Acme Corp.

# Scan Report

| | |
|---|---|
| **Reporting Period:** | January 5, 2025 - February 8, 2025 |
| **Prepared by:** | Curveball Solutions |
| **Contact:** | james.bowyer@curveballsolutions.com |

# Why M365 protection matters

## 90%

of breaches worldwide are caused by phishing. (2023)

## 29%

identity-based attacks result in wire fraud. (2024)

**Automation means everyone is targeted.** Even organizations with less than 1,000 employees have a 70% chance of getting 1 BEC attack attempt per week.

**These attacks get past spam filters.** Often, an attacker hacks a trusted colleague and weaponizes their account. (e.g. Brad Smith shared document with you.)

## £35 billion

lost over the last decade due to business email compromise (BEC), making it the costliest cybercrime. (2013-2023)

## £96,000

is the average cost per incident involving wire fraud. (2023)

**These attacks get past MFA.** There was a 146% increase in MFA-bypass phishing attacks in 2024. Now, 75% of BEC attacks bypass MFA. (Here's how)

# What Threat Hunting Did We Perform?

Curveball Solutions gathered and analyzed the last 6 months of activity (2,363,245 logs) in Acme Corp.'s M365 environment.

- From Entra, Exchange, SharePoint, OneDrive, Teams, and more.

Curveball Solutions then carefully threat hunted for attacker patterns.

- First, Curveball Solutions analyzed classic signals like impossible travel and proxy use.
- Then, Curveball Solutions built a behavioral baseline for Acme Corp. and analyzed sophisticated attacker signals.

Curveball Solutions uses this same analytical engine to stop M365 attacks in real-time. By finding a historical attack, we know we can stop it in real-time.

# We found an active attacker in your environment.

No active monitoring was in place.
Add monitoring to prevent future damage.

| | |
|---|---|
| Account: | Nick Renner |
| Time to detection: | 2 days |

Notes:

- Dwell Time: 2 days
- Caused by Phishing
- AiTM (Attacker in the Middle)
- Sensitive Data Accessed
- Sent Out Emails
- Used Inbox Rules
- Abused Delegated Permissions
- Past Incident

The attacker had access for 2 days and 25 minutes.

The attacker sent 4 malicious emails from your environment.

The attacker accessed 50 emails, including 134 sensitive emails such as "Your New Invoice Is Available Online.".

The attacker accessed a sensitive file, including one named "-Wire-Transfer-Form-Template.docx".

The attacker bypassed MFA and logged in from an IP address in New York, NY (see how).

The user was phished by a malicious email titled "Amended acme corp employee handbook" that bypassed email protection.

# We found 2 confirmed compromises in the last 6 months

In one case, the attacker remained undetected for **1 day, 7 hours, and 58 minutes.**

| Account | Attacker Active For | Preview of Harm | |
|---|---|---|---|
| Anakin Skywalker | 1 day | Financial Risk, Data Theft, Reputational Harm | Attacker accessed 8 financial records, including "Invoice and PO Confirmation for March Services".<br><br>Attacker then sent a malicious email. |
| Nick Renner | 2 days | Financial Risk, Data Theft, Reputational Harm | Attacker accessed 10 financial records, including "Invoice Reminder Notice from Aurora Billing Services".<br><br>Attacker then sent 4 malicious emails. |

# We found an attack caught late

We analyzed 6 months of activity in your Microsoft environment.
We found an attacker who remained in the account for **1 day, 7 hours, and 58 minutes.**

| Emails exposed: | Potentially sensitive exposed: | Malicious emails sent: |
|---|---|---|
| 29 | 26 | 1 |

| Account | Time to Detection | Notes |
|---|---|---|
| Anakin Skywalker | 1 day | Dwell Time: 1 day & 7 hours<br>AiTM (Attacker in the Middle)<br>Sensitive Data Accessed<br>Sent Out Emails<br>Used Inbox Rules<br>Past Incident |

## What the attacker did:

- Attacker gained access on February 4th, 2026. Retained access for 1 day.
- Attacker added a malicious inbox rule with capability to hide emails.
- Attacker accessed 29 emails, including:
  - "Invoice and PO Confirmation for March Se..."
  - "ACH Remittance Advice - Payment ID #2389..."
  - "ACH Remittance Advice - Payment ID #2389..."
  - "ACH Remittance Advice - Payment ID #2389..."
- Attacker sent a malicious email, including:
  - "Re: test"
- Attacker accessed a potentially sensitive file:
  - "Invoice-NabooGardens-Feb2026.pdf"

# What should have happened?

| Time (UTC) | Attacker Action | |
|---|---|---|
| Feb 4 08:30 PM | @ Failed login (Buffalo, NY) | |
| Feb 4 08:32 PM | Attacker logged in · MFA bypassed | |
| Feb 4 08:32 PM | Attacker login triggers behavioral detection | Attacker locked out |
| ~~Feb 4 08:32 PM~~ | ~~Attacker pivoted to new IP (Buffalo, NY)~~ | Attacker locked out |
| ~~Feb 4 09:53 PM~~ | ~~Accessed: ACH Remittance Advice - Payment ID #2389...~~ | Attacker locked out |
| ~~Feb 4 10:02 PM~~ | ~~Accessed: Invoice and PO Confirmation for March Se...~~ | Attacker locked out |
| ~~Feb 5 12:21 PM~~ | ~~Accessed: Wire Transfer Confirmation - Account End...~~ | Attacker locked out |
| ~~Feb 5 03:23 PM~~ | ~~Accessed: Billing Summary and Payment Schedule - A...~~ | Attacker locked out |
| ~~Feb 5 03:36 PM~~ | ~~Accessed: 2024 Year-End Tax Summary - Action Requi...~~ | Attacker locked out |

## Curveball Solutions detects & blocks these attacks:

- ✓ Attack blocked at initial access
- ✓ Attack blocked **before** emails accessed
- ✓ Attack blocked **before** reputational harm
- ✓ Attack blocked **before** files accessed

# With Curveball Solutions, you can stop this from happening again.

With Curveball Solutions as your trusted cyber partner, you can prevent:

| | |
|---|---|
| Financial Risk | Prevent attackers from **stealing invoice details** and **sending malicious financial requests** to clients. |
| Reputational Harm | Like the **5 malicious emails** sent to contacts. |
| Data Theft | Like the **79 emails** stolen by attackers. |

james.bowyer@curveballsolutions.com

Active monitoring is already in place. We can keep this protection live.

↓

We baseline to employee behavior. No business disruption.

↓

Stop Account Compromises before attackers can cause harm.