

# Stolen Credentials

- [Stolen Credentials: Detection](#)
- [Mitigation Plan for Stolen Credentials](#)

# Stolen Credentials: Detection

Stolen credentials refer to user account information (typically usernames or email addresses and passwords) that have been compromised and made available in underground markets or public data dumps. These leaks often result from data breaches of various organizations and can pose significant risks when employees use the same credentials across personal and professional accounts.

## How We Detect Stolen Credentials

Our process for identifying stolen credentials involves:

1. **Data Collection:**
  - We maintain access to extensive databases of leaked credentials from various sources.
  - These databases are regularly updated with new leaks and breaches.
2. **Asset Identification:**
  - We compile a list of email domains and usernames associated with your organization.
3. **Database Scanning:**
  - We scan the leaked credential databases for matches with your organization's email domains and usernames.
4. **Pattern Matching:**
  - We look for common username patterns that might be associated with your organization but not use your official email domain.
5. **Historical Analysis:**
  - We check for credentials leaked in past breaches that might still be in use.
6. **Continuous Monitoring:**
  - Our systems continuously monitor for new leaks and breaches, providing real-time alerts for newly compromised credentials.

## What We Look For

1. **Email Addresses:** Corporate email addresses found in leaked databases.

2. **Username:** Common username formats used by your organization.
3. **Password:** Leaked passwords associated with identified emails or usernames.
4. **Additional PII:** Other personally identifiable information that may be included in the leak.
5. **Breach Sources:** Information about where and when the credentials were leaked.

# Implications of Stolen Credentials

1. **Account Takeover:** Attackers can potentially access corporate accounts using stolen credentials.
2. **Data Breaches:** Compromised accounts can lead to unauthorized access to sensitive corporate data.
3. **Phishing Campaigns:** Stolen email addresses can be targeted in sophisticated phishing attacks.
4. **Reputation Damage:** If exploited, stolen credentials can lead to incidents that damage company reputation.
5. **Financial Loss:** Both direct theft and remediation costs can result in significant financial impact.
6. **Regulatory Issues:** Exposure of certain types of data can lead to compliance violations and fines.

# Mitigation Plan for Stolen Credentials

When our scanning process identifies stolen credentials associated with your organization in leaked databases, it's crucial to act quickly and implement a comprehensive mitigation strategy. Here's a detailed plan to address this security risk:

## Immediate Actions

- 1. Password Resets**
  - Force immediate password changes for all affected accounts.
  - Ensure new passwords meet strong complexity requirements.
- 2. Account Lockdowns**
  - Temporarily lock affected accounts until the user verifies their identity.
  - Implement additional authentication steps for these accounts.
- 3. Multi-Factor Authentication (MFA)**
  - Enable MFA for all affected accounts immediately.
  - Prioritize rolling out MFA across the entire organization if not already implemented.
- 4. Access Review**
  - Conduct an immediate review of access logs for affected accounts.
  - Look for any suspicious activities or unauthorized access attempts.
- 5. Notification and Education**
  - Notify affected users about the credential leak.
  - Provide clear instructions on how to secure their accounts.
  - Educate users on the risks of password reuse across multiple sites.

## Short-term Strategies

- 6. Credential Screening**
  - Implement a system to screen new passwords against lists of known compromised passwords.
  - Prevent users from setting passwords that have been previously exposed in leaks.
- 7. Enhanced Monitoring**
  - Increase monitoring of affected accounts for a set period (e.g., 30-60 days).
  - Set up alerts for unusual login patterns or access attempts.

## 8. **Phishing Awareness**

- Conduct a phishing awareness campaign, as leaked email addresses may be targeted.
- Provide training on how to identify and report suspicious emails.

## 9. **VPN and Remote Access Review**

- Review and tighten security for VPN and remote access systems.
- Implement or enhance network segmentation to limit potential damage from compromised accounts.

# Long-term Strategies

## 10. **Password Policy Enhancement**

- Review and strengthen organizational password policies.
- Consider implementing passphrases instead of complex passwords.
- Enforce regular password changes, but balance this with usability to prevent password fatigue.

## 11. **Single Sign-On (SSO) Implementation**

- Consider implementing SSO to reduce the number of credentials users need to manage.
- Ensure the SSO solution itself is highly secure and supports strong authentication methods.

## 12. **Passwordless Authentication**

- Explore and implement passwordless authentication methods where possible (e.g., biometrics, security keys).

## 13. **Continuous Monitoring for Credential Leaks**

- Implement a continuous monitoring solution for detecting newly leaked credentials.
- Set up automated alerts and response procedures for future credential leaks.

By implementing these mitigation strategies, organizations can significantly reduce the risks associated with stolen credentials, enhance overall security posture, and better protect sensitive information from unauthorized access. Regular review and updating of these practices will help maintain robust security in the face of evolving threats.