INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:38 UTC

Tycoon2FA Rebounds in Days: Why Domain Seizures Alone Cannot Stop PhaaS Operations

THREAT CAMPAIGN | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0089
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	Microsoft 365, Gmail, Microsoft Azure (SharePoint/OneDrive abused for payload hosting); cloud account credentials broadly
Published	2026-03-23
Discovery Source	Rss

Executive Summary

Tycoon2FA, a phishing-as-a-service platform sending approximately 30 million emails per month, rebounded to full operational capacity within days of a March 4, 2026 Europol and Microsoft domain seizure affecting 330 domains. The platform uses adversary-in-the-middle techniques to steal session cookies and bypass multi-factor authentication, targeting Microsoft 365 and Gmail accounts across organizations of all sizes. The rapid recovery demonstrates that infrastructure takedowns alone produce only temporary disruption, and organizations cannot rely on law enforcement action as their sole defensive control.

Technical Analysis

Tycoon2FA is a PhaaS platform operating at scale, delivering AiTM phishing attacks that intercept session tokens post-authentication, defeating TOTP and push-based MFA (CWE-287: Improper Authentication; CWE-384: Session Fixation; CWE-940: Improper Verification of Source of a Communication Channel). The platform proxies authentication flows in real time between the victim and legitimate identity providers, capturing session cookies that grant authenticated access without requiring credentials. Microsoft SharePoint and OneDrive are being abused as payload-hosting infrastructure, exploiting trusted Microsoft domains to bypass email security filters and increase delivery legitimacy. Relevant MITRE ATT&CK techniques include T1185 (Browser Session Hijacking), T1566/T1566.002 (Phishing/Spearphishing via Link), T1564.008 (Hide Artifacts: Email Hiding Rules), T1598.003 (Spearphishing via Service), T1583.001 (Acquire Infrastructure: Domains), T1071.003 (Web Protocols: Mail), T1090 (Proxy), T1078/T1078.004 (Valid Accounts/Cloud Accounts), T1608.001 (Stage Capabilities: Upload Malware), T1539 (Steal Web Session Cookie), T1557

(Adversary-in-the-Middle), and T1534 (Internal Spearphishing). No CVE is associated with this campaign. The platform is unattributed to a named threat group as of March 4, 2026. Primary source: BleepingComputer reporting on post-disruption rebound (T3). Microsoft sources cited for SharePoint and OneDrive infrastructure abuse context (T1).

Action Checklist

1. Step 1, Immediate: Enable or enforce phishing-resistant MFA (FIDO2/hardware keys) for all Microsoft 365 and Gmail accounts, prioritizing privileged and executive accounts. TOTP and push-based MFA do not stop AiTM session theft.
2. Step 2, Immediate: Configure Microsoft Entra ID (Azure AD) Conditional Access policies to bind sessions to device compliance state and flag or block sign-ins from anomalous IP ranges and unexpected geographies.
3. Step 3, Detection: Search email gateway and Microsoft Defender for Office 365 logs for inbound messages containing links to SharePoint or OneDrive URLs followed by a redirect to a credential-harvesting page. Flag any SharePoint/OneDrive link where the final destination is not a Microsoft-controlled domain.
4. Step 4, Detection: Query Entra ID sign-in logs for impossible travel events, token replay indicators (same token reused from multiple IPs), and authentication successes immediately followed by mailbox rule creation or OAuth application consent (T1564.008, T1534).
5. Step 5, Assessment: Audit all active Entra ID sessions and OAuth application permissions granted in the past 30 days. Revoke suspicious sessions and review third-party app consent for anomalous scope grants.
6. Step 6, Communication: Notify IT leadership and affected business unit owners of the active campaign. Issue user awareness guidance specifically calling out Microsoft 365 and Gmail login prompts arriving via SharePoint or OneDrive links as a current threat vector.
7. Step 7, Long-term: Evaluate deployment of Microsoft Entra ID token protection (Conditional Access: require token binding) and continuous access evaluation to reduce session cookie reuse window. Review email security policy to restrict or sandbox inbound SharePoint/OneDrive links from external senders.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and external IR firm if any user account shows signs of active compromise (mailbox rule creation, OAuth app installed, impossible travel with email forwarding rule), or if more than 5% of organization's M365/Gmail user base shows phishing link clicks in gateway logs within past 14 days.
Recovery Notes	Post-containment: (1) Force password reset for all affected users and revoke all active sessions. (2) Audit mailbox forwarding rules, delegation permissions, and Outlook rules on all compromised accounts; remove unauthorized rules and reset to default. (3) Require re-enrollment in phishing-resistant MFA for all users who clicked malicious links. Conduct 30-day post-incident review of detection gaps (what did SIEM/MDO miss?) and validate that Conditional Access policies caught impossible travel events during attack window. Document lessons learned and update playbook.

