Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

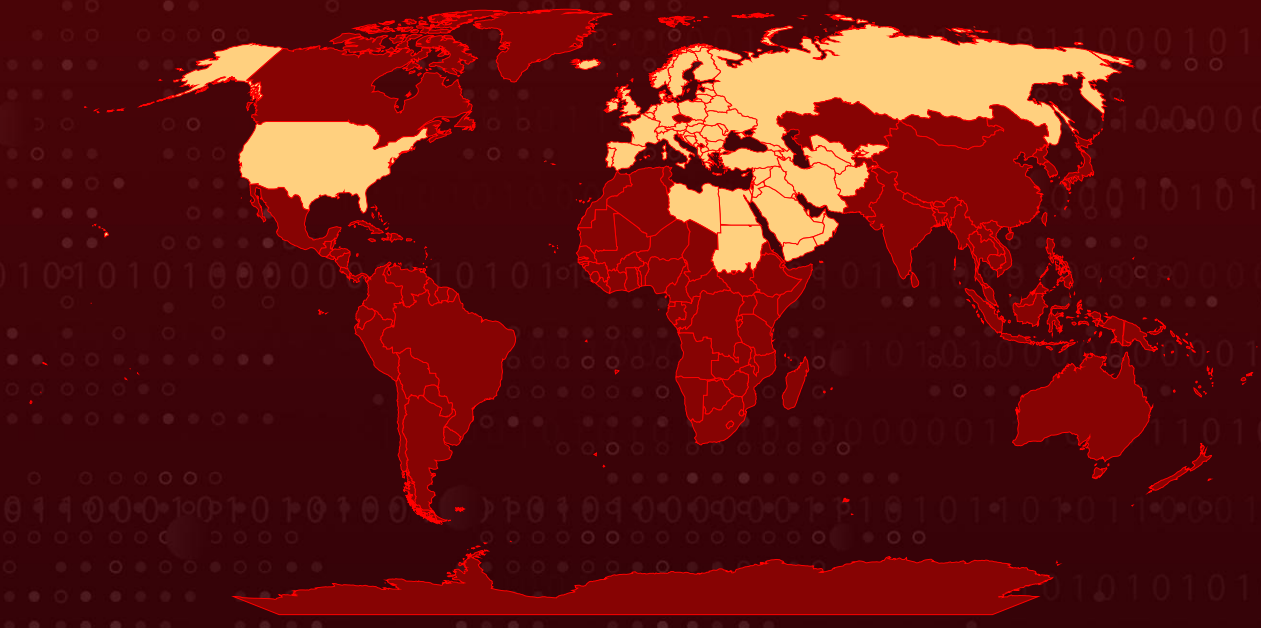
Spraying for Access: Iran-Aligned Actors Turn Weak Credentials into Intelligence

Date of Publication	Admiralty Code	TA Number
April 08, 2026	A1	TA2026092

Summary

First Seen: March 3, 2026
Targeted Regions: Middle East, United States, Europe
Targeted Products: Microsoft 365
Targeted Industries: Government, Municipalities, Energy, Satellite, Aviation, Maritime, Private Sector, Technology, Software, Transportation, Logistics, Healthcare, Medical, Manufacturing, Industrial, Professional Service, Education, Research, Commercial, Retail, Consumer Goods, Banking, Finance, Insurance
Threat Actor: Iran-nexus threat actor
Attack: An Iran-linked threat actor conducted a large-scale password spray campaign against Microsoft 365 tenants across the Middle East, executing three distinct attack waves on March 3, 13, and 23, 2026. The campaign primarily targeted Israeli municipalities and UAE organizations, impacting over 300 entities in Israel and more than 25 in the UAE. The attackers leveraged Tor exit nodes for scanning, commercial VPN services geolocated in Israel for authentication, and sought to access sensitive email content and cloud data. The campaign is assessed to support kinetic operations and Bombing Damage Assessment efforts during the ongoing regional conflict.

Attack Regions



© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

Targeted Non-Targeted

Attack Details

#1 It began quietly, but at scale. A wave of coordinated login attempts swept across hundreds of organizations, with a sharp focus on Israel and the United Arab Emirates. Rather than relying on noisy brute-force attacks, the operators used password spraying, a far more calculated approach that tests a handful of commonly used passwords across a wide range of accounts. The strategy hinges on a simple but effective assumption: somewhere in the target pool, weak credentials will exist. To stay under the radar, the attackers rotated source IP addresses and funneled traffic through constantly shifting Tor exit nodes, disguising their activity with a User-Agent string mimicking Internet Explorer 10 on Windows 7 to blend into legitimate traffic patterns.

#2 Once valid credentials were identified, the campaign shifted gears from reconnaissance to active intrusion. The threat actor abandoned Tor in favor of commercial VPN services such as Windscribe and NordVPN, leveraging IP ranges geolocated within Israel. This was a deliberate move to sidestep geo-restrictions and conditional access policies, allowing malicious logins to appear as though they originated from within trusted regions. The infrastructure supporting this activity was traced to AS35758 (Rachamim Aviel Twito), a network previously associated with Iran-aligned operations across the Middle East.

#3 With authenticated access in hand, the attackers moved swiftly but quietly. Instead of deploying malware or triggering disruptive actions, they exploited the legitimacy of compromised accounts to access sensitive data within Microsoft 365 environments. Their focus centered on email communications and potentially broader cloud-hosted assets, enabling intelligence collection without raising immediate alarms. This low-noise, high-impact approach underscores a growing trend in credential-based intrusions, where access itself becomes the primary weapon.

