Acme MSP

[redacted]

Threat Remediation Report

Affected account:

[redacted]

[redacted]

January 26, 2025

Threat Remediation Report

[redacted]
January 26, 2025

Summary

Remediated

- An attacker gained access to [redacted]'s M365 account ([redacted]).
- The attacker added 1 inbox rule to the account, but Acme MSP has removed them.
- Acme MSP has taken care of the threat. No further action necessary.

The attacker had access to the account for **2 months, 11 days, 7 hours, and 31 minutes**.

Accessed	Sent	Modified	Deleted
50 emails	4 emails	4 emails	22 emails
0 documents	0 documents	0 documents	0 documents

Phishing Email

Removed from all inboxes

- [redacted] received a phishing email from [redacted].
- Acme MSP has removed the phishing email from all inboxes across the company

[redacted]

Phish

These emails typically come from trusted third parties who have been compromised.

Threat Remediation Report

[redacted]
January 26, 2025

Data Access

Acme MSP has completed a thorough analysis of the attacker's activity. Below is the data with which the attacker interacted.

Accessed

50 emails
0 documents

Sent

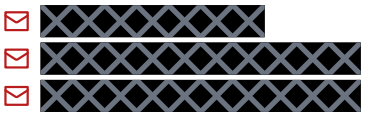
4 emails
0 documents

Modified

4 emails
0 documents

Deleted

22 emails
0 documents



Threat Remediation Report

[redacted]
January 26, 2025

Persistence

The attacker added 4 malicious persistence mechanisms to the account.

Malicious DKIM Signing Config Modified

1/24/2025, 10:57:27 PM
[redacted]

Added Malicious Recipient Permission

1/24/2025, 10:43:57 PM
[redacted]

Added Malicious Mailbox Permission

1/24/2025, 10:45:57 PM
[redacted]

Edited Malicious Inbox Rule Deleted

1/24/2025, 12:12:18 AM
[redacted]

Threat Remediation Report

[redacted]
January 26, 2025

Timeline

Timestamp	Attacker Action	Note
Jan 22 02:19:02 PM PST	Email: Read	-
Jan 22 02:19:54 PM PST	Login: Failed	[redacted]
Jan 22 02:20:13 PM PST	Login: Pending MFA Challenge	[redacted]
Jan 22 02:20:57 PM PST	Login: Successful	[redacted]
Jan 22 02:34:41 PM PST	Login: Successful	[redacted]
8 attacker actions omitted (1 email access, logged in 5 times)		
Jan 22 02:37:46 PM PST	Email: Read	-
1 attacker action omitted (logged in 1 time)		
Jan 22 04:29:26 PM PST	Email: Read	-
Jan 22 04:34:35 PM PST	Email: Read	-
Jan 22 04:34:35 PM PST	Email: Updated	-
Jan 22 04:36:01 PM PST	Email: Read	-
Jan 22 04:36:01 PM PST	Email: Updated	-
Jan 22 04:38:55 PM PST	Email: Read	-
Jan 22 04:39:12 PM PST	Email: Updated	-
21 attacker actions omitted (18 email accesses, logged in 2 times, attempted login unsuccessfully 1 time)		
Jan 23 02:51:25 PM PST	Login: Successful	[redacted]
15 attacker actions omitted (2 email accesses, logged in 7 times, attempted login unsuccessfully 6 times)		
Jan 23 03:53:28 PM PST	Login: Successful	[redacted]
35 attacker actions omitted (19 email accesses, logged in 14 times, attempted login unsuccessfully 1 time)		
Jan 23 04:34:19 PM PST	Email: Read	-
Jan 23 04:36:13 PM PST	Login: Successful	[redacted]
Jan 23 04:36:26 PM PST	Email: Read	-
Jan 23 04:36:55 PM PST	Email: Read	-
457 attacker actions omitted (sent 4 emails, 325 email accesses, logged in 39 times, attempted login unsuccessfully 51 times)		
Apr 4 07:57:45 PM PDT	Email: Read	-

Frequently Asked Questions

Why does it matter that the attacker sent emails from the compromised account?

Emails sent from a legitimate, compromised account appear trustworthy. Recipients—employees, vendors, or customers—are far more likely to open attachments, click links, or follow instructions when they come from a familiar address. This trust lets attackers spread malware, steal credentials, or trick people into wiring money to fraudulent accounts.

Why does it matter that the attacker accessed information?

Even reading internal emails or files gives attackers valuable intelligence. The attacker can learn who approves payments, what invoices look like, and how people communicate. That knowledge allows them to craft highly convincing fake requests or target other employees for further compromise.

Why does it matter that the attacker changed account settings?

Attackers often update mailbox rules, forwarding settings, or recovery emails to maintain access. These silent changes can let them keep monitoring or stealing messages even after passwords are reset—prolonging the breach and making cleanup more difficult.

Why does it matter that the attacker logged in from new locations or devices?

Unusual logins may indicate the attacker is using stolen credentials remotely. Even if the attacker doesn't take obvious actions right away, maintaining access from an unfamiliar location allows them to observe, plan, and strike later—making early detection and response critical.

What is the risk if the attacker only viewed contacts or email threads?

Even without sending messages, attackers can map your organization's relationships. The attacker can learn who controls finances, who approves invoices, and how teams communicate. This information helps them design targeted social engineering attacks—either immediately or in future campaigns against your business or partners.

Why might an attacker sit and wait in an account?

Sometimes attackers maintain access to the account as a backdoor for later use. The attacker may monitor communications, steal new credentials, or sell the access to another criminal group. The absence of obvious damage doesn't mean the risk is gone—it often means the attacker is biding their time and collecting information.

Frequently Asked Questions

What is an Account Compromise?

An Account Compromise occurs when an attacker gains access to an employee account. Often, this occurs via phishing, and often bypasses MFA. An attacker will seek control of an account in order to execute financial fraud (e.g. updating incoming/outgoing invoices with the attacker's bank account information) or to use your organization as a reputational foothold, phishing other companies from your domain.

What was the attacker's intention?

The attacker's goal is often financial gain or data theft. Some typical objectives:

1. Send invoice frauds or payment requests from the compromised account to trick customers or vendors into wiring money to attacker-controlled bank accounts.
2. Use the breached email to request wire transfers or change payment instructions.
3. Harvest sensitive information (contracts, financial statements, HR data) for extortion or resale.
4. Use the account as a foothold to move laterally in your network, infect systems, or impersonate trusted contacts.

Why is this dangerous?

Strong trust erosion: Because the attack comes from inside an account that looks legitimate, recipients (employees, customers, partners) are more likely to trust and act on malicious requests.

1. Hard to detect: Because the login looks valid (with MFA approval), most monitoring tools won't flag it.
2. Financial losses: Companies have lost millions in BEC scams where fraudulent wires were authorized under "trusted" credentials.
3. Data exposure & reputational damage: Leaked internal communications, breaches of customer or employee private data, and damage to your business's reputation can follow.
4. Pivoting risks: Once inside, attackers can expand access, e.g. taking over additional accounts, installing malware, or gaining domain admin privileges.

How do we stop this?

We continuously monitor Microsoft 365 logs to detect suspicious logins and unusual access to email, SharePoint, and Teams that may indicate account compromise. When a compromise is detected, often involving a phishing message that has bypassed other security controls, we proactively identify and remove the malicious email from all user mailboxes. This rapid response prevents a broader, tenant-wide incident, and minimizes both business disruption and organizational risk.