



THREAT ADVISORY

Passkey-Themed Social Engineering Leads to Cloud Compromise and Data Theft

PREPARED BY

Drona Cyber Solutions Pvt Ltd

DATE OF ISSUE

September 15, 2026

CLASSIFICATION MATRIX

TLP : GREEN

Executive Summary & Threat Anatomy

Strategic Context: Sophisticated threat groups are bypassing multi-factor authentication (MFA) safeguards not by breaking cryptography, but by subverting identity operations through helpdesk vishing and credential-proxy infrastructures to stage multi-cloud tenant compromises.

Drona Cyber Solutions Pvt.Ltd and Microsoft Threat Intelligence have documented an escalating series of attacks operated by financially motivated clusters (tracked as **Storm-3121** and **Storm-3032**, with affiliations to **ShinyHunters** and **Helix**). The campaign targets enterprise Microsoft 365 environments by luring authenticated personnel via passkey-themed vishing and SMS lures.

Observed Intrusion Kill Chain

PHASE 1 HELPDESK LURE	PHASE 2 AiTM PROXY	PHASE 3 MFA PERSISTENCE	PHASE 4 GRAPH DISCOVERY
Vishing and SMS pose as corporate IT enforcing passkey/SSO enrollment.	Victims land on proxy sites capturing active session tokens and passwords.	Actors access My Sign-Ins to register rogue software OTP tokens (NO_DEVICE).	Programmatic REST API inventory of users, SharePoint sites, and drives.

Attack Mechanism & Persistence Patterns

- **Deceptive Ingress & Infrastructure:** Phishing domains are systematically registered via Nicenic, embedding target tenant strings (e.g., <org>.integratedsso[.]com). Compromised corporate Microsoft Teams accounts are also weaponized for lateral social engineering.
- **Rogue MFA Registration:** The primary post-compromise objective is adding an actor-owned authentication factor to ensure persistence. Forensic telemetry identifies newly registered software tokens logged as SoftwareTokenActivated with device labels set to NO_DEVICE.
- **Low-and-Slow Exfiltration:** Threat actors employ automated Python scripts leveraging the Python-HTTPX user agent to pull down sensitive mailboxes and SharePoint libraries at rates strictly under 1,000 files/hour to bypass traditional DLP rate limits.

Strategic Remediation & Controls

CONTROL DOMAIN	STRATEGIC ACTION ITEM	IMPACT
Phishing-Resistant MFA	Enforce FIDO2 hardware tokens or Windows Hello for Business via Conditional Access; deprecate push and SMS authenticators.	Critical Prevention
Managed Device Compliance	Mandate compliant and Intune-managed devices for cloud resource access; apply web-only download blocks on unmanaged endpoints.	Critical Gate
Flow Hardening	Block Device Code Authentication and Authentication Transfer flows in Entra ID unless an explicit exception exists.	High Defense
Graph API Monitoring	Deploy UEBA alerting for rapid /users and /sites API calls paired with non-standard user agents (e.g., Python-HTTPX).	High Detection

MITRE ATT&CK; Matrix Mapping

TACTIC	TECHNIQUE ID	TECHNIQUE DESCRIPTION
Initial Access / Persistence	T1078.004	Valid Cloud Accounts
Credential Access	T1556.006	Modify Auth Flow: Multi-Factor Authentication
Discovery	T1087.004 / T1069.003	Cloud Account & Group Enumeration (Graph API)
Collection & Exfiltration	T1213 / T1567	Data from Cloud Repositories & Exfiltration Over Web Service

Indicators of Compromise (IOCs)

INDICATOR	TYPE	DESCRIPTION
passkeyhelpdesk[.]com	Domain	Credential Phishing Infrastructure
integratedsso[.]com	Domain	Tenant-Spoofing Phishing Infrastructure
portalsetuphub[.]com	Domain	Lure Landing & Auth Proxy Portal
Python-HTTPX	User Agent	Automated Microsoft 365 Exfiltration Script

