THE PREVALENCE AND IMPACT OF ACCOUNT TAKEOVER

WHAT ORGANIZATIONS NEED TO KNOW

ENZOIC

Introduction

Although other forms of authentication exist, passwords remain the primary means of authentication for most organizations. Unfortunately, many individuals use weak or easily guessable passwords, or they reuse passwords across multiple systems. According to Bitwarden's 2023 Password Decision Survey, 90% of employees admit to reusing passwords. While the risk of having these passwords exposed remains the same, the damages are multiplied across accounts sharing the same password.

Attackers take advantage of these poor password hygiene behaviors to steal corporate credentials and gain access to sensitive information. Account Takeover attacks are becoming more sophisticated and frequent. Successful attacks can lead to privilege escalation, impersonation, data breaches, and reputational damage and are used to launch malware. Given that compromised credentials are the #1 cause of a data breach, according to Verizon's 2022 DBIR Report, it is essential that organizations understand what ATO is, who is targeted, and what they can do to prevent it.

What is Account Takeover (ATO)?

ATO is a form of identity theft where cybercriminals steal employee passwords to gain access to an organization's information. Once an attacker gains access to a corporate account, they can access additional lists of employee credentials, financial information, and company data. An attacker can employ malware or have ongoing access to the company for nefarious reasons. The entry point is often a single compromised corporate credential.

Who is a Target for ATO?

Everyone using passwords for authentication is vulnerable to ATO attacks. This includes organizations that may not use passwords as the primary method of authentication, but as a secondary method or as one step in a multifactor authentication process. Large, high-revenue companies like national banks or healthcare organizations are targets because their payoff is often massive if hackers can complete a successful attack. However, small- and mid-sized companies are also targeted. Cybercriminals are catching on to the fact that smaller organizations may not have the resources to establish cybersecurity protocols or IT team members to keep things locked down.

What Attacks Can Lead to an ATO?

Cybercriminals can obtain lists of credentials from the Dark Web to use in attack methods like credential stuffing or password spraying attacks. Credential stuffing involves using lists of usernames and passwords from a data breach to access accounts on other sites. Password spraying involves using a single password across multiple accounts. The source of the data that cybercriminals use for these attacks is commonly found on the Dark Web or in underground hacking forums and thus requires an established level of access in these communities to be able to view this data.

What Happens When an Account Becomes Exposed?

The consequences of a hacker gaining unauthorized access to an account in an organization's environment can be severe. The hacker can steal sensitive data, including financial data, customer data, intellectual property, and confidential information about the organization. This can lead to financial losses, as the hacker can use the compromised account to carry out fraudulent activities, transfer money to their accounts, or make unauthorized purchases or transactions.

Reputational damage can result, and customer trust can be eroded if customer data or confidential information is stolen. In some industries, corporations are required to comply with regulations and laws related to data privacy and security, and failing to protect sensitive data can lead to regulatory fines and legal penalties. The hacker can also carry out attacks such as phishing, malware attacks, or ransomware attacks, leading to operational disruption and downtime. Compromised accounts can make impersonation and social engineering significantly more effective, and this serves as a springboard for sophisticated attacks that rely on privilege escalation or human error somewhere in the attack chain.

Often, the impact can be industry-specific and vary by the organization, depending on if they handle trade secrets, patents, or research and development data. It is critical for organizations to implement robust security measures to mitigate the risk of account compromise and the resulting consequences.

How to Prevent ATO Attacks?

To prevent ATO attacks, organizations can take several steps:

- Enforce Password Policies
  Organizations should enforce password policies that require unique passwords. This practice can reduce the effectiveness of password spraying and credential stuffing attacks. Adhering to a robust framework such as NIST 800-63b is one way to ensure a strong password policy.

- Monitor Credentials in Your Environment for Exposure on the Dark Web
  A password that is safe today may become compromised at any time. Regulatory frameworks, such as NIST, require organizations to monitor passwords for compromise and reset those that have been detected in a breach. Continuously monitoring and remediating when a password has been exposed greatly reduces the risk of ATO.

- Delete Unused Accounts
  When accounts are left inactive or unmonitored, they can become vulnerable to unauthorized access or misuse. Former employees may still have access, and these accounts can be targeted and compromised by hackers.

Conclusion

ATO attacks are a significant threat to organizations of all sizes. Attackers can use stolen credentials to gain access to sensitive information, leading to data breaches and reputational damage. To prevent ATO attacks, organizations should enforce password policies, monitor passwords for exposure in a data breach, and delete unused accounts. By implementing these measures, organizations can safeguard their confidential data and diminish the risk of security events.