Forensic Artifacts	Entra ID sign-in logs (JSON export, raw, unfiltered): IP addresses, geolocation, device IDs, token details, anomaly flags | Exchange mailbox audit logs: mailbox rule creation/deletion events, forwarding rule changes, delegate access changes, eDiscovery export requests | Entra ID audit logs: OAuth2 permission grant events, application consent events, conditional access policy evaluations, directory object modifications | Email gateway logs (SMTP, mail flow): inbound message metadata, URL scanning results, sender reputation, phishing signature matches, redirect chains | Microsoft Defender for Office 365 logs: Safe Links detonation results, URL reputation verdicts, file attachment analysis, campaign clustering

Per-Action IR Details

Step 1 — Immediate: Enable or enforce phishing-resistant MFA (FIDO2/hardware keys) for all Microsoft 365 and Gmail accounts, prioritizing privileged and executive accounts. TOTP and push-based MFA do not stop AiTM session theft.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation phase: preventive measures)

Controls: NIST 800-53 IA-2(1) - Multi-factor authentication, NIST 800-53 IA-2(12) - Multi-factor authentication for privileged access, CIS Controls 6.5 - Require MFA for all users

Compensating: For organizations without hardware key distribution capability: (1) enforce conditional access policies blocking TOTP/SMS MFA; (2) enforce Windows Hello for Business sign-in on all corporate devices (Win 10+); (3) use Azure AD passwordless phone sign-in as interim measure pending hardware key procurement. Document phased rollout timeline with executive sponsorship.

Evidence: Capture baseline before enabling FIDO2: (1) audit report of current MFA enrollment status per user (export from Entra ID MFA registration details); (2) device inventory list showing which devices support FIDO2/platform authenticators; (3) documented list of service accounts or legacy systems that cannot support FIDO2 (required for compensating controls). Preserve in secure audit log system; do not store in user-accessible locations.

Step 2 — Immediate: Configure Microsoft Entra ID (Azure AD) Conditional Access policies to bind sessions to device compliance state and flag or block sign-ins from anomalous IP ranges and unexpected geographies.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation: preventive controls); NIST 800-53 AC-3(7) - Conditional access

Controls: NIST 800-53 AC-2(7) - Session binding and device trust, NIST 800-53 SI-4(1) - Anomalous traffic detection, CIS Controls 6.1 - Establish access control policies

Compensating: Without native Conditional Access: (1) configure Microsoft Defender for Cloud Apps (free tier) to flag impossible travel (sign-in from two geographies in <2-hour window); (2) export Entra ID sign-in logs daily to CSV and manually review for geographic anomalies using geoIP lookup (free: MaxMind GeoLite2); (3) create alert rule in Excel/Google Sheets checking IP geolocation against corporate IP whitelist; (4) require VPN for all off-campus access and block unapproved IP ranges at firewall. Document process and SLA for manual review (max 4-hour response).

Evidence: Before policy deployment: (1) extract baseline of legitimate sign-in patterns (IP ranges, geographies, device types) from Entra ID sign-in logs (past 60 days); (2) document approved geographic regions and IP ranges per business unit; (3) identify service accounts or shared devices that legitimately sign in from multiple geographies (may require policy exceptions; document exceptions with business justification). Export to immutable audit log; preserve raw sign-in log export as forensic baseline.

Step 3 — Detection: Search email gateway and Microsoft Defender for Office 365 logs for inbound messages containing links to SharePoint or OneDrive URLs followed by a redirect to a credential-harvesting page. Flag any SharePoint/OneDrive link where the final destination is not a Microsoft-controlled domain.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 (Detection and Analysis); NIST 800-53 SI-4(5) - URL analysis and detonation

Controls: NIST 800-53 SI-4 - Information system monitoring, NIST 800-53 SI-7 - Software, firmware, and information integrity, CIS Controls 4.1 - Establish email security controls

Compensating: Without Defender for Office 365: (1) query email gateway logs (Postfix/Exim/Exchange Transport logs) for Subject lines and body text containing 'sharepoint.com' or 'onedrive.com'; use grep to extract all URL targets: `grep -oP '(https?://[^\s]+)' email_logs.txt | sort | uniq`; (2) use VirusTotal API (free tier: 4 requests/min) to check final destination of each SharePoint/OneDrive link; flag redirects to non-microsoft.com domains; (3) cross-reference sender domain against known phishing-as-a-service indicators (check against abuse.ch PhishTank database, free weekly download); (4) manually review flagged emails in quarantine folder daily; document patterns in incident tracker.

