**Prepared by:** Kaylah Freeman-Thomas
**Date:** February 17, 2025
**Classification:** Internal - Security Team

---

# 1. Overview

This report investigates credential leaks detected on the dark web using OSINT techniques. The goal is to identify **exposed credentials, assess threat actor tactics, and recommend mitigation measures** to reduce the risk of account compromises.

---

# 2. Key Findings

## Credential Exposure Analysis

- **5 sets of credentials linked to corporate email addresses** were found on dark web forums.
- **3 compromised accounts show active login attempts** from unauthorized locations.
- **Leaked credentials contain plaintext passwords**, increasing the risk of credential stuffing.

## Threat Actor Insights

- The identified leaks **originate from underground marketplaces** and **hacker forums**.
- Threat actors **sell login credentials** bundled with **browser session cookies** to bypass MFA.
- **Credential stuffing tools** such as **OpenBullet** and **Sentry MBA** were referenced in forum discussions.

---

# 3. Attack Methodology Analysis

Threat actors leverage stolen credentials in the following phases:

## Phase 1: Credential Acquisition

- **Techniques Used:**
    - Data breaches from unsecured databases

    - Phishing campaigns targeting employees
    - Malware (keyloggers, infostealers)

### Phase 2: Credential Exploitation

- **Tactics Observed:**
    - Automated login attempts using credential stuffing bots
    - Selling stolen credentials on dark web markets
    - Bypassing multi-factor authentication (MFA) using stolen session cookies

---

# 4. Risk Assessment

### Severity Level: HIGH

- **Potential Impact:**
    - **Account Takeover:** Unauthorized access to internal systems.
    - **Privilege Escalation:** Attackers could **escalate privileges** within SaaS platforms.
    - **Data Exfiltration:** Sensitive customer or company data may be extracted.

---

# 5. Recommended Mitigation Strategies

### Immediate Actions (Within 24 Hours)

- **Force password resets** for all exposed accounts.
- **Implement mandatory Multi-Factor Authentication (MFA)**.
- **Block known compromised IP addresses** linked to unauthorized access attempts.

### Long-Term Strategies

1. **Dark Web Monitoring:** Establish an automated threat intelligence feed.
2. **Password Policy Enforcement:** Require **strong, unique passwords** per account.
3. **Security Awareness Training:** Educate employees on **phishing risks** and **password hygiene**.
4. **Account Lockout Measures:** Limit failed login attempts to prevent **brute-force attacks**.

---

# 6. Conclusion

Dark web activity suggests that **corporate credentials have been actively traded** among cybercriminals. Without immediate **mitigation efforts**, affected accounts **remain at risk** for **fraud, data theft, and ransomware attacks**.

By enforcing **MFA, monitoring the dark web, and strengthening authentication policies**, organizations can **reduce exposure and prevent credential-based attacks**.

---

# 7. Appendix: Supporting Data

### Threat Intelligence Sources:

- **Shodan Breach Database**
- **Have I Been Pwned (HIBP)**
- **Recorded Future Dark Web Intelligence**

### MITRE ATT&CK Techniques Used:

- **T1078 - Valid Accounts**
- **T1110 - Brute Force**
- **T1555 - Credentials from Password Stores**
- **T1586 - Compromise Accounts**