

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. **Usernames:** Common username formats used by your organization.
3. **Passwords:** 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.

Revision #1

Created 19 September 2024 11:06:29 by Admin

Updated 19 September 2024 11:06:56 by Admin