INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-08 06:10 UTC

Pink Extortion Group Targets Microsoft 365 Users via Voice Phishing (Vishing)

THREAT CAMPAIGN | **HIGH** | CVSS 8.1

SCC Item ID	SCC-CAM-2026-0423
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	8.1
Affected Products	Microsoft 365 users (enterprise and individual accounts)
Discovery Source	Gemini

Executive Summary

A threat group tracked as 'Pink' is targeting Microsoft 365 accounts through voice phishing, phone calls designed to manipulate employees into surrendering credentials or approving authentication prompts. Enterprise accounts are the primary target, with attackers seeking unauthorized access to email, files, and internal systems. If successful, this attack vector can bypass technical controls entirely, as the victim authorizes access themselves.

Technical Analysis

The Pink Extortion Group campaign leverages voice phishing (vishing) against Microsoft 365 users. Mapped MITRE techniques include T1598.004 (Spearphishing Voice), T1621 (Multi-Factor Authentication Request Generation, MFA fatigue), T1078.004 (Valid Accounts: Cloud Accounts), T1534 (Internal Spearphishing), and T1567 (Exfiltration Over Web Service). Relevant CWEs: CWE-287 (Improper Authentication), CWE-1390 (Weak Authentication), CWE-940 (Improper Verification of Source of a Communication Channel). No CVE applies; this is a social engineering campaign, not a software vulnerability. No confirmed IOCs, victim counts, or attributed infrastructure are available from Tier 1 sources (CISA, MITRE, NVD) as of analysis date. The actor name 'Pink' carries low confidence; corroboration from a primary authoritative source is pending. Tactics are consistent with previously documented groups such as Scattered Spider and LAPSUS$, which used identical vishing and MFA fatigue techniques against cloud-identity environments.

Action Checklist

1. Step 1: Containment. Immediately enforce number matching on Microsoft Authenticator MFA prompts (if not already enabled in Entra ID admin center) to block MFA fatigue attacks; disable legacy authentication

protocols in Microsoft 365 that bypass MFA enforcement (Entra ID Conditional Access). Per NIST AC-7, enforce consecutive failed logon limits on all cloud accounts.

2. Step 2: Detection. Query Entra ID (Azure AD) sign-in logs for anomalous MFA approval events, especially approvals preceded by multiple failed attempts or approvals from unexpected geographies. Review Microsoft 365 Unified Audit Log for access events following MFA approvals outside business hours. Flag patterns matching T1621 (repeated MFA push notifications in short windows). Per NIST AU-6 and CIS 8.2, ensure audit logging is enabled and log review is occurring on a defined schedule.

3. Step 3: Eradication. Revoke active sessions and rotate credentials for any accounts showing anomalous MFA approval patterns (NIST AC-2, D3-CRO). Enforce Conditional Access policies requiring compliant devices and blocking sign-ins from non-corporate locations. Remove any OAuth application grants or delegated permissions added during suspected compromise windows.

4. Step 4: Recovery. Validate that MFA number matching is active across all user accounts, not only administrative roles (CIS 6.3, CIS 6.5). Confirm Conditional Access policies are enforced in blocking mode, not audit mode. Monitor Entra ID sign-in logs for 14 days post-remediation for re-authentication attempts from previously flagged sessions or IPs.

5. Step 5: Post-Incident. Conduct targeted security awareness training focused specifically on vishing recognition and the internal procedure for reporting unexpected MFA prompts (NIST AC-8 system use notification baseline). Review and update the help desk identity verification protocol, a common initial access vector for this attack class, to prevent social engineering of IT staff into account resets. Document the control gap if legacy authentication was enabled.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to legal and executive leadership if Unified Audit Log evidence confirms the Pink group accessed mailboxes containing PII, PHI, or financial data — triggering breach notification obligations under GDPR, HIPAA, or state privacy laws — or if any Entra ID Global Administrator account shows an anomalous MFA approval event, indicating potential full-tenant compromise.
Recovery Notes	Post-containment, verify that all Conditional Access policies targeting legacy authentication and non-compliant devices are confirmed in 'On' (blocking) mode rather than 'Report-only' by exporting the policy state via Microsoft Graph API or the Entra portal, and cross-reference against the pre-incident baseline. Monitor Entra ID sign-in logs and Unified Audit Log daily for 14 days for re-authentication attempts from Pink group-associated IPs, new MFA method registrations on previously compromised accounts, and any new OAuth app consent grants — all three are re-entry indicators specific to this campaign's post-initial-access behavior. If any re-entry indicator fires during the monitoring window, treat it as a new incident and restart the containment phase rather than extending the current timeline.

