Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

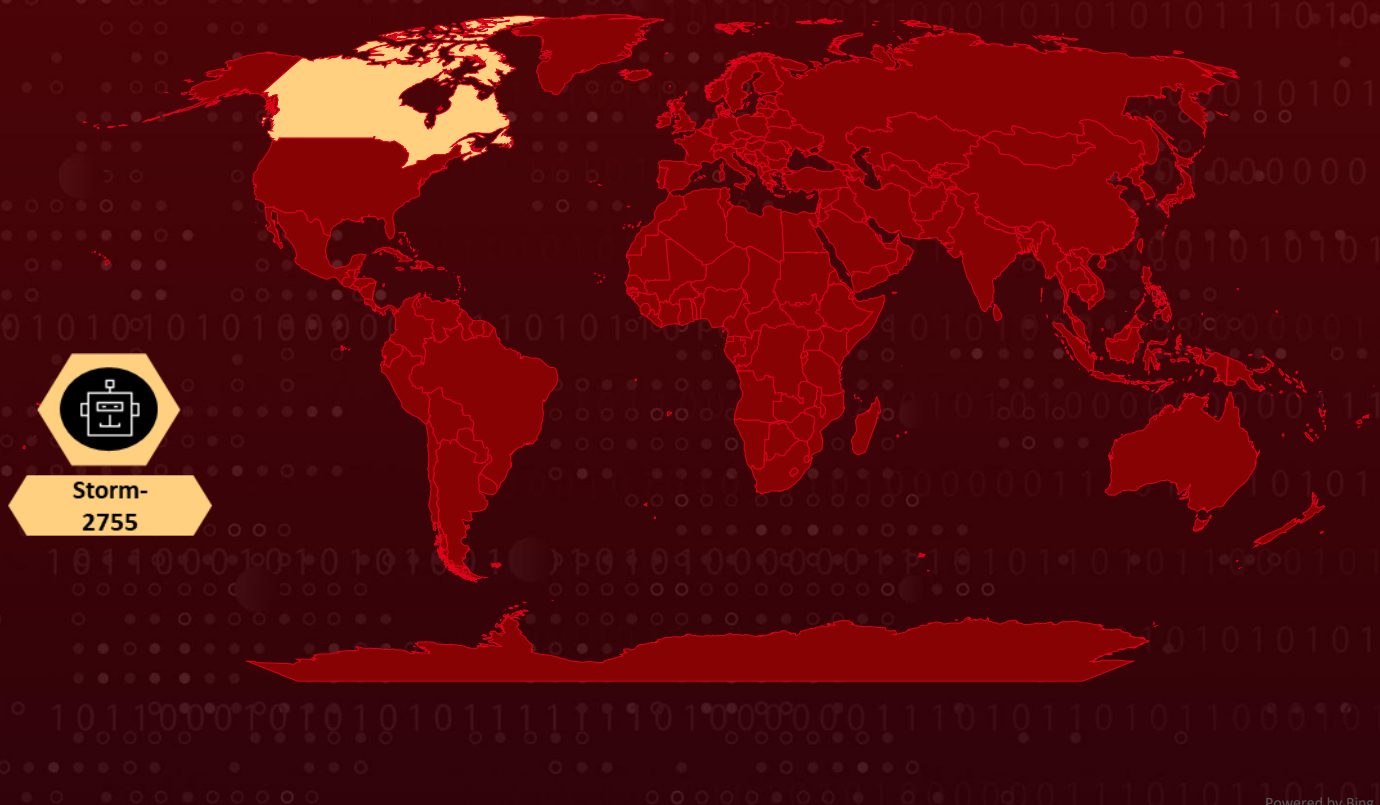
Storm-2755's Silent Payroll Heist Targeting Canada