Evidence: Preserve BEFORE initiating detection: (1) full email gateway message queue logs (including headers, sender IP, message body) for past 30 days (minimum 1TB capacity for medium org); (2) Microsoft Defender for Office 365 threat intelligence logs (if available) showing URL reputations and detonation results; (3) proxy or network egress logs showing outbound HTTPS connections to SharePoint/OneDrive domains (destination IP, SNI hostname, TLS certificate chain); (4) DNS query logs showing resolution of sharepoint.com and onedrive.com domains (for correlation with gateway logs). Store in read-only audit archive; calculate SHA-256 hash of raw logs for integrity verification.

Step 4 — Detection: Query Entra ID sign-in logs for impossible travel events, token replay indicators (same token reused from multiple IPs), and authentication successes immediately followed by mailbox rule creation or OAuth application consent (T1564.008, T1534).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 (Detection and Analysis); NIST 800-53 AU-12 - Audit generation; MITRE ATT&CK T1564.008 (Hide Artifacts: Email Hiding Rules), T1534 (Internal Spearphishing)

Controls: NIST 800-53 AU-12 - Audit record generation, NIST 800-53 SI-4(16) - Decoy objects and honeypots, CIS Controls 8.5 - Detect and investigate unauthorized changes

Compensating: Without advanced SIEM: (1) export Entra ID sign-in logs (raw JSON) via PowerShell: `Get-MgAuditLogSignIn -Filter "createdDateTime gt 2026-02-03" -Top 10000 | ConvertTo-Json | Out-File signin_logs.json`; (2) parse JSON using Python or jq to identify: (a) sign-in success followed by mailbox rule creation within 5 minutes (query Exchange mailbox rule logs: `Get-InboxRule -Mailbox * -IncludeHidden | Select-Object Name,CreatedDate,ModifiedDate`; cross-reference with sign-in timestamp); (b) impossible travel by calculating distance between consecutive sign-in IPs and comparing to max feasible speed (1000 km/hour threshold); use geoIP lookup API; (c) token replay by identifying same Entra ID SessionId used from 2+ different IP addresses within 30-minute window. Create CSV output for manual triage. Spreadsheet macros can automate pattern matching for small orgs (<500 users).

Evidence: Preserve BEFORE querying: (1) Entra ID sign-in logs (raw JSON export, unfiltered, past 90 days minimum); (2) Exchange mailbox audit logs showing mailbox rule creation/modification (enable first: `Set-Mailbox -Identity * -AuditEnabled $true -AuditLogAgeLimit 90`); (3) Entra ID Audit Logs showing OAuth app consent events (query: `Get-MgAuditLogDirectoryAudit -Filter "activityDisplayName eq 'Consent to application'"`) with associated user context and app permissions; (4) network access logs showing IP geolocation context for each sign-in IP (store in lookup table); (5) if available, Azure AD Identity Protection risk events (export from portal: High/Medium risk flagged users). Store all logs in SIEM or immutable audit storage with tamper-evident checksums.

Step 5 — Assessment: Audit all active Entra ID sessions and OAuth application permissions granted in the past 30 days. Revoke suspicious sessions and review third-party app consent for anomalous scope grants.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 (Containment); NIST 800-53 AC-2(5) - Session management and invalidation

Controls: NIST 800-53 AC-2(5) - Inactivity timeout, session termination, NIST 800-53 AC-3 - Access enforcement (scope validation), CIS Controls 6.1 - Access control enforcement

Compensating: Without Entra ID P2 license (required for session revocation): (1) use PowerShell to enumerate active sessions and app consents (no license required): `Get-MgUserOAuth2PermissionGrant -UserId [user-id] | Select-Object ClientId, Scope`; cross-reference ClientId against Microsoft app registry (Microsoft Graph portal); flag consents for apps not in authorized whitelist; (2) manually revoke suspicious OAuth apps: `Remove-MgUserOAuth2PermissionGrant -UserId [user-id] -OAuth2PermissionGrantId [grant-id]`; (3) for session

invalidation without revocation capability: reset user password via Entra ID (forces all active tokens to expire within 1 hour on most apps; verify with vendor); (4) export list of all OAuth consents granted in past 30 days; distribute to application owners for manual validation; request written justification for unfamiliar app integrations. Maintain audit trail in spreadsheet with timestamp and approver name.