#4 Israeli municipalities emerged as the primary targets, both in volume and intensity. Notably, there appears to be a correlation between the cities targeted in this campaign and those impacted by Iranian missile strikes in March. This overlap suggests the operation may have been aligned with broader strategic objectives, potentially supporting military efforts through intelligence gathering and Bombing Damage Assessment (BDA).

#5 The campaign unfolded in three distinct waves, March 3, March 13, and March 23, 2026, each representing a deliberate burst of activity rather than continuous probing. Based on the targeting patterns, infrastructure links, and behavioral overlap with previously observed operations, the activity has been attributed with moderate confidence to an Iran-nexus threat actor. The tactics, particularly the use of Tor for initial access and VPN-based localization for persistence, closely mirror tradecraft associated with groups like Gray Sandstorm, reinforcing the likelihood of state-aligned involvement.

Recommendations

Monitor Sign-In Logs for Password Spray Patterns: Review Microsoft 365 sign-in logs for multiple authentication failures distributed across numerous distinct user accounts from the same source IP address within a short timeframe, which is the hallmark pattern of password spray activity.

Block Tor Exit Nodes and Anonymization Networks: Implement conditional access policies to block authentication attempts originating from known Tor exit nodes and other high-risk anonymization networks that have been observed in this campaign's scanning infrastructure.

Apply Geo-Fencing on Microsoft 365 Authentication: Configure conditional access controls to restrict authentication to approved geographic locations relevant to your organization's operations, reducing the attack surface for adversaries using geographically proxied VPN connections.

Strengthen Credential Hygiene and Password Policies: Implement strong password policies that prohibit commonly used passwords and enforce complexity requirements. Conduct periodic password audits to identify accounts with weak or previously breached credentials that are vulnerable to spray attacks.

Enable and Retain Comprehensive Audit Logging: Ensure that Microsoft 365 Unified Audit Logging is enabled and retained for an appropriate period to support post-compromise investigation, allowing security teams to trace attacker actions after any suspected successful authentication.

Enforce Tenant-Wide Multi-Factor Authentication: Deploy multi-factor authentication (MFA) across all Microsoft 365 user accounts, with stricter MFA enforcement and phishing-resistant methods for privileged and administrative roles, to ensure that compromised passwords alone are insufficient for access.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Reconnaissance	T1589: Gather Victim Identity Information	T1589.001: Credentials
Initial Access	T1078: Valid Accounts	T1078.004: Cloud Accounts
Credential Access	T1110: Brute Force	T1110.003: Password Spraying
Defense Evasion	T1090: Proxy	T1090.003: Multi-hop Proxy
Collection	T1114: Email Collection	T1114.002: Remote Email Collection
Command and Control	T1573: Encrypted Channel	

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	185[.]191[.]204[.]202, 185[.]191[.]204[.]203, 169[.]150[.]227[.]3, 169[.]150[.]227[.]143, 169[.]150[.]227[.]146

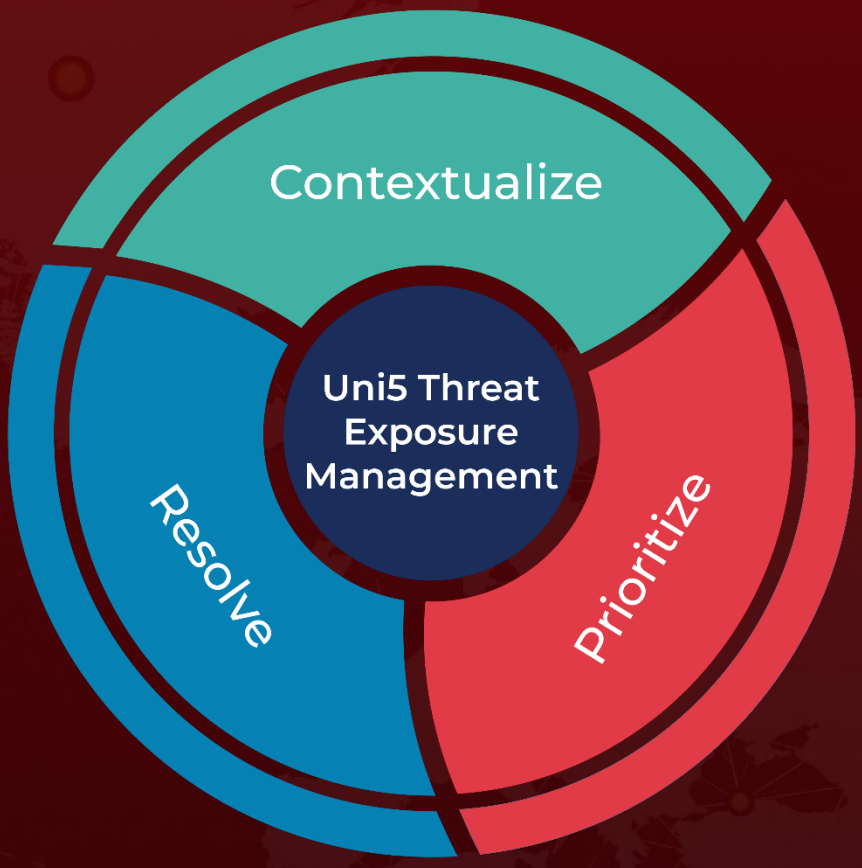
References

https://blog.checkpoint.com/research/iran-nexus-password-spray-campaign-targeting-cloud-environments-with-a-focus-on-the-middle-east/

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 08, 2026 • 7:30 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com