Curveball Solutions

Acme Corp.

Threat Remediation Report

Affected account:

Asha Streich (Financial Director)

asha.streich@acmecorp.com

January 20, 2026

Contact us: james.bowyer@curveballsolutions.com

Threat Remediation

Asha Streich (Financial Director)
January 20, 2026

Summary

Remediated

- The user was phished by an email titled '[EXTERNAL] Brad Smith shared "ConEd LLC Due Pay Application" with you'.
- The attacker used an Attacker-in-the-Middle (AiTM) technique to send the user to a fake sign-in portal, where they entered their credentials and MFA code.
- An attacker gained access to Asha Streich's M365 account (asha.streich@acmecorp.com).
- The attacker created an inbox rule to hide malicious activity from the user, but Curveball Solutions has removed it.
- The attacker added a malicious application to this account, allowing them to read emails, send messages, and access data without the user's knowledge, but Curveball Solutions has removed it.
- **Curveball Solutions successfully discovered and removed the attacker** from Asha Streich's M365 account.
- **Curveball Solutions has taken care of the threat. No further action necessary.**

The attacker had access to the account for **4 minutes**. Microsoft logging was delayed by **3 minutes**. The attack was caught **48 seconds** after Microsoft published audit logs, and was contained **1 minute** later.

Accessed	Sent	Modified	Deleted
1 email	0 emails	0 emails	0 emails
2 documents	0 documents	0 documents	0 documents

Phishing Email

Removed from all inboxes

- Asha Streich (Financial Director) received a phishing email from brad.smith@conedaccting.com.
- The phish was also sent to henry.braun@acmecorp.com and holly.connelly@acmecorp.com.
- **Curveball Solutions has removed the phishing email from all inboxes across Acme Corp., preventing 2 further compromises.**

Brad Smith
brad.smith@conedaccting.com

Phish

[EXTERNAL] Brad Smith shared "ConEd LLC Due Pay Application" with you

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

Threat Remediation

Asha Streich (Financial Director)
January 20, 2026

Timeline

Timestamp	Attacker Action	Note
Jan 20 12:29:21 PM GMT	Login: Pending MFA Challenge	Attempted login to: officehome
Jan 20 12:29:51 PM GMT	Login: Successful	Logged into: officehome
Jan 20 12:30:41 PM GMT	Login: Successful	Logged into: officehome
Jan 20 12:31:12 PM GMT	Login: Successful	Logged into: office 365 exchange online
Jan 20 12:31:40 PM GMT	Email: New Inbox Rule	-
Jan 20 12:31:41 PM GMT	File: File Accessed	Attacker target: "/Shared Documents/HR/Policies/Employee-Handbook-2026.pdf"
Jan 20 12:32:10 PM GMT	App: Registered em client	-
Jan 20 12:32:45 PM GMT	File: File Accessed	Attacker target: "/Shared Documents/HR/Policies/PTO-Policy-2026.pdf"
Jan 20 12:32:54 PM GMT	Email: Read	Attacker target: "[EXTERNAL] RE: Fairway PO P124 - Initial Mailbox Order"
Jan 20 12:33:15 PM GMT	Curveball Solutions: Flagged Attacker Activity	-
Jan 20 12:34:20 PM GMT	Curveball Solutions: Killed current sessions	-
Jan 20 12:34:20 PM GMT	Curveball Solutions: Locked account	-
Jan 20 12:34:20 PM GMT	Curveball Solutions: Disabled Inbox Rule	-
Jan 20 12:34:20 PM GMT	Curveball Solutions: Disabled App Registration	-
Jan 20 12:35:16 PM GMT	Login: Failed	Attempted login to: office 365 exchange online
Jan 20 12:40:04 PM GMT	Login: Failed	Attempted login to: office 365 exchange online
Jan 21 11:59:44 PM GMT	Login: Failed	Attempted login to: officehome
Jan 22 12:00:00 AM GMT	Login: Failed	Attempted login to: officehome

Persistence

The attacker added 2 malicious persistence mechanisms to the account.

Curveball Solutions removed all of the malicious persistent rules and registrations.

Malicious App Registration

Disabled ✓ Curveball Solutions, Jan 20, 12:34 PM

1/20/2026, 12:32:10 PM

App Name: em client

App ID: e9a7fea1-1cc0-4cd9-a31b-9137ca5deedd

Service Principal ID: 6891ea7e-6992-4ad5-ab0d-fdc9ca3e0f55

New Malicious Inbox Rule

Disabled ✓ Curveball Solutions, Jan 20, 12:34 PM

1/20/2026, 12:31:40 PM

Display Name: .

Conditions:

> **Sender contains**: @conedaccting.com

Actions:

> **Move to folder**: Deleted Items

Exceptions:

No exceptions

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.