Evidence: Preserve BEFORE revoking: (1) complete dump of all user OAuth2 permission grants (export via Graph API or PowerShell output to CSV); include ClientId, Scope, ConsentType, and CreatedDateTime for all users; (2) screenshot or API export of Entra ID Risky Users and Risk Events (Identity Protection portal) showing flagged users and associated risk conditions; (3) list of all registered applications in Entra ID tenant (export: `Get-MgApplication | Select-Object DisplayName, AppId, CreatedDateTime | Export-Csv`); (4) baseline of pre-incident application consent (snapshot from 30 days prior, if available); (5) mailbox forwarding rules for all compromised accounts (query: `Get-Mailbox -ResultSize Unlimited | Get-MailboxForwarding | Where {$_.DeliverToMailboxAndForward -eq $true}`). Store in forensic evidence repository with forensic hash chain.

Step 6 — Communication: Notify IT leadership and affected business unit owners of the active campaign. Issue user awareness guidance specifically calling out Microsoft 365 and Gmail login prompts arriving via SharePoint or OneDrive links as a current threat vector.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation: training and awareness); NIST 800-53 AT-3 - Security awareness training

Controls: NIST 800-53 AT-3 - Awareness training, NIST 800-53 AT-3(1) - Role-specific training, CIS Controls 3.3 - Address unauthorized software

Compensating: Without formal security awareness platform: (1) compose email alert with specific threat indicators: 'Do not enter Microsoft 365 or Gmail credentials into login prompts that appear after clicking links from SharePoint, OneDrive, or email'; include screenshot of legitimate vs. phishing login page; (2) distribute via all-staff email, slack/teams channel, and intranet with visual infographic; (3) schedule optional 15-min town hall or recorded briefing explaining AiTM technique in plain language; (4) create one-page desk reference card (print and laminate) showing red flags: mismatched URL, unusual domain after redirect, missing Microsoft branding. Measure awareness by polling random users: 'What should you do if you see a login prompt from a SharePoint link?' Expected answer required to proceed. Log engagement metrics (email opens, click-through on awareness link, poll responses) for incident documentation.

Evidence: Preserve BEFORE sending awareness message: (1) list of all users who clicked on confirmed phishing links (extract from email gateway logs, MDO logs, or user-submitted reports); (2) timestamp of when awareness notice is sent (for timeline documentation); (3) copy of final message text and images sent (including all distribution channels); (4) pre-campaign baseline of user phishing report rates (if available, from prior awareness campaigns); (5) optionally, record of simulated phishing test results from past 60 days (if conducted). Store in incident communications log with audit trail showing who approved and sent each message.

Step 7 — Long-term: Evaluate deployment of Microsoft Entra ID token protection (Conditional Access: require token binding) and continuous access evaluation to reduce session cookie reuse window. Review email security policy to restrict or sandbox inbound SharePoint/OneDrive links from external senders.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.4 (Recovery); NIST 800-53 AC-3(13) - Token binding and session security

Controls: NIST 800-53 AC-3(13) - Session binding; token protection, NIST 800-53 SI-7(1) - Information system monitoring; integrity verification, CIS Controls 2.1 - Basic email security controls

Compensating: Without Entra ID P2 (token binding) and CAE (continuous access evaluation): (1) enforce session timeout policies: reduce Entra ID token lifetime from default (60 min) to 15–30 min using Conditional Access token lifetime policies, or via PowerShell: `Set-AzureADPolicy -Definition @('{"TokenLifetimePolicy":{"Version":1,"AccessTokenLifetime":"15:00:00"}}') -DisplayName MyTokenPolicy`; (2) configure email gateway rules to warn-on or sandbox all inbound messages with SharePoint/OneDrive links from external domains; set policy to 'External: On (Safe Attachments scan only)' + manual review for exec recipients; (3) deploy URL rewriting proxy to prepend warning page before external SharePoint/OneDrive links are clicked; free

option: squid proxy with URL rewrite rules; (4) enable and review Azure AD Identity Protection rulesets monthly (impossible travel, anomalous token claims, etc.); flag at threshold 'Medium' or above for manual investigation. Document all policy changes in change management system with business justification and rollback procedure.