Forensic Artifacts	Entra ID Sign-in Logs — 'MFA Auth Detail' and 'IP Address' fields for all MFA approval events in the compromise window, specifically filtering for approvals where 'Authentication Requirement' was MFA but 'Client App' shows legacy protocol clients (IMAP, MAPI, POP, SMTP Auth), which indicates successful legacy auth bypass by the Pink group prior to number matching enforcement. | Microsoft 365 Unified Audit Log — 'MailItemsAccessed' and 'FileAccessed' operations timestamped within 30 minutes of each flagged MFA approval, providing direct evidence of data access following vishing-induced authentication; also 'Add OAuth2PermissionGrant' and 'Add delegated permission grant to service principal' events indicating attacker-installed persistence via app consent. | Entra ID Audit Logs — 'Register security info' and 'Delete security info' events on compromised accounts, which would indicate the Pink group attempted to replace the victim's MFA method with an attacker-controlled authenticator after gaining initial access via vishing. | Corporate telephony logs or Microsoft Teams call records — inbound call timestamps to targeted users correlated against Entra ID MFA push notification timestamps; this is the primary artifact linking the voice social engineering vector to the technical authentication events and is unique to vishing-initiated campaigns like Pink. | Entra ID Enterprise Applications consent log — full export of OAuth2 permission grants and delegated permissions per compromised user account scoped to the incident window, preserving evidence of any persistent application-level access the Pink group may have established to survive credential rotation and session revocation.

Per-Action IR Details

Step 1: Containment — Immediately enforce number matching on Microsoft Authenticator MFA prompts to block MFA fatigue attacks; disable legacy authentication protocols in Microsoft 365 that bypass MFA enforcement (Entra ID Conditional Access). Per NIST AC-7, enforce consecutive failed logon limits on all cloud accounts.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST AC-7 (Unsuccessful Logon Attempts), NIST AC-17 (Remote Access), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: For teams without Entra ID P1/P2 licensing, use PowerShell to immediately block legacy authentication at the tenant level: Connect-ExchangeOnline and run Set-AuthenticationPolicy -BlockLegacyAuth $true, then assign the policy to all users via Set-User -AuthenticationPolicy. Enumerate legacy auth-enabled service accounts with: Get-User -ResultSize Unlimited | Where {$_.AuthenticationPolicy -eq $null}. For MFA number matching, verify it is enforced (not 'Microsoft managed') via the Entra portal under Authentication Methods > Microsoft Authenticator > Configure.

Evidence: Before enforcing number matching or blocking legacy auth, export the Entra ID sign-in logs for the preceding 72 hours filtered on 'Authentication Requirement: Single-factor authentication' and 'Client App: Legacy Authentication Clients (IMAP, MAPI, POP, SMTP Auth)' to preserve evidence of any accounts already accessed via legacy auth bypass. Also capture a snapshot of the Conditional Access policy blade showing current state — specifically any policies in 'Report-only' mode that were not yet enforcing MFA — as this documents the pre-containment control gap relevant to the Pink group's exploitation window.

Step 2: Detection — Query Entra ID (Azure AD) sign-in logs for anomalous MFA approval events, especially approvals preceded by multiple failed attempts or approvals from unexpected geographies. Review Microsoft 365 Unified Audit Log for access events following MFA approvals outside business hours. Flag patterns matching T1621 (repeated MFA push notifications in short windows). Per NIST AU-6 and CIS 8.2, ensure audit logging is enabled and log review is occurring on a defined schedule.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-2 (Event Logging), NIST AU-3 (Content Of Audit Records), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, use Microsoft's free tooling directly: (1) In the Entra portal, navigate to Identity > Monitoring > Sign-in logs and filter on 'Authentication Requirement: Multifactor authentication' + 'Authentication Detail: MFA completed' + 'IP address: not in [corporate IP ranges]'. Export to CSV. (2) Use PowerShell to query Unified Audit Log for post-MFA mailbox access: Search-UnifiedAuditLog -StartDate (Get-Date).AddDays(-7) -EndDate (Get-Date) -Operations 'MailItemsAccessed' -ResultSize 5000 | Where {$_.UserIds -in $flaggedAccounts}. (3) For T1621 MFA fatigue detection without SIEM, use the free Microsoft Entra Workbook 'Sign-in Analysis' under Azure Monitor Workbooks if Log Analytics is enabled at no-cost tier.