Incident response — first 60 minutes

Window	Action	Operational objective
0–10 min	Validate	Confirm user-reported vishing/SMS event; identify account, device, IP and suspicious authentication timeline.
10–20 min	Contain	Revoke active sessions/refresh tokens for confirmed compromise; block risky access where appropriate.
20–35 min	Remove persistence	Review and remove unauthorized authentication methods, devices, mailbox rules and suspicious app grants.
35–50 min	Scope	Search Graph, SharePoint, OneDrive and Exchange activity for reconnaissance and collection across the same identity/time window.
50–60 min	Preserve	Export relevant identity, Graph, SaaS and helpdesk logs; record timestamps, source IPs, user agents and affected repositories.

Threat Hunting Playbook

Use the following hypotheses to drive a focused hunt. The objective is not to match one IOC, but to identify progression from identity abuse to cloud collection.

H1 — Rogue authentication method

Find users with a new authentication method/device shortly after an unusual sign-in. Validate whether the user initiated the change.

H2 — Identity-to-Graph escalation

Find identities that touch multiple Graph reconnaissance categories in a short interval: directory, privilege, application, repository and mailbox.

H3 — Recon-to-collection progression

Prioritize sessions where discovery is followed by /content, file, message or attachment retrieval.

H4 — Automated SaaS collection

Search for rare user agents, automation signatures, unusual API clients, or sustained download behavior — but correlate with the user, device and source network.

H5 — Helpdesk-to-cloud linkage

Correlate MFA/passkey reset or enrollment tickets with subsequent risky sign-ins, new devices, Graph activity and data access.

Example advanced hunting logic (pseudocode)

```
IdentityEvents
| where RiskySignIn == true
| join kind=inner AuthMethodChanges on UserId
| where AuthMethodTime between (SignInTime .. SignInTime + 30m)
| join kind=inner GraphEvents on UserId
| summarize ReconCategories=dcount(ReconCategory),
APIRequests=count(),
FirstGraph=min(Timestamp),
LastGraph=max(Timestamp)
by UserId, IPAddress
| where ReconCategories >= 2 and APIRequests >= 20
```

Analyst note

Thresholds should be calibrated against the organization's normal SaaS automation. Microsoft's current guidance emphasizes sequence-based correlation and cautions against treating a single IP, domain or user-agent match as conclusive. □cite□turn0search0□

Executive Checklist & IOCs

Phishing-resistant MFA	Risky sign-in + new auth method	Revoke sessions/tokens	Review Graph app consent
Block unnecessary device-code flows	Graph reconnaissance correlation	Remove rogue methods/devices	Review privileged service principals
Managed device for sensitive SaaS	Abnormal SharePoint/OneDrive downloads	Reset/secure account	Tighten verification helpdesk
Restrict security-info registration	Exchange REST anomalies	Scope affected repositories	Test incident playbooks

IOC / hunting reference

Indicator	Type	Use in investigation
passkeyhelpdesk[.]com	Domain	Passkey support lure; pivot from proxy/DNS/email/URL telemetry.
integratedsso[.]com	Domain	Tenant/SSO spoofing theme; search historical DNS and proxy logs.
portalsetuphub[.]com	Domain	Setup/authentication lure infrastructure.
Python-HTTPX	User agent	Hunt for automated SaaS access, but validate against identity, IP, volume and sequence.

Important: indicators are changeable. Microsoft notes that domains, IP addresses and hosting providers can change quickly; behavioral sequence and cross-workload correlation provide a more durable detection basis.

□cite□turn0search0□

Recommended reading / source basis

The original advisory content supplied for this report was expanded with current Microsoft Security Research published 9 September 2026, including the observed attack sequence, telemetry priorities, mitigation guidance, and hunting concepts.

□cite□turn0search0□

This advisory is intended for defensive threat intelligence, security monitoring, incident response and control-design purposes. Validate tenant-specific configuration and log availability before operational deployment.



**Securing Today,
Empowering Tomorrow**



Drona Cyber Sloutions



info@dronacybersolutions.com



+91 81609 68270



www.dronacybersolutions.com