Evidence: Preserve BEFORE implementing token protection/CAE: (1) baseline metrics on token lifetime and session duration (query Entra ID logs for average session duration in past 90 days); (2) list of critical applications that depend on long-lived tokens (check compatibility with shorter token lifetimes before deployment); (3) pre-remediation email gateway filter rules (export rules and mail flow policies); (4) baseline of user sign-out/sign-in frequency to establish threshold for token timeout tuning (don't set timeout too short or productivity impact will trigger policy override). Store policy baseline in change control system with approved change request.

Detection Guidance

Primary behavioral indicators: (1) Authentication success from an IP address not matching the device's prior session IP within the same token lifetime, indicative of session cookie replay. (2) Mailbox rules created immediately after authentication, particularly rules forwarding mail externally or hiding messages (T1564.008). (3) Inbound emails containing URLs resolving to SharePoint or OneDrive that redirect to non-Microsoft domains. Query Microsoft Defender for Office 365 URL trace logs for clicks on sharepoint.com or onedrive.live.com links that resolve to external redirect chains. (4) In Entra ID sign-in logs, filter for 'Sign-in from unfamiliar location' combined with 'Token issuer type: Azure AD' and a session age under 10 minutes at the point of anomalous activity. (5) Monitor for OAuth consent grants to new applications with Mail.Read, Mail.ReadWrite, or full_access_as_user scopes following a sign-in event. KQL example for Entra ID sign-in anomaly (Microsoft Sentinel): SigninLogs | where ResultType == 0 | where RiskLevelDuringSignIn in ('high','medium') | where AuthenticationRequirement == 'singleFactorAuthentication' or MfaDetail has_any ('') | project TimeGenerated, UserPrincipalName, IPAddress, Location, AppDisplayName, RiskLevelDuringSignIn. Supplement with hunting for impossible travel: SigninLogs | summarize locations=make_set(Location), ips=make_set(IPAddress) by UserPrincipalName, bin(TimeGenerated, 1h) | where array_length(locations) > 1. Note: specific IOC domains from the disrupted infrastructure are not published in available sources as of this writing; no domain or IP IOCs are confirmed for inclusion.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`[not available]`	330 domains seized by Europol and Microsoft on 2026-03-04 have not been published in accessible sources as of configuration date. Monitor threat intelligence feeds (ISAC, Microsoft DART, CrowdStrike Falcon Intel) for post-seizure IOC releases.	LOW

Framework Mappings

MITRE-ATTACK

- **T1185** — Browser Session Hijacking
- **T1566** — Phishing

- **T1564.008** — Email Hiding Rules
- **T1598.003** — Spearphishing Link
- **T1583.001** — Domains
- **T1071.003** — Mail Protocols
- **T1566.002** — Spearphishing Link
- **T1090** — Proxy
- **T1078.004** — Cloud Accounts
- **T1078** — Valid Accounts
- **T1608.001** — Upload Malware
- **T1539** — Steal Web Session Cookie
- **T1557** — Adversary-in-the-Middle
- **T1534** — Internal Spearphishing

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **IA-8** — Identification and Authentication (Non-Organizational Users)

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **6.3**
- **6.4**
- **6.5**
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(5)(i)** — Security Awareness and Training

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1185	Browser Session Hijacking	Collection
T1566	Phishing	Initial-Access
T1564.008	Email Hiding Rules	Defense-Evasion
T1598.003	Spearphishing Link	Reconnaissance
T1583.001	Domains	Resource-Development
T1071.003	Mail Protocols	Command-And-Control
T1566.002	Spearphishing Link	Initial-Access
T1090	Proxy	Command-And-Control
T1078.004	Cloud Accounts	Defense-Evasion
T1078	Valid Accounts	Defense-Evasion
T1608.001	Upload Malware	Resource-Development
T1539	Steal Web Session Cookie	Credential-Access
T1557	Adversary-in-the-Middle	Credential-Access
T1534	Internal Spearphishing	Lateral-Movement

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/tycoon2fa-phishing-p...	T3
Disrupting active exploitation of on-premises SharePoint ... - Microsoft	https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting...	T1
Cloud data security measures in SharePoint & OneDrive	https://learn.microsoft.com/en-us/sharepoint/safeguarding-your-data	T1

Source	URL	Tier
Critical SharePoint flaw, real-time cyberattack prevention, CISA's ...	https://www.youtube.com/watch?v=qNeXaHpfWIc	T3
The Hidden Security Gaps in Your Microsoft 365 and Azure ...	https://revealrisk.com/blog/the-hidden-security-gaps-in-your-micros...	T3

Generated 2026-03-29 18:38 UTC by TJS Security Command Center