"Payroll Pirate" Campaign: AiTM Session Hijacking and Microsoft Graph Reconnaissance Across Multiple Client Environments

June 11th, 2026

Attack Type	Adversary-in-the-Middle (AiTM) session theft and token replay, Microsoft Graph API directory reconnaissance, and business email compromise (BEC) targeting payroll redirection. No malware or endpoint footprint.
Targeting	Payroll, HR, finance, and administrative personnel. Microsoft reporting documents geographic targeting of Canadian employees via SEO poisoning and malvertising. SRA observed activity in healthcare, food services, and manufacturing client environments.
SRA Observed Activity	Suspicious Exchange Online Graph Reconnaissance Activity. Compromised accounts observed across various clients with ongoing activity and investigation.
Impact	Bulk directory enumeration of payroll and HR personnel, MFA bypass through replay of stolen session tokens.

Executive Summary

SRA identified an active "Payroll Pirate" intrusion campaign across multiple monitored client environments. The activity appears to align with campaigns Microsoft attributes to Storm-2755 and the related cluster Storm-2657. The actor steals authenticated Microsoft 365 sessions through AiTM techniques, replays the stolen tokens to bypass MFA, enumerates the directory through the Microsoft Graph API to identify payroll and HR personnel, and ultimately redirects employee salary payments by social engineering HR staff or by directly modifying banking details in HR SaaS platforms such as Workday.

The Graph reconnaissance queries observed in each environment were nearly identical, targeting users whose attributes match keywords such as payroll, pay, hr, human, resources, support, info, finance, account, and admin, paired with $top=999 and $skiptoken pagination for bulk harvesting. Access tokens observed in the Graph activity matched tokens previously issued to legitimate user sign-ins, confirming session theft and token replay rather than credential compromise alone.

The attack chain is identity- and cloud-based, so detection depends on Microsoft Entra sign-in telemetry and Microsoft Graph activity logs rather than endpoint EDR. Based on this activity, SRA recommends that clients enable Microsoft Graph activity logging and ship those logs to ADX to provide visibility into the reconnaissance stage of this campaign.

Activity Observed in SRA-Monitored Environments

Multiple SRA clients were observed to be impacted by this threat. The following activity was common across compromised environments:

- **Initial failed authentications.** Compromised users first generated failed OfficeHome sign-ins with ResultType 90014 (a required credential field was missing), an authentication step detail of MFA requirement skipped due to remembered device, and an iOS source operating system. These attempts originated from seemingly random US mobile carrier IP space (AT&T, Verizon, T-Mobile).

- **Account takeover sequence.** An interactive sign-in to Microsoft Outlook with error code 50199 (Login:reprocess) was immediately followed by a Cmsi:cmsi interactive sign-in, both from user-agent Firefox 142.0 on Windows. Within 30 seconds, a non-interactive OAuth2:Token sign-in requested a Microsoft Graph token, with the user-agent shifting to Firefox 131.0.

- **Token replay characteristics.** The Graph token requests presented as nonInteractiveUser logons from unmanaged, device-less sessions claiming multiFactorAuthentication, and carried the same UniqueTokenIdentifier values later observed in the Graph API enumeration.

- **Graph reconnaissance.** Enumeration began with a bulk pull of /v1.0/users?$top=999, followed by OR-chained $search queries across displayName, givenName, surname, jobTitle, mail, and userPrincipalName for payroll and HR keywords, paginated with $skiptoken.

- **Infrastructure split.** Graph enumeration traffic originated primarily from Canadian residential ISP space (Videotron, Rogers, TELUS, Bell, Shaw), while initial authentication attempts came from US mobile carriers. This split is consistent with residential proxy infrastructure.

- **Broad delegated scopes.** Tokens used in the enumeration carried extensive delegated permissions, including Directory.Read.All, Files.ReadWrite.All, Group.ReadWrite.All, Chat.ReadWrite, and User.ReadWrite, giving the actor wide latitude beyond directory reads.

- **Persistent token-based access**. Unremediated users continue to generate non-interactive sign-ins to Office 365 Exchange Online approximately every three hours, using the Firefox 131.0 user-agent, originating from IPs across multiple US states, and presenting a new token identifier with each occurrence.

Safeguards/Recommendations

- **Phishing-Resistant MFA and Conditional Access Enforcement:** Deploy FIDO2/passkeys, Windows Hello for Business, or Certificate-Based Authentication, then enforce them through Conditional Access authentication strength policies for employees and external users accessing critical applications. Enabling phishing-resistant methods without enforcement allows attackers to force victims down to weaker authentication paths during the phishing flow.

- **Enable Microsoft Graph activity logs and ship them to a SIEM or Security Datalake.** Graph audit telemetry detected this campaign and is the only data source covering the directory

reconnaissance stage. SRA is coordinating onboarding instructions for monitored clients.

- **Remediate compromised accounts fully.** Revoke all active sessions and refresh tokens via the Entra Admin Center or M365 Admin Center (not the Azure Portal), reset credentials, re-register MFA methods, remove malicious inbox rules, review application consent grants, and revert any payroll or banking changes. Application consent grants deserve particular scrutiny. The broad delegated scopes observed in this activity raise the possibility of OAuth-based persistence through a consented application, which survives password resets, token revocation, and MFA re-registration entirely. Audit enterprise applications and consent grants for anything added or modified during the compromise window.

- **Harden session controls.** Enforce Conditional Access requiring compliant or hybrid-joined devices, enable continuous access evaluation (CAE) to revoke tokens when risk conditions change, and apply sign-in frequency controls to limit replayed session lifetime.

- **Alert on suspicious inbox rule creation.** Rules that delete or hide messages matching direct deposit, bank, or payroll keywords are a high-fidelity signal of payroll fraud staging.

- **Monitor HR SaaS platforms.** Connect Workday (or equivalent) to Microsoft Defender for Cloud Apps and alert on payment election changes, account changes, and new MFA device enrollments.

- SRA published related research on AiTM session theft in Defending and Threat Hunting AiTM Phishing, which can be leveraged to harden against this campaign and similar token-replay activity.

Indicators of Compromise

Indicator	Type
axios/1.7.9	User-agent
Firefox 131.0 (rv:131.0)	User-agent
Firefox 142.0 (rv:142.0)	User-agent
216.247.226[.]32	IPv4
24.53.42[.]79	IPv4
99.239.33[.]130	IPv4
75.152.86[.]244	IPv4
144.172.190[.]50	IPv4
72.143.216[.]88	IPv4

173.178.178[.]139	IPv4
216.16.184[.]145	IPv4
108.208.40[.]144	IPv4
70.83.127[.]83	IPv4
24.202.0[.]56	IPv4
72.45.107[.]194	IPv4
47.55.96[.]251	IPv4
70.24.235[.]36	IPv4
199.126.64[.]61	IPv4
70.67.169[.]118	IPv4
99.244.137[.]184	IPv4

References

- **Investigating Storm-2755: “Payroll pirate” attacks targeting Canadian employees**
- **Investigating targeted “payroll pirate” attacks affecting US universities**
- **Investigating OAuth App Abuse with the Graph Activity Log**
- **Microsoft Entra authentication and authorization error codes**
- **Defending and Hunting AiTM Attacks - Security Risk Advisors**