Evidence: Capture from Entra ID sign-in logs: the 'MFA Auth Method', 'MFA Auth Detail', 'Conditional Access Policies Applied', 'Risk Level', 'Risk Detail', and 'IP Address' fields for every MFA approval event in the investigation window. From the Unified Audit Log, preserve 'MailItemsAccessed' and 'FileAccessed' operations (Operations field) timestamped within 30 minutes of each flagged MFA approval — these correlate the vishing-induced approval to downstream data access by the Pink group. Also capture any 'Add app role assignment to service principal' or 'Consent to application' events in the Unified Audit Log, which would indicate the attacker added OAuth persistence during the authorized session.

Step 3: Eradication — Revoke active sessions and rotate credentials for any accounts showing anomalous MFA approval patterns (NIST AC-2, D3-CRO). Enforce Conditional Access policies requiring compliant devices and blocking sign-ins from non-corporate locations. Remove any OAuth application grants or delegated permissions added during suspected compromise windows.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Without an automated identity governance platform, execute session revocation via PowerShell: Revoke-AzureADUserAllRefreshToken -ObjectId for each flagged account, or run the bulk equivalent via: Get-AzureADUser -All $true | ForEach-Object { Revoke-AzureADUserAllRefreshToken -ObjectId $_.ObjectId } scoped to the compromised account list. To enumerate and remove OAuth app grants added during the compromise window: Get-AzureADUserOAuth2PermissionGrant -ObjectId | Where {$_.StartTime -gt ''} then Remove-AzureADOAuth2PermissionGrant. Force password reset via: Set-AzureADUserPassword -ObjectId -Password -ForceChangePasswordNextLogin $true.

Evidence: Before revoking sessions, export the full OAuth application consent list for each compromised account via Entra portal (Identity > Applications > Enterprise Applications > filter by 'User consent') — this preserves evidence of any persistence mechanisms the Pink group may have installed as delegated mail read or send-as permissions. Capture the 'ModifiedProperties' field from Unified Audit Log events 'Add OAuth2PermissionGrant' and 'Add delegated permission grant to service principal' scoped to the compromise window. These app grants survive password resets and session revocations and are a known persistence technique associated with MFA-bypass campaigns targeting M365.

Step 4: Recovery — Validate that MFA number matching is active across all user accounts, not only administrative roles (CIS 6.3, CIS 6.5). Confirm Conditional Access policies are enforced in blocking mode, not audit mode. Monitor Entra ID sign-in logs for 14 days post-remediation for re-authentication attempts from previously flagged sessions or IPs.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-3 (Access Enforcement), NIST AC-17 (Remote Access), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: Validate number matching enforcement without Entra P2 licensing using PowerShell: Get-MgPolicyAuthenticationMethodPolicy | Select -ExpandProperty AuthenticationMethodConfigurations | Where

{$_.Id -eq 'MicrosoftAuthenticator'} | ConvertTo-Json -Depth 5 — confirm 'numberMatchingRequiredState' is 'enabled' not 'default'. For 14-day post-remediation monitoring without SIEM, create a daily scheduled PowerShell task that queries: Search-UnifiedAuditLog -StartDate (Get-Date).AddDays(-1) -EndDate (Get-Date) -Operations 'UserLoggedIn' | Where {$_.ClientIP -in $flaggedIPs} and emails results to the security team via Send-MailMessage. Track previously flagged IPs in a local watchlist CSV updated after each Pink group IOC disclosure.

Evidence: During the recovery validation window, preserve daily exports of Entra ID sign-in logs filtered on: (1) IP addresses identified during the initial compromise, (2) User agents matching mobile or browser clients used in the original vishing-initiated sessions, and (3) any new MFA registration events ('Register security info' in Unified Audit Log) — the Pink group is known to attempt MFA method re-registration on accounts where session tokens have been revoked, as a re-entry technique. These logs constitute the evidentiary baseline for demonstrating clean recovery if regulatory notification becomes necessary.

