Contents

Introduction

An account was compromised, leading to unauthorized access to one account of an M365 tenant. The hacker utilized this access to send bulk emails to a Gmail tenant. Upon discovery, the M365 admin created a support ticket, which was then assigned to me for resolution.

---

1. Issue/Problem Description

The affected mailbox had Multi-Factor Authentication (MFA) disabled, which provided an opportunity for the hacker to access the mailbox and misuse it for sending bulk emails to another Gmail tenant. The primary concern was how to effectively respond to and manage the situation.

---

2. User Affected/Scope

User Affected:

- The primary user affected was the owner of the compromised mailbox.

Scope:

- The scope of the impact extended to all individuals who received the unauthorized emails, potentially leading to a broader security incident.

---

3. Business Impact

Business Impact of Compromised Accounts:

1. **Email Service Disruption**: The misuse of the account for spam or phishing can trigger Microsoft's outbound spam controls, leading to account suspension or limitations.
2. **Sender Reputation Damage**: The mass emailing can damage the organization's domain reputation, causing future legitimate emails to be blocked or marked as spam by email providers.
3. **Regulatory and Compliance Violations**: Unauthorized disclosure of sensitive information can lead to breaches of data protection laws, resulting in legal consequences.
4. **Operational Costs**: Resources must be allocated for incident response, legal advice, and public relations to address the breach's fallout.
5. **Loss of Trust**: A breach can erode trust among customers and partners, affecting long-term business relations and retention.
6. **Security Risks**: The compromised account may be exploited for further attacks, escalating to a more significant security event.
7. **Preventative Measures**: It is critical to implement robust security protocols, including MFA and employee security awareness training, to prevent such incidents.

---

4. Troubleshooting Steps

I assisted the customer with the following steps to address the compromised account:

- Reset the user's password immediately.
- Re-enable MFA for the affected account.
- Block any further access to the account.
- Sign out of all active sessions to terminate unauthorized access.

---

5. Resolution and Recovery

- Conducted a message trace to track the sent emails.
- Identified the bulk emails in a “Getting status” or pending state.
- Advised the customer to instruct the recipient Gmail tenant to create a transport rule to block or delete emails originating from the compromised account.

---

6. Preventative Measures

To prevent similar incidents in the future, the following measures are recommended:

- Enforce MFA for all users without exception.
- Regularly review and update security protocols.
- Conduct frequent security training sessions for all employees.
- Implement advanced threat protection solutions like Microsoft Defender for Office 365.

---

7. Outcome After Troubleshooting

Following the implementation of the troubleshooting steps, the following outcomes were observed:

- **Password Reset and MFA Implementation**: The compromised account’s password was successfully reset, and Multi-Factor Authentication was enabled, preventing further unauthorized access.
- **Account Access Blocked**: All sessions associated with the compromised account were terminated, effectively blocking the hacker’s access.
- **Email Flow Restored**: The outbound spam filter temporarily blocked the account from sending emails, but after verifying the account’s security, the email flow was restored.

- **Message Trace and Email Status**: A message trace was conducted, revealing that the bulk emails sent to the Gmail tenant were in a "Getting status" or pending state. This allowed for quick action to be taken to mitigate the spread of the unauthorized emails.
- **Transport Rule Implementation**: The recipient Gmail tenant was advised to create a transport rule to block or delete emails originating from the compromised account, which was successfully implemented, preventing the spread of spam or phishing emails.
- **Incident Review and Documentation**: A thorough review of the incident was conducted, and all actions taken were documented to improve future response strategies.
- **Security Posture Strengthening**: The incident prompted a review of the organization's security measures, leading to the strengthening of policies and protocols to prevent similar occurrences in the future.