Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

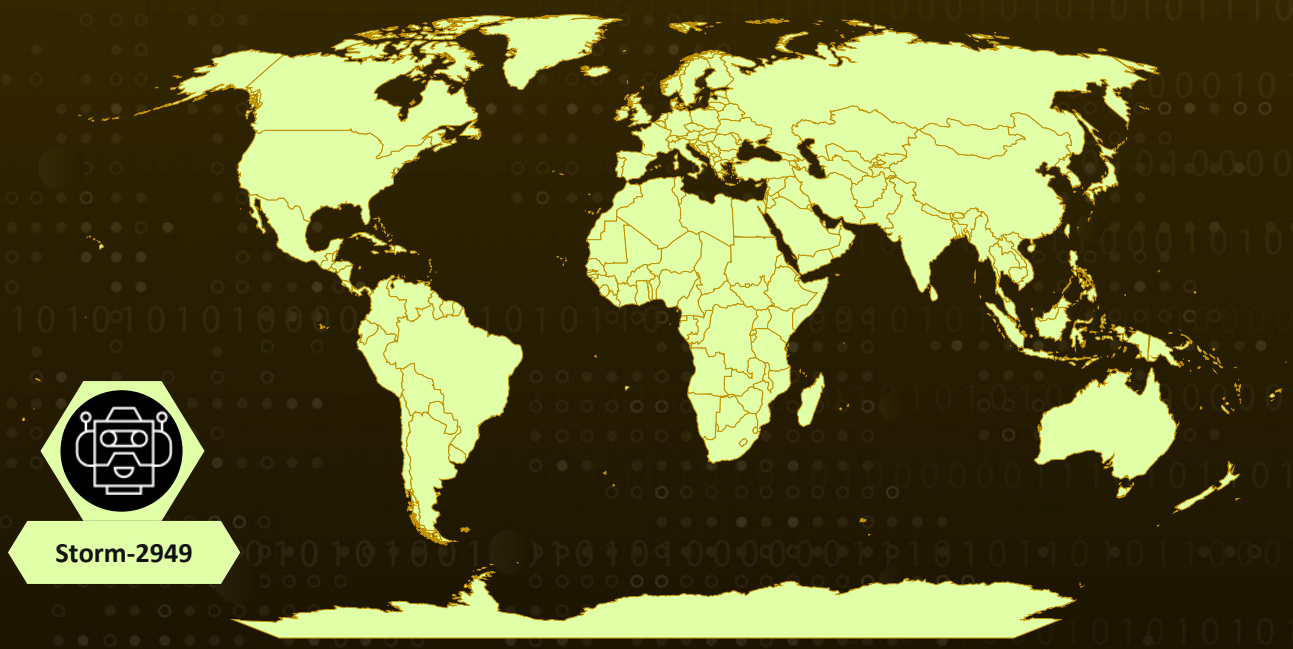
Inside Storm-2949's Cloud Takeover Campaign Targeting Microsoft 365 and Azure

Date of Publication	Admiralty Code	TA Number
May 20, 2026	A1	TA2026139

Summary

First Seen: 2026
Targeted Regions: Worldwide
Targeted Platforms: Microsoft Entra ID, Microsoft 365, Microsoft Azure (SaaS, PaaS, IaaS)
Threat Actor: Storm-2949
Attack: Storm-2949 conducted a multi-phase, identity-driven cloud breach campaign that abused Microsoft's Self-Service Password Reset (SSPR) process through social engineering. The threat actor compromised privileged user accounts, including IT staff and senior leadership, then leveraged legitimate Azure management features to escalate access across Microsoft 365 and Azure infrastructure, exfiltrating sensitive data from OneDrive, SharePoint, Azure Key Vaults, Storage accounts, SQL databases, and production web applications without deploying traditional malware.

Attack Regions



Attack Details

#1

A threat actor tracked as Storm-2949 has been targeting Microsoft 365 and Azure production environments by abusing legitimate applications and built-in administrative features to steal sensitive data. The campaign began with a carefully orchestrated social engineering operation that exploited Microsoft's Self-Service Password Reset (SSPR) mechanism. Attackers initiated password reset requests for selected employees, including IT administrators and senior executives, before posing as internal IT support staff to contact the victims directly. Under the guise of routine account verification, users were tricked into approving malicious multifactor authentication (MFA) prompts, unknowingly handing control of their accounts to the attackers.

#2

Once access was obtained, the threat actor reset passwords, removed all previously registered authentication methods, and enrolled their own Microsoft Authenticator instance on attacker-controlled devices. This effectively locked out legitimate users while granting Storm-2949 persistent control over the compromised accounts. The same technique was repeated across several users within the organization, allowing the attackers to expand their foothold steadily. After compromising the identities, the group leveraged the Microsoft Graph API through a custom Python-based tool to enumerate users, applications, service principals, and privileged roles within the Microsoft Entra ID environment. Their activity showed a clear focus on identifying high-value accounts and uncovering additional paths for privilege escalation and long-term persistence.

