Identity Compromise Detection - Threat Report

Prepared by: Kaylah Freeman-Thomas

Date: February 17, 2025

Classification: Internal - Security Team

---

1. Overview

This report investigates identity compromises observed in user authentication logs. The analysis focuses on **failed login attempts**, **unusual geographic activity**, and **dark web exposure**. The goal is to assess risk levels and recommend countermeasures to mitigate account compromise threats.

---

2. Threat Summary

Key Findings:

- **12 user accounts flagged as compromised** due to **repeated failed login attempts**.
- **High-risk activity originated from Russia and China**, targeting admin and privileged accounts.
- **5 accounts linked to known credential leaks on the dark web**, increasing exposure risk.
- **Login attempts occurred outside normal business hours**, indicating automated bot-driven attacks.
- **Multiple IPs used for login attempts**, suggesting credential stuffing or brute-force tactics.

Data Insights:

Metric	Value
Total Login Attempts	450+
Failed Logins from Untrusted IPs	210+
Countries Involved	5
Known Compromised Accounts	12
Dark Web Matches	5

---

3. Attack Methodology Analysis

Threat actors used the following **tactics, techniques, and procedures (TTPs)** from the **MITRE ATT&CK** framework:

- **T1078 - Valid Accounts**: Attempted unauthorized access using previously stolen credentials.
- **T1110 - Brute Force**: Repeated login attempts against admin accounts.
- **T1190 - Exploit Public-Facing Application**: Some login attempts were observed on exposed web services.
- **T1589 - Gather Victim Credentials**: Dark web exposure analysis shows previously leaked credentials.

Attack Chain Analysis:

1. **Reconnaissance:** Threat actors acquired leaked credentials from **dark web marketplaces**.
2. **Credential Stuffing:** Automated login attempts using credential lists from previous breaches.
3. **Privilege Escalation Attempt:** Unusual access requests on admin-level accounts.

---

4. Risk Assessment

Threat Severity: High

Potential Impact:

- Unauthorized access to **sensitive corporate data**.

- Increased risk of **ransomware deployment** if attackers escalate privileges.
- Potential regulatory compliance violations (**GDPR, CCPA, NIST**, etc.).

---

5. Recommendations & Mitigation Strategies

Immediate Actions (Within 24 Hours)

✅ **Force password resets** for all **compromised accounts**.
✅ **Block IP addresses** associated with high-risk login attempts.
✅ **Enable MFA (Multi-Factor Authentication)** for all admin accounts.
✅ **Conduct an incident response meeting** to assess broader exposure.

Long-Term Security Measures

1️⃣ **Implement Conditional Access Policies:** Restrict logins from high-risk locations.
2️⃣ **Dark Web Monitoring:** Proactively search for exposed credentials.
3️⃣ **Behavioral Analytics for Login Attempts:** Detect unusual access patterns.
4️⃣ **Security Awareness Training:** Educate employees on phishing and password hygiene.

---

6. Conclusion

This analysis confirms that at least **12 accounts were targeted using known attack vectors**, with **5 accounts directly linked to leaked credentials**. Without **immediate remediation**, the risk of **data exfiltration, account takeover, or ransomware deployment** remains high.

By enforcing **multi-layered authentication**, monitoring login behaviors, and restricting access from high-risk locations, the organization can **mitigate these threats and reduce exposure**.

---

7. Appendix: Supporting Data

MITRE ATT&CK Techniques Used:

T1078 - Valid Accounts
T1110 - Brute Force
T1190 - Exploit Public-Facing Application
T1589 - Gather Victim Credentials