Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

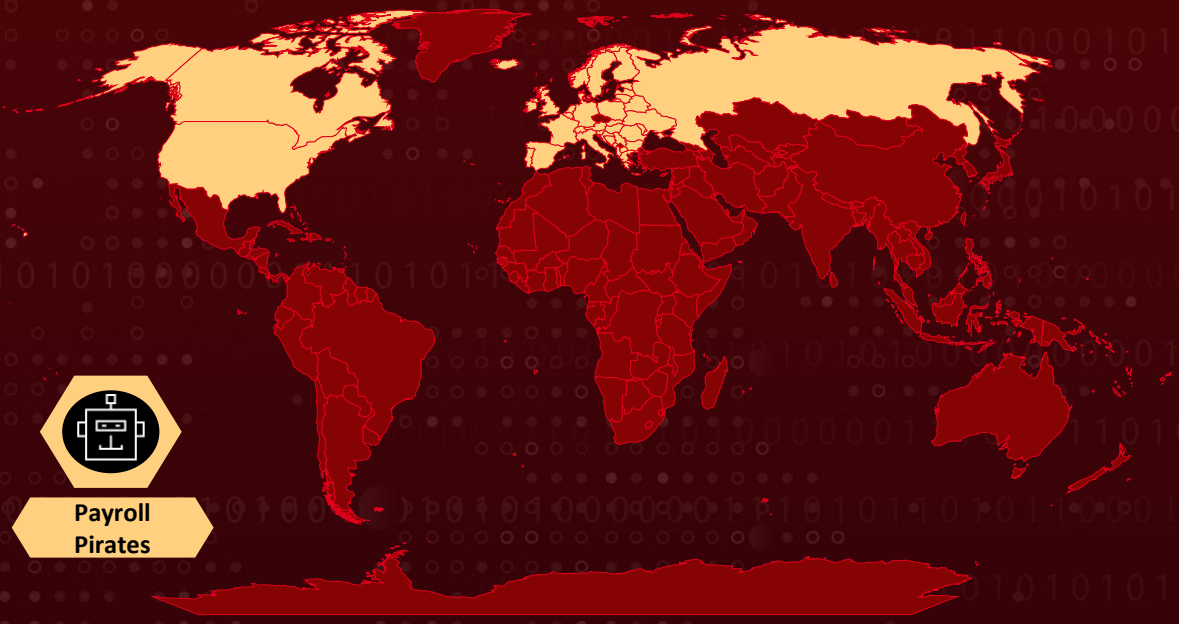
Payroll Pirates Abuse AiTM Phishing to Compromise Microsoft 365

Date of Publication	Admiralty Code	TA Number
August 11, 2026	A1	TA2026229

Summary

First Seen: July 2026
Targeted Regions: United States, Canada, Europe
Targeted Products: Microsoft 365, Microsoft Outlook, Microsoft Graph API, Microsoft Entra ID
Targeted Industries: Healthcare, Education, Manufacturing, Government, Professional Services
Threat Actor: Payroll Pirates (alias Storm-2755)
Attack: Payroll Pirates is an active, financially motivated phishing operation that hijacks Microsoft 365 accounts to search finance and payroll mailboxes quietly. Victims receive fake voicemail notification emails that route them through a chain of trusted Google and Amazon services to an adversary-in-the-middle (AiTM) page that proxies the real Microsoft login and steals the session, even when multi-factor authentication is enabled. Using rotating residential proxies to blend in as ordinary home traffic, the attackers keep access alive on an eight-hour refresh cycle, use the Microsoft Graph API to locate payroll, HR, and finance staff, and collect emails about payments, banking, and direct deposits, ultimately positioning themselves to reroute salary payments to accounts they control.

Attack Regions



Attack Details

#1 Payroll Pirates start with phishing emails that look like a voicemail notification. Each email uses a Microsoft logo and fake call details, caller ID, date, length, and a reference number to feel real and urgent. When the victim clicks the "OPEN [Organization] VOICEMAIL PORTAL" button, they are bounced through several trusted services (Google Meet, Google ad links, and a file hosted on Amazon S3) so email filters don't flag the link. The final page is a fake Microsoft login run by the attacker, sitting on a lookalike domain, usually a Microsoft-style or misspelled "Office" name registered only days earlier.

#2 That fake page is an adversary-in-the-middle (AiTM) proxy: instead of just stealing a password, it passes the victim's login straight to the real Microsoft in real time. So even with MFA turned on, once the victim signs in, the attacker captures the live session token and gets in without being asked for a code. Before the login, the page also quietly fingerprints the visitor's browser and checks their country, which the attackers use to pick a matching proxy so their later logins look local. Suspicious sign-ins from these proxies usually appear within minutes.

#3 From then on, automated logins refresh the stolen session about every eight hours using rotating home-internet (residential proxy) addresses, often showing odd signs like a Firefox or Python client instead of the expected Edge, while keeping the same session ID. With access held, the attackers use the Microsoft Graph API to find staff in payroll, HR, and finance, then read their emails about invoices, payments, banking, and benefits. They mostly stay quiet to avoid setting off alarms, with no password or MFA changes, though in a few cases they created inbox rules to hide messages. The goal is money: the collected information sets them up to reroute salary and direct-deposit payments to their own accounts.

#4 This campaign closely overlaps with the Payroll Pirates activity Microsoft tracks as Storm-2755. In an earlier Storm-2755 wave against Canadian employees, the attackers reached victims through poisoned search results and malicious ads instead of email, but stole sessions the same way. After finding finance staff, they emailed HR with "Question about direct deposit" messages, hid the replies with inbox rules, and, when that didn't work, logged into Workday themselves to change bank details and redirect a victim's salary.

