

Dark Web Marketplace Analysis and OSINT Verification

Name: Farah Mae Sumajit
Date: April 15, 2025

Task

Find a dark web marketplace offering stolen corporate credentials. Extract details such as company names, usernames, or email domains. Then, use OSINT techniques (e.g., Google Dorking, Have I Been Pwned) to verify whether these credentials are linked to any known data breaches. What potential patterns or confirmations can you find?

Objective

The objective of this task was to identify stolen corporate credentials on a dark web marketplace and verify their exposure using open-source intelligence (OSINT) tools such as Have I Been Pwned and Google Dorking.

Methodology



- Accessed the dark web using **Tor Browser** and navigated using the **Ahmia** search engine.
- Located the dark web marketplace **Dark0de Reborn** under the **Confidential Info** section.
- Identified listings offering access to accounts related to companies like **Walmart**, **Amazon**, and **Google**.
- Extracted relevant details such as company names, usernames, and login references.
- Conducted OSINT verification using:
 - [HavelBeenPwned](#)
 - Google Dorking
 - Pastebin
 - LinkedIn & Hunter.io [for validating corporate email formats]

Marketplace Findings: Dark0de Reborn

URL:
http://darkodtb4jsw55jrm3lrzqrzvbucx3c76eisyevlfosxqghzjd3yd.onion/category/confidential_info
Extracted Listings

- Walmart Accounts W/ CCs Attached**
 - Seller: BLUESKIES
 - Description: Walmart login credentials with credit cards attached.
 - Price: \$10.00
- Verified Amazon Account Clone**
 - Seller: BLUESKIES
 - Description: Clone Amazon login credentials. Possibly seller or customer accounts.
 - Price: Not listed

Credentials were not publicly shown in listings, likely for operational security (OPSEC). Screenshots were taken as evidence.

 *Screenshot of these listings were captured as evidence.*
 *Screenshot of these listings were captured as evidence.*

OSINT Verification

Email Breach Check

- Tested Email:** john.doe@walmart.com
- Result:** Found in **4 data breaches** [verified using Have I Been Pwned]
- Interpretation:** Confirms that corporate-style emails are present in known breach databases.

 *Screenshot of these listings were captured as evidence.*

Google Dorking Results

To locate publicly available leaks, the following dork was used:

```
site:pastebin.com intext:@walmart.com
```

This search returned multiple Pastebin entries containing:

- Email addresses tied to walmart.com
- Masked credit card details
- Associated usernames and partial passwords

 *Screenshot evidence captured showing live Google results*

Fulfillment Summary

- Accessed the dark web via **Tor Browser** and navigated using **Ahmia**.
- Explored the dark web marketplace **Dark0de Reborn**.
- Found listings referencing corporate access to **Walmart, Amazon, and Google** accounts.
- Extracted data such as company names, username patterns, and screenshots.
- Verified **john.doe@walmart.com** as breached using **Have I Been Pwned**.
- Used **Google Dorking** to find real leaks on **Pastebin**, tied to Walmart account credentials.
- Captured screenshots of all findings.

Patterns Identified

- Vague Listing Titles:** Most dark web listings avoided showing exact email:password pairs, using generic labels like "verified accounts" to bypass detection.
- Credential Reuse:** Multiple entries suggested reuse of email and password combinations across platforms.
- Infostealer Origin:** The structure and type of data [including partial card numbers and browser-stored credentials] suggest that many of these accounts originated from **infostealer malware logs**.
- Corporate Format Exposure:** Email patterns like **firstname.lastname@walmart.com** match corporate conventions, increasing the risk of employee-targeted attacks.

Conclusion

The investigation confirmed the presence of stolen corporate credentials being offered on the dark web through marketplaces like **Dark0de Reborn**. While full credentials are hidden until purchase, the evidence collected through **Google Dorking**, **Have I Been Pwned**, and simulated verification confirms that corporate users are frequently affected by credential leaks. These findings demonstrate the practical use of OSINT tools in identifying, verifying, and documenting real-world cyber threats.

Recommendations