#3

With multiple cloud accounts under their control, Storm-2949 moved deeper into Microsoft 365 services, targeting OneDrive and SharePoint repositories to locate and exfiltrate sensitive information. The attackers specifically searched for IT documentation related to VPN setups, remote access workflows, and internal infrastructure, likely to facilitate further lateral movement into the victim's broader network. In one case, thousands of files were downloaded from a single OneDrive account in a single operation. The campaign later shifted toward Azure, where the compromised accounts already possessed privileged custom Azure RBAC roles across multiple subscriptions. The attackers targeted Azure App Services, Key Vaults, SQL databases, Storage accounts, and virtual machines in an effort to gain wider access across the production environment.

#4 Although direct access to a primary production web application was initially blocked by gateway protections, the attackers bypassed the restriction by compromising auxiliary web apps and extracting deployment credentials through Azure publishing profiles. Within minutes, Storm-2949 altered Key Vault access policies and retrieved numerous secrets, including database credentials and identity tokens, significantly increasing the scope of the breach. The group also manipulated SQL firewall rules, enabled public access to Azure Storage accounts, and harvested SAS tokens and account keys to exfiltrate large volumes of blob data over several days using custom Azure SDK-based scripts.

#5 On the infrastructure side, the attackers abused the VMAccess extension to create local administrator accounts on virtual machines and used Azure Run Command to deploy scripts aimed at stealing managed identity tokens through the Azure Instance Metadata Service (IMDS). They further installed ScreenConnect on compromised systems after disabling Microsoft Defender protections, disguising the remote access software as legitimate Windows components. From there, the attackers conducted host discovery, credential harvesting, certificate theft, and file-share scanning for sensitive information before attempting to erase traces of their activity by clearing event logs, deleting temporary files, and removing command history artifacts.

Recommendations

- **Enforce Phishing-Resistant MFA for Privileged Accounts:** Require phishing-resistant MFA methods (such as FIDO2 security keys or certificate-based authentication) for all administrators, IT staff, and senior leadership accounts to prevent SSPR-based social engineering attacks from succeeding.
- **Pre-register MFA for All Privileged Users:** Ensure that all users with privileged roles already have registered MFA methods prior to any reset events, reducing the window for an attacker to enroll their own device during an SSPR flow.
- **Apply Least Privilege for Azure RBAC:** Audit and reduce the scope of custom Azure RBAC roles across all subscriptions, ensuring that no single user account holds Owner or overly broad permissions across Key Vaults, Storage accounts, SQL servers, and App Services simultaneously.

Harden Azure Key Vault Access: Restrict public network access to Key Vaults via private endpoints, enable purge protection, retain Key Vault logs for at least one year, regularly audit RBAC role assignments, and prefer Azure RBAC over Key Vault access policies.

Secure Azure Storage and SQL Configurations: Enforce private endpoints for Azure Storage accounts, disable anonymous blob access, use Azure Policy to prevent public access configurations, and configure SQL server firewall rules to restrict access to known trusted IP ranges with monitoring for unauthorized changes.

Enable Tamper Protection on Endpoints: Ensure Microsoft Defender Antivirus tamper protection is enabled across all endpoints and VMs to prevent threat actors from disabling real-time protection and behavior monitoring.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1078: Valid Accounts	T1078.004: Cloud Accounts
	T1566: Phishing	T1566.003: Spearphishing via Service
Execution	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.006: Python
Persistence	T1098: Account Manipulation	T1098.005: Device Registration
Defense Evasion	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
	T1070: Indicator Removal	T1070.001: Clear Windows Event Logs
	T1036: Masquerading	T1036.004: Masquerade Task or Service

Tactic	Technique	Sub-technique
Collection	T1530: Data from Cloud Storage	
Discovery	T1087: Account Discovery	T1087.004: Cloud Account
	T1580: Cloud Infrastructure Discovery	
Credential Access	T1528: Steal Application Access Token	
	T1552: Unsecured Credentials	T1552.001: Credentials In Files
Lateral Movement	T1021: Remote Services	T1021.007: Cloud Services Dashboard
Command and Control	T1219: Remote Access Software	
Exfiltration	T1567: Exfiltration Over Web Service	

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	176[.]123[.]4[.]44, 91[.]208[.]197[.]87, 185[.]241[.]208[.]243

References

https://www.microsoft.com/en-us/security/blog/2026/05/18/storm-2949-turned-compromised-identity-into-cloud-wide-breach/

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

May 20, 2026 • 10:00 AM

More at www.hivepro.com