Date of Publication	Admiralty Code	TA Number
April 15, 2026	A1	TA2026101

Summary

First Seen: April 2026
Targeted Region: Canada
Targeted Platforms: Microsoft 365, Microsoft Entra ID
Threat Actor: Storm-2755
Attack: Storm-2755 is a sophisticated, financially motivated cyber threat that targets employees through fake Microsoft 365 login pages pushed via search manipulation and malicious ads, capturing session tokens to bypass multi-factor authentication and gain silent access to corporate accounts. Once inside, it hides activity, scans for payroll and HR data, and manipulates inboxes to avoid detection before executing its core objective, tricking HR teams or directly altering systems like Workday to reroute salary payments into attacker-controlled accounts, resulting in real financial loss while remaining largely undetected.

Attack Regions



CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-27152	Axios SSRF and Credential Leakage Vulnerability	Axios version before 1.8.2	✗	✗	✓

Attack Details

#1

Storm-2755 is a financially driven threat group targeting employees in Canada. Its goal is simple to redirect salaries by taking control of workplace accounts. The attack begins with search manipulation and malicious ads that push fake Microsoft 365 login pages to the top of search results. These pages look legitimate but are controlled by the attacker.

#2

When a victim signs in, the attacker silently intercepts the entire login process. Instead of just stealing usernames and passwords, Storm-2755 captures active session tokens, allowing it to bypass standard multi-factor authentication. Storm-2755 exploits CVE-2025-27152's absolute URL bypass in Axios 1.7.9 to relay stolen session tokens and OAuth cookies from the AiTM phishing proxy to Microsoft 365 infrastructure, enabling authenticated session replay that bypasses non-phishing-resistant MFA.

#3

Once inside, the attacker avoids using malware and instead relies on the stolen session to remain undetected. Access is quietly maintained by repeatedly refreshing the session in the background. In some cases, the attacker strengthens control by changing passwords or authentication settings. With access secured, Storm-2755 searches emails and internal systems for payroll and HR-related information. It then sets up inbox rules to hide its activity, ensuring that any messages related to financial changes go unnoticed by the victim.

#4

The final step is execution. The attacker sends convincing emails to HR or finance teams, requesting changes to direct deposit details. If this fails, the attacker logs directly into HR platforms like Workday and edits the payment information manually. The result is the same salary payments are redirected to accounts controlled by the attacker, causing direct financial loss.

Recommendations

- **Revoke Compromised Tokens and Sessions:** Immediately revoke all active tokens and sessions for any accounts exhibiting indicators of compromise, including sign-ins associated with the Axios user-agent or the bluegraintours[.]com domain.
- **Audit and Remove Malicious Inbox Rules:** Review all mailbox rules across the organization for rules that filter on financial keywords such as "direct deposit," "bank," or "payroll" and route messages to hidden folders. Remove any unauthorized rules and restore suppressed emails.
- **Enforce Conditional Access Policies:** Configure Conditional Access policies to enforce device compliance, restrict sign-ins from unmanaged devices, and apply session lifetime controls that limit token validity and force reauthentication at shorter intervals.
- **Enable Continuous Access Evaluation (CAE):** Activate CAE in Microsoft Entra to ensure that access tokens are re-evaluated and revoked in near real time when risk conditions change, such as user risk elevation or session anomaly detection.
- **Monitor for Axios User-Agent in Sign-In Logs:** Create detection rules in SIEM/XDR platforms to alert on sign-in events where the user-agent string contains "Axios" or "axios/1.7.9," particularly when associated with non-interactive sign-ins to the OfficeHome application.
- **Block Legacy Authentication Protocols:** Disable legacy authentication protocols that do not support modern security controls, reducing the attack surface available for token replay and session hijacking techniques.
- **Update Axios to Patched Versions:** Organizations using the Axios HTTP client in their applications should upgrade to version 1.8.2 or later (or 0.30.0 for legacy branches) to remediate CVE-2025-27152 and prevent SSRF and credential leakage vulnerabilities.
- **Reset Credentials and MFA for Affected Accounts:** For any accounts identified as compromised, reset both the password and all registered MFA methods to prevent the attacker from maintaining access through previously established persistent credentials.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1608: Stage Capabilities	T1608.005: Link Target
	T1583: Acquire Infrastructure	T1583.001: Domains
Initial Access	T1566: Phishing	T1566.003: Spearphishing via Service
	T1189: Drive-by Compromise	
Credential Access	T1557: Adversary-in-the-Middle	
	T1539: Steal Web Session Cookie	
Persistence	T1078: Valid Accounts	T1078.004: Cloud Accounts
	T1098: Account Manipulation	
Discovery	T1087: Account Discovery	
	T1114: Email Collection	T1114.002: Remote Email Collection
Defense Evasion	T1564: Hide Artifacts	T1564.008: Email Hiding Rules
Lateral Movement	T1534: Internal Spearphishing	
Impact	T1657: Financial Theft	

