Post Incident Review – Account Compromise:

Category: Security Threat
Subcategory: Phishing/ AiTM Session Hijack / MFA Bypass
User: darrell.hayashi@purolator.com
Date Range: Feb 26 - Feb 27, 2026
Status: Resolved
Severity Level: High
Reference: INC0286154

1. Incident Summary

On February 26, 2026, a Purolator employee received a phishing email impersonating a known external contact at Teamsters Canada. The email contained a link to a fraudulent Microsoft login portal operated via the EvilProxy AiTM framework. The user completed what appeared to be a legitimate login, during which the attacker silently captured the authenticated session cookie, bypassing MFA entirely. The attacker gained unauthorized access to the user's Office 365 mailbox for approximately 29 hours, accessed 36 emails, created a malicious inbox rule to conceal activity, and conducted reconnaissance of sensitive internal correspondence including legal, financial, and HR-related emails. The account was fully contained on February 28. A thorough email exposure review was completed on March 2, and findings were shared with Legal for risk assessment.

2. Initial Vector

On Feb 26 at 1:14 PM EST, the user received a phishing email in his Purolator inbox appearing to originate from Andrée Bélanger at abelanger@teamsters.ca - a known external contact at Teamsters Canada. The email was styled as a SharePoint document-sharing notification, stating that a protected document had been shared and prompting the user to click "Open Message Here." The email passed Proofpoint's inbound filters as the sending domain had a legitimate DKIM and SPF record at the time of delivery, which contributed to it being permitted.

The embedded link directed the user to a fraudulent website hosted at afnagro.com/office/microsoftportalsecured.html, designed to mimic a Microsoft login portal. This page was operated as an AiTM (Adversary-in-the-Middle) reverse proxy using the EvilProxy framework, confirmed by Okta threat intelligence on source IP 64.23.238.66 (DigitalOcean LLC, domain: cloudwaysapps.com). The proxy relayed the user's credentials and MFA challenge to the real Microsoft/Okta service in real time - the user completed the login flow believing it was legitimate - after which the attacker silently captured the authenticated session cookie, bypassing MFA entirely.

Okta logs recorded a high-risk sign-on policy evaluation at 1:16 PM EST from Santa Clara, CA, flagging: new country, new city, new ASN, new IP, and anomalous device - all within two minutes of the phishing link being clicked.

3. Attack Timeline

- Feb 26, 1:14 PM EST - Phishing email received and URL clicked by user from Toronto, ON. URL permitted by Proofpoint. Attacker captured session cookie via EvilProxy reverse proxy.
- Feb 26, 1:16-1:39 PM EST - Multiple successful logins to Okta and Office 365 from US-CA (Santa Clara). Attacker established persistent access using the hijacked session cookie.
- Feb 26, 3:11-3:12 PM EST - Attacker pivoted to a second IP from US-TX (Dallas). Bulk mailbox access began. A malicious inbox rule was created to automatically move emails from @teamsters.ca to Deleted Items, likely to conceal labour/legal correspondence from the user.
- Feb 27, 8:16 AM - 5:22 PM EST - Continued logins and mailbox access from Dallas, TX. Emails accessed included invoice approval threads, compensation-related emails, and legal correspondence. A total of 20 suspicious login events (15 successful, 5 failed) and 58 message access events were recorded across both days.

4. Containment/Resolution Actions

- Feb 27, approx. 6:52 PM EST - Azure AD and Okta sessions revoked by Keshava through RedX following an Okta alert. Note: SecOps was not on the original alert thread, resulting in a delayed coordinated response.
- Feb 27 - Account suspended in Okta. No password reset applied at this stage
- Feb 28, 12:23 PM EST - Okta password reset issued, temporary password provided to user.
- Feb 28 – Additional containment actions completed:
    - MFA factors audited in Okta, nothing suspicious found.
    - Endpoint PCL-2MQ5350W7Y reviewed in CrowdStrike, no detections found.
    - Incident ticket created and verification email sent to end user.

5. Eradication & Recovery

- Feb 28 - Okta account unsuspended following password reset and MFA audit confirmation.
- Feb 28 - Security analyst connected with user via call. Malicious inbox rule (@teamsters.ca to Deleted Items) identified and removed directly from the user's Outlook. Account access fully restored.
- Feb 28 - Attacker IPs 64.23.238.66 and 64.227.206.14 flagged as IOCs and submitted for blocking.
- Mar 2 - Security analyst conducted a 1-on-1 review with the user covering all 36 emails accessed during the compromise window. 15 of 36 were identified as containing sensitive or classified information. User confirmed the nature of each email at a high level without disclosing full content. Findings documented and shared with Legal and Privacy team for risk assessment and determination of required notifications.

6. Email Exposure Summary

Of the 36 unique emails accessed by the attacker, 15 were identified as sensitive. Categories included: limited PII with invoice details, personal compensation information, CBI shared broadly across the organization, external legal correspondence and active case information, external council billing, and PII including medical information. Three emails were personal to the user and excluded from the legal review. The remaining 12 were shared with the Privacy and Legal team for assessment and determination of any required notifications.

7. Lessons Learned

- Alert coverage gap: SecOps was not included on the original Okta alert email that triggered the initial response, resulting in a delayed coordinated containment. A formal on-call process and alert routing review is required to prevent recurrence.
- Containment scope: When an account is suspended in Okta, future containment steps must include an immediate password reset alongside session revocation and account suspension to fully cut off access.
- AiTM detection-to-response time: The time between the initial phishing click (Feb 26, 1:14 PM) and full containment (Feb 27, 6:52 PM) was approximately 29 hours. Faster automated detection and response for AiTM-classified alerts in Proofpoint would significantly reduce the window of exposure.
- Inbox rule as an indicator: The creation of a mailbox obfuscation rule shortly after attacker access is a strong persistence and concealment indicator. Monitoring for new inbox rule creation events should be incorporated as a detection rule going forward.
- Phishing URL permitted: The initial phishing URL was permitted by Proofpoint at time of click due to the sending domain passing DKIM and SPF validation. This suggests the sender's account (abelanger@teamsters.ca) may itself have been compromised and used as a delivery vehicle. AiTM-specific URL detection improvements in Proofpoint are needed to catch these earlier in the kill chain.

8. Post-Incident Actions

- SIEM migration: Migrating to an enhanced SIEM platform with a new vendor targeted for Q2, to improve detection coverage and response capabilities across the environment.
- Proofpoint alerting: Tightening alert processes in Proofpoint, with a specific focus on AiTM detections to accelerate containment timelines and reduce time-to-respond.
- User awareness: Security awareness communication sent to all Purolator employees covering AiTM phishing and ClickFix attack techniques. Affected user and relevant individuals added to targeted security training on ZenGuide.
- On-call process: Formalising the on-call methodology to ensure SecOps is always included on critical alerts, regardless of the originating platform or alert thread.

- Email exposure review: Completed review of all emails accessed during the compromise window. Sensitive emails identified and findings shared with Legal and Privacy team for risk assessment and determination of any required notifications.

Appendix: IOCs

- 64.23.238.66 - DigitalOcean LLC / cloudwaysapps.com (EvilProxy AiTM framework)
- 64.227.206.14 - Perimeter 81 LLC
- afnagro.com/office/microsoftportalsecured.html - Fraudulent login portal
- Mailbox Rule: @teamsters.ca emails auto-moved to Deleted Items
- MITRE T1539 - Steal Web Session Cookie
- MITRE T1114.002 - Remote Email Collection

Document prepared by: Jasraj Johal | Security Analyst | Purolator

Date: March 5, 2026

Distribution: Internal Security Team, CISO