Recommendations

- **Revoke Active Sessions Immediately:** For any account tied to this campaign, revoke all active sessions and tokens right away, password resets alone do not evict an AiTM-stolen session.
- **Rotate Credentials and Re-Register MFA:** Reset passwords and re-enroll MFA for every affected user to invalidate captured authentication material.
- **Audit Payroll and HR Platforms for Direct-Deposit Changes:** Review activity in systems such as Workday and ADP across the full suspected dwell period, paying particular attention to bank-account and direct-deposit modifications.
- **Hunt the Eight-Hour Session-Refresh Pattern:** Search identity logs for a single SessionID recurring at roughly eight-hour intervals across changing IPs, ASNs, and regions to surface additional compromised accounts.
- **Deploy Phishing-Resistant MFA:** Adopt FIDO2 security keys, Windows Hello for Business, or certificate-based authentication, which bind sign-in to the legitimate service and defeat the credential-and-session relay used here.
- **Enforce Managed-Device Access via Conditional Access:** Require compliant or Entra hybrid-joined devices so stolen sessions cannot be replayed from unmanaged attacker infrastructure, and review exclusions and legacy authentication paths for gaps.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1583: Acquire Infrastructure	T1583.001: Domains
Initial Access	T1566: Phishing	T1566.002: Spearphishing Link
Credential Access	T1557: Adversary-in-the-Middle	
	T1111: Multi-Factor Authentication Interception	
	T1539: Steal Web Session Cookie	
Defense Evasion	T1550: Use Alternate Authentication Material	T1550.004: Web Session Cookie
	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
	T1684: Social Engineering	T1684.001: Impersonation
Command and Control	T1090: Proxy	T1090.002: External Proxy
Discovery	T1087: Account Discovery	T1087.004: Cloud Account
Collection	T1114: Email Collection	T1114.002: Remote Email Collection

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	ogads-pa[.]clients6[.]google[.]com, ep1[.]adtrafficquality[.]google, ep2[.]adtrafficquality[.]google, res[.]public[.]onecdn[.]static[.]microsoft, idp[.]keyreniao[.]com, mslogin[.]milocaroline[.]com, api[.]country[.]is, idp[.]korminel[.]com, idp[.]kualabemo[.]com, int[.]camberwolis[.]com, msauth[.]monlinelogicaline[.]com, msonline[.]logicalineonline[.]com, office[.]ofreace[.]com, office[.]ofercarc[.]com, office[.]ofrecie[.]com, office[.]ofreice[.]com, office[.]ofrecre[.]com, office[.]ocrifere[.]com, office[.]ocifire[.]com, login[.]oficarine[.]com, login-microsoftonline[.]offirmtm[.]com, wisemediapa-ttern[.]digital, sky2025forge[.]digital, skyprimeworks[.]digital, 1systemsevolve[.]digital, xsyst-emsquantum[.]digital, tec-hnoplatform2025[.]digital, evolveelevateunion[.]digital, offirmtm[.]com, keyreniao[.]com, korminel[.]com, kualabemo[.]com, milocaroline[.]com, monlinelogicaline[.]com, logicalineonline[.]com, ofrecie[.]com, ofreace[.]com, ofreice[.]com, ofrecre[.]com, ofercarc[.]com, ocrifere[.]com, ocifire[.]com, oficarine[.]com

TYPE	VALUE
URLs	hxxps[:]//meet[.]google[.]com/linkredirect?dest=hxxps[:]//www[.]google[.]com/url?q=amp/adservice[.]google[.]com[.]ph/ddm/clk/424929466;226923624;r;u=ds&sv1=64195420186&sv2=3261659123742877&sv3=6702577448695742699&gclid=EAIaIQobChMIurHiwbHn8gIVBZ53Ch2TZAIsEAQYASABEgKAL_D_BwE;?//s3[.]us-east-1[.]amazonaws[.]com/amzn-5646353653563view/url, hxxps[:]//graph[.]microsoft[.]com/v1[.]0/users?$top=999, hxxps[:]//graph[.]microsoft[.]com/v1[.]0/me
IPv4	142[.]250[.]137[.]155, 142[.]250[.]137[.]156, 142[.]250[.]137[.]157, 142[.]250[.]137[.]154, 192[.]178[.]192[.]132, 187[.]124[.]129[.]44, 153[.]92[.]1[.]166, 104[.]26[.]0[.]226 , 104[.]26[.]1[.]226 , 172[.]67[.]75[.]199, 72[.]62[.]0[.]181, 31[.]97[.]76[.]103, 177[.]7[.]56[.]248, 194[.]5[.]157[.]204, 24[.]252[.]167[.]69, 76[.]216[.]220[.]215, 70[.]108[.]9[.]117, 172[.]58[.]132[.]24, 136[.]50[.]134[.]1, 108[.]147[.]103[.]62, 67[.]250[.]183[.]230, 68[.]42[.]211[.]57, 97[.]165[.]174[.]158, 24[.]224[.]34[.]191, 172[.]59[.]214[.]230, 97[.]85[.]102[.]3
IPv6	2607[:]fb91[:]4[:]4df6[:]431d[:]cce[:]acca[:]3939, 2600[:]4040[:]a33a[:]8e00[:]8121[:]ff13[:]8c19[:]736e, 2603[:]6013[:]7e00[:]be3a[:]bac2[:]4575[:]6826[:]9b79, 2603[:]6013[:]7e00[:]be3a[:]bac2[:]4575[:]6826[:]9b79

References

https://arcticwolf.com/resources/blog/payroll-pirates-strange-new-tides-in-business-email-compromise/

https://hivepro.com/threat-advisory/storm-2755-silent-payroll-heist-targeting-canada/

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 Demo of **HivePro**.

REPORT GENERATED ON

August 11, 2026 • 07:30 AM

More at www.hivepro.com