Indicators of Compromise (IOCs)

TYPE	VALUE
Domain	bluegraintours[.]com
User-Agent	axios/1.7.9

Patch Link

https://github.com/axios/axios/releases/tag/v1.8.2

References

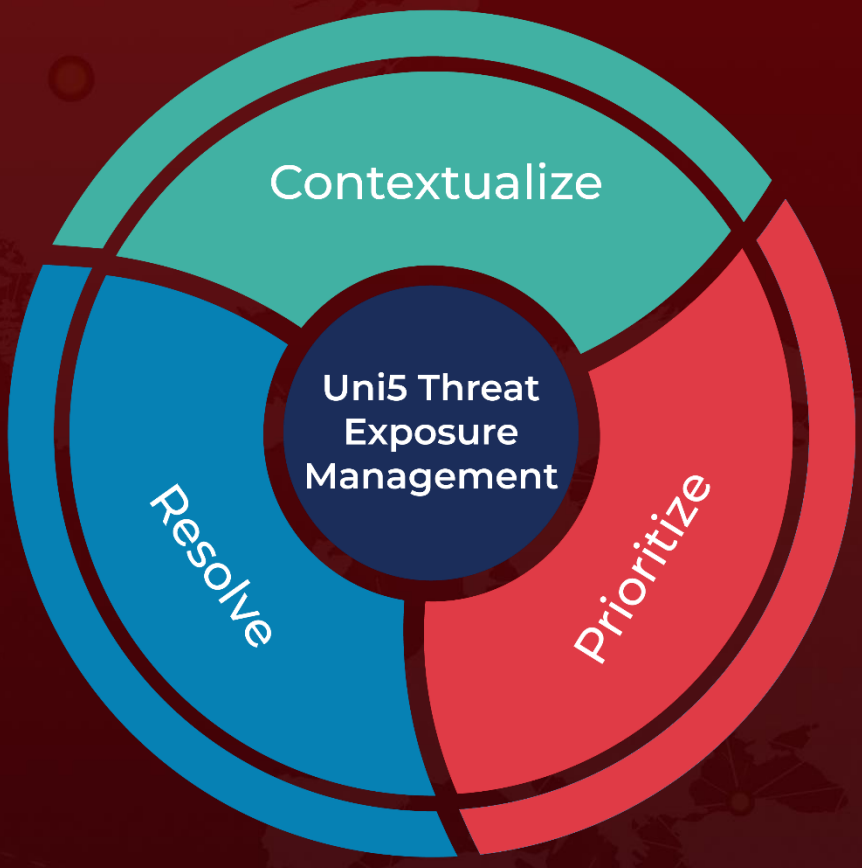
https://www.microsoft.com/en-us/security/blog/2026/04/09/investigating-storm-2755-payroll-pirate-attacks-targeting-canadian-employees/

https://github.com/advisories/GHSA-jr5f-v2jv-69x6

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

April 15, 2026 • 06:30 AM

More at www.hivepro.com