Threat Remediation Report

Asha Streich (Financial Director)
January 20, 2025

Summary

Remediated

- An attacker gained access to Asha Streich's M365 account (asha.streich@acmecorp.com).
- **Acme MSP successfully discovered and removed the attacker** from Asha Streich's M365 account.
- The attacker added 1 inbox rule and 1 app registration 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 **4 minutes**. Microsoft logging was delayed by **3 minutes**. The attack was caught **48 seconds** after Microsoft published audit logs, and was contained **5 seconds** later.

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

Phishing Email

Removed from all inboxes

- Asha Streich (Financial Director) received a phishing email from brad.smith@conedaccting.com on 1/20/2025.
- The phish was also sent to henry.braun@acmecorp.com and holly.connelly@acmecorp.com.
- **Acme MSP has removed the phishing email from all inboxes across Acme Corp.**

Brad Smith
brad.smith@conedaccting.com

1/20/2025, 11:39:47 AM Phish

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

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

Analyst Note

Malicious login to officehome from IP in Phoenix, Arizona belonging to "global internet solutions llc". The real user typically logs in from New York.

Signals Used for Detection

- Datacenter IP
- Suspicious Proxy Use
- Accessed Mail with Financial Docs
- Inbox Rule Activity
- Malicious App: EM Client
- Rapid Browser Switching

Threat Remediation Report

Asha Streich (Financial Director)
January 20, 2025

Timeline

Timestamp	Attacker Action	Note
Jan 20 12:28:26 PM	Login: Pending MFA Challenge	Unsuccessful, came from Phoenix, AZ. Attempted login to: officehome
Jan 20 12:28:47 PM	Login: Successful	First successful login, came from Phoenix, AZ. Logged into: officehome
Jan 20 12:29:21 PM	Login: Pending MFA Challenge	Attempted login to: officehome
Jan 20 12:29:51 PM	Login: Successful	Logged into: officehome
Jan 20 12:30:32 PM	Login: Successful	Attacker pivoted network, now coming from a proxy IP in Dallas, TX. Logged into: officehome
2 attacker actions omitted (logged in 2 times)		
Jan 20 12:30:54 PM	File: File Previewed	Attacker target: "Documents/Desktop/Urgent/Amenities - Work Tracker/acme rpr - amenity progress tracker - 12.14.2024.xlsx"
1 attacker action omitted (logged in 1 time)		
Jan 20 12:31:40 PM	Email: New Inbox Rule	-
Jan 20 12:32:10 PM	App: Registered em client	-
Jan 20 12:32:54 PM	Email: Read	Attacker target: "[EXTERNAL] RE: Fairway PO P124 - Initial Mailbox Order"
Jan 20 12:33:15 PM	Acme MSP: Flagged Attacker Activity	-
Jan 20 12:33:20 PM	Acme MSP: Killed current sessions	-
Jan 20 12:33:20 PM	Acme MSP: Locked account	-
Jan 20 12:33:20 PM	Acme MSP: Disabled Mail Filter Rule	-
Jan 20 12:33:20 PM	Acme MSP: Disabled App Registration	-
Jan 20 12:35:16 PM	Login: Failed	Attempted login to: office 365 exchange online
Jan 20 12:40:04 PM	Login: Failed	Attacker tried to log in again but failed, came from a proxy IP in Dallas, TX. Attempted login to: office 365 exchange online
Jan 21 11:59:44 PM	Login: Failed	Attacker tried to log in again but failed, came from a proxy IP in Dallas, TX. Attempted login to: officehome
Jan 22 12:00:00 AM	Login: Failed	Attacker tried to log in again but failed, came from Red Chute, LA. Attempted login to: officehome

Threat Remediation Report

Asha Streich (Financial Director)
January 20, 2025

Background

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.