Step 5: Post-Incident — Conduct targeted security awareness training focused specifically on vishing recognition and the internal procedure for reporting unexpected MFA prompts (NIST AC-8 system use notification baseline). Review and update the help desk identity verification protocol — a common initial access vector for this attack class — to prevent social engineering of IT staff into account resets. Document the control gap if legacy authentication was enabled.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST AC-8 (System Use Notification), NIST AC-1 (Policy And Procedures), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For teams without a dedicated security awareness platform, build a vishing-specific tabletop scenario using the CISA Vishing Guide (freely available) and run a 30-minute walk-through with help desk and front-line staff covering: (1) how to identify unsolicited MFA push calls claiming to be IT, (2) the internal number to call back to verify IT identity before taking any account action, and (3) the step to text or call the user directly on a known number before approving any help desk-initiated account reset. Document the help desk verification gap as a formal risk acceptance or remediation item referencing the specific Pink group TTP of impersonating IT support to trigger password resets that eliminate MFA entirely.

Evidence: For the post-incident report, preserve: (1) the Unified Audit Log export showing the full attack timeline from first anomalous MFA push to last unauthorized access event, (2) any call records or telephony logs from the corporate phone system or Teams call logs that correlate with the MFA push timestamps — these are the primary evidence of the vishing vector itself, (3) the pre-remediation Conditional Access policy export showing any 'Report-only' or legacy auth exceptions that constituted the exploitable control gap, and (4) a screenshot or JSON export of the Authentication Methods policy state at time of discovery, documenting whether number matching was in 'Microsoft managed' (non-enforced) mode at the time of the Pink group campaign.

Detection Guidance

Primary log sources: Microsoft Entra ID (Azure AD) Sign-in Logs and the Microsoft 365 Unified Audit Log. Detection indicators for this campaign: (1) MFA push notification bursts, multiple authentication requests for one account within a 5-minute window, especially outside business hours (T1621 pattern); (2) successful MFA approval immediately following a burst of failed attempts, indicates potential MFA fatigue success; (3) sign-in from an unexpected IP or geography within minutes of a vishing call window (correlate with HR/helpdesk call records if available, or with employee calendars if employees report the call to security team immediately); (4) new OAuth app consent grants or inbox rule creation post-authentication (T1534, T1567 post-access indicators); (5) account password reset or MFA method change initiated via helpdesk without a user-confirmed request (social engineering of IT staff vector). Per NIST AU-6, these logs must be reviewed on a defined schedule. Per CIS 8.2, confirm audit logging is enabled across all Microsoft 365 workloads. No confirmed IOCs

(IPs, domains, hashes) are available from primary sources at this time; behavioral detection is the primary mechanism.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`none confirmed`	No IOCs available from primary authoritative sources as of analysis date. Campaign infrastructure is unconfirmed.	LOW

Framework Mappings

MITRE-ATTACK

- **T1567** — Exfiltration Over Web Service
- **T1534** — Internal Spearphishing
- **T1598.004** — Spearphishing Voice
- **T1078.004** — Cloud Accounts
- **T1621** — Multi-Factor Authentication Request Generation

OWASP-TOP10-2021

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

NIST-800-53R5

- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **AT-2** — Literacy Training and Awareness

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **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.8.8** — Management of technical vulnerabilities

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1567	Exfiltration Over Web Service	Exfiltration
T1534	Internal Spearphishing	Lateral-Movement
T1598.004	Spearphishing Voice	Reconnaissance
T1078.004	Cloud Accounts	Defense-Evasion
T1621	Multi-Factor Authentication Request Generation	Credential-Access

Sources

Source	URL	Tier
9 out of 10 Enterprises Have Vulnerabilities in their Microsoft 365 ...	https://www.coreview.com/news/enterprises-vulnerabilities-microsoft...	T3
What specific vulnerabilities do Microsoft 365 and other SaaS ...	https://www.arcserve.com/faq/specific-vulnerabilities-microsoft-365...	T3
Microsoft 365 vulnerabilities and suggested workarounds - Reddit	https://www.reddit.com/r/sysadmin/comments/1h6o4mx/microsoft_365_vu.. .	T3
Improve Microsoft Office 365 Security with a Vulnerability Assessment	https://www.bitlyft.com/resources/microsoft-office-365-security-	T2
The Microsoft 365 Security Mistakes That Lead to Breaches - YouTube	https://www.youtube.com/watch?v=Z-SHJM7jriQ	T3

Generated 2026-06-08 06:10 UTC by TJS Security Command Center