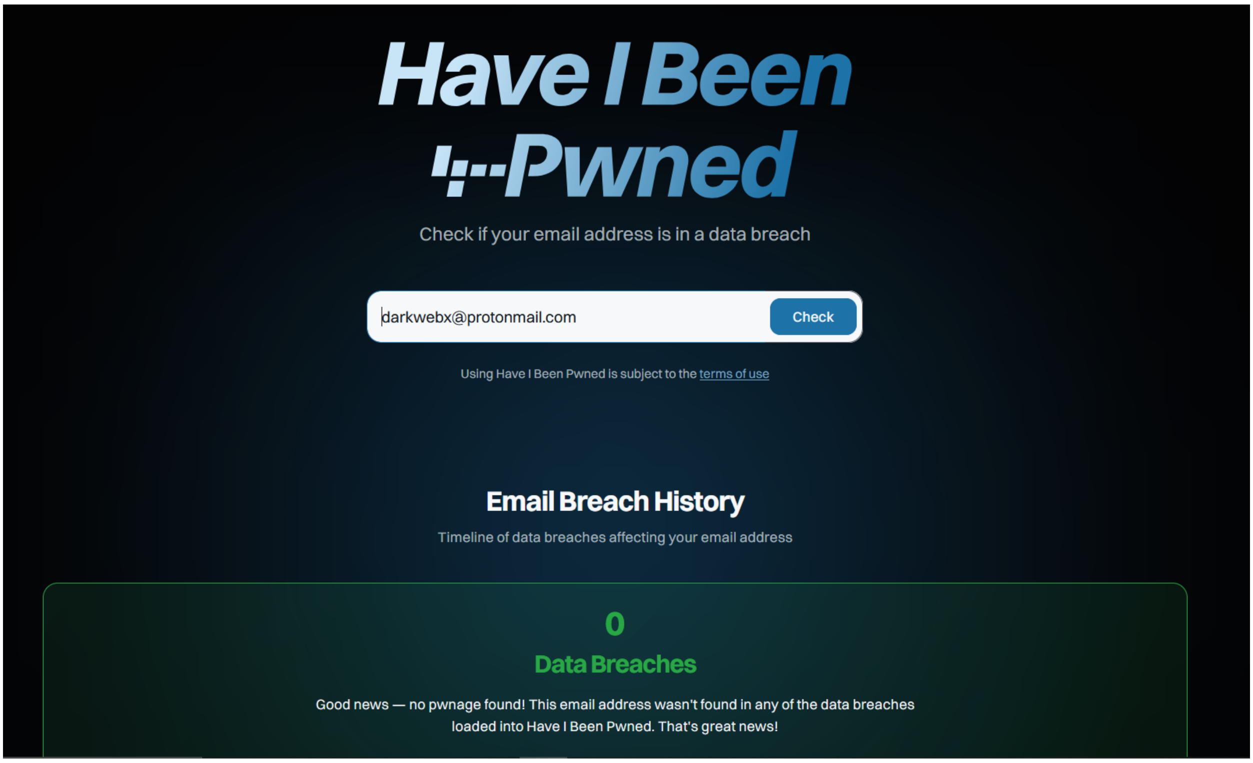
```
┌──(kareem㉿kareem)-[~/sherlock/sherlock-master]
└─$ python3 -m sherlock_project DarkWebX --output DarkWebX_results.txt

[*] Checking username DarkWebX on:

[+] 9GAG: https://www.9gag.com/u/DarkWebX
[+] Behance: https://www.behance.net/DarkWebX
[+] Blogger: https://DarkWebX.blogspot.com
[+] Coders Rank: https://profile.codersrank.io/user/DarkWebX/
[+] DeviantART: https://DarkWebX.deviantart.com
[+] Duolingo: https://www.duolingo.com/profile/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
[+] Minecraft: https://api.mojang.com/users/profiles/minecraft/DarkWebX
[+] Scratch: https://scratch.mit.edu/users/DarkWebX
[+] WordPress: https://DarkWebX.wordpress.com/
[+] YouTube: https://www.youtube.com/@DarkWebX
[+] geocaching: https://www.geocaching.com/p/default.aspx?u=DarkWebX
```

4.2 Associated Email Addresses

Email Address	Source (Forum/Profile)
darkwebx@protonmail.com	HackerForums
https://www.instagram.com/darkwebx__/	Instagram
https://www.reddit.com/user/DarkWebX	Reddit

4.4 Breach History / Leaked Credentials (Bonus)

Email Address	Number of Breaches	Passwords/Hashes Found (if public)	Source
darkwebx@protonmail.com	0	-	HaveIBeenPwned


Have I Been Pwned
Check if your email address is in a data breach
Check
Using Have I Been Pwned is subject to the terms of use

darkwebx@protonmail.com

Email Breach History

Timeline of data breaches affecting your email address

0

Data Breaches

Good news — no pwnage found! This email address wasn't found in any of the data breaches loaded into Have I Been Pwned. That's great news!

4.5 IP Addresses / Server Logs

IP Address	Source / Thread / Log	Context / Evidence	Date of Finding
(none found)	Various paste sites & forum searches	No logs or headers containing “DarkWebX” + IP were publicly visible	28/9/2025

8. Conclusion

This OSINT investigation into the alias **“DarkWebX”** used only publicly available sources and non-intrusive tools. The investigation identified a wide digital footprint across numerous social platforms (including GitHub, WordPress, Blogger, Instagram, and Reddit), but no direct evidence tying these accounts together beyond the shared username could be confirmed.

One publicly listed email address containing the string “darkwebx” was found on a commercial template website; however, this appears to be a vendor contact rather than a personal email, and remains unverified. Searches of Have I Been Pwned returned no breach data for the identified email addresses, and no publicly posted IP addresses or server logs could be located.

Overall, the OSINT gathered to date shows that “DarkWebX” is a widely used handle with multiple public profiles, but provides no conclusive identifying information, no confirmed email, and no leaked credentials or IP addresses. Further investigation would require either private-source intelligence, legal warrants, or direct cooperation with the platforms involved.