INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-10 06:15 UTC

VENOM PhaaS Platform Targets C-Suite Credentials via AiTM and Device-Code Phishing to Bypass MFA

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0163
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Microsoft 365, Microsoft SharePoint, Microsoft authentication APIs (C-suite executive accounts)
Published	2026-04-09T17:37:04
Discovery Source	Rss

Executive Summary

VENOM is a closed-access phishing-as-a-service platform actively targeting CEOs, CFOs, and VPs with attacks designed to steal Microsoft 365 session tokens and bypass multi-factor authentication. The platform uses adversary-in-the-middle and device-code phishing techniques that exploit legitimate Microsoft authentication flows, which push-notification and TOTP-based MFA do not prevent. Organizations relying on Microsoft 365 for executive communications, financial approvals, and sensitive data access face elevated risk of account takeover, business email compromise, and downstream fraud.

Technical Analysis

VENOM is a PhaaS platform observed since at least November 2025, operating as a closed-access service to reduce operator exposure. Attack chains combine two MFA bypass techniques: adversary-in-the-middle (AiTM) proxying, which intercepts and relays Microsoft authentication sessions to capture valid session tokens in real time, and device-code phishing (T1621), which abuses the Microsoft OAuth 2.0 device authorization grant flow to obtain long-lived tokens without user-visible authentication prompts. No CVE is associated; the platform exploits legitimate protocol behavior, not software vulnerabilities. Affected surfaces include Microsoft 365, Microsoft SharePoint, and Microsoft authentication APIs. Evasion techniques include Unicode-rendered QR codes to defeat image-based phishing scanners, double Base64-encoded URL fragments to bypass URL analysis and detonation sandboxes, and target reconnaissance and filtering (T1589, T1592) to block researcher IPs and automated crawlers from accessing phishing infrastructure. Relevant CWEs: CWE-287 (improper

authentication), CWE-384 (session fixation), CWE-940 (improper verification of source of a communication). MITRE ATT&CK techniques include T1566 and T1566.001 (spearphishing), T1557 (AiTM), T1621 (MFA request generation), T1550.001 (application access token use), T1528 (steal application access token), T1539 (steal web session cookie), T1111 (MFA interception), T1556.006 (multi-factor authentication manipulation), T1027 (obfuscated files/information), T1078 (valid accounts), T1589 (gather victim identity information), T1592 (gather victim host information), and T1598.003 (spearphishing link for credential harvesting). No patch exists; defense requires authentication architecture changes and conditional access policy enforcement.

Action Checklist

1. Containment, Immediately enable Microsoft Entra ID Conditional Access policies requiring compliant or Azure AD-joined devices for all C-suite accounts. Disable the OAuth 2.0 device authorization grant flow for your tenant unless operationally required (Microsoft Entra admin center > Identity > Applications > App registrations > Authentication flows). Block legacy authentication protocols that do not support modern token binding.
2. Detection, Review Microsoft Entra ID Sign-In Logs (Azure Portal > Entra ID > Monitoring > Sign-in logs) for C-suite accounts. Filter for: sign-ins from unexpected geographic locations or ASNs, device-code flow authentication events (token grant type = 'urn:ietf:params:oauth:grant-type:device_code'), sign-ins immediately followed by inbox rule creation or mail forwarding changes, and session token reuse from IP addresses inconsistent with the authenticated device. Correlate with Microsoft 365 Unified Audit Log for mail delegation and forwarding rule events.
3. Eradication, Revoke all active Microsoft 365 sessions and refresh tokens for C-suite accounts using the Microsoft Entra admin center or PowerShell (using Microsoft.Graph module: Revoke-MgUserSignInSession or legacy: Revoke-AzureADUserAllRefreshToken). Audit and remove any OAuth application consents granted during the suspected window. Inspect and remove suspicious inbox rules and mail forwarding configurations in Exchange Online. Rotate credentials for affected accounts after session revocation.
4. Recovery, After session revocation and credential rotation, re-enroll executive accounts under phishing-resistant MFA (FIDO2 security keys or Windows Hello for Business). Validate Conditional Access policy enforcement by testing sign-in behavior from unmanaged devices. Monitor Entra ID sign-in logs for the following 30 days for recurrence of device-code flow authentication events targeting previously affected accounts.
5. Post-Incident, This campaign exposes three control gaps: (1) reliance on TOTP/push-notification MFA as a sufficient control against session token theft; (2) unrestricted OAuth device-code flow availability; (3) absence of executive account behavioral baselines in SIEM. Implement phishing-resistant MFA (FIDO2) for all privileged and C-suite accounts, enforce continuous access evaluation (CAE) in Microsoft Entra, and build detection rules for device-code grant type authentication events in your SIEM against executive account identities.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate immediately to executive leadership, legal counsel, and cyber insurance carrier if any evidence of downstream BEC activity is found (wire transfer requests, invoice tampering, external mail forwarding of financial or M&A communications), if affected accounts had access to material non-public information triggering SEC disclosure obligations, or if the IR team cannot confirm full session token revocation and OAuth consent removal within 4 hours of detection.
Recovery Notes	After session revocation and FIDO2 re-enrollment, monitor Microsoft Entra ID Sign-In Logs and the Microsoft 365 Unified Audit Log daily for 30 days, specifically filtering for device-code grant type authentication events and any new OAuth application consent grants targeting previously compromised executive UPNs. Validate that Continuous Access Evaluation (CAE) is enforced for all C-suite accounts by confirming the `xms_cc` claim is present in access tokens, which ensures near-real-time session termination if risk signals are detected post-recovery. Retain all forensic exports — Entra ID sign-in logs, inbox rule snapshots, OAuth consent records, and Unified Audit Log extracts — for a minimum of 12 months in immutable storage to support any regulatory inquiry or legal proceedings arising from the VENOM campaign compromise.
Forensic Artifacts	Microsoft Entra ID Sign-In Logs filtered for `grantType = 'urn:ietf:params:oauth:grant-type:device_code'` against C-suite UPNs — the primary forensic signature of VENOM device-code phishing; preserves attacker IP addresses and timing of stolen token issuance | Microsoft 365 Unified Audit Log entries for `New-InboxRule`, `Set-InboxRule`, `UpdateInboxRules`, and `Add-MailboxPermission` operations on executive mailboxes — documents post-compromise persistence and BEC staging actions performed by VENOM operators using stolen session tokens | OAuth application consent grant records from Entra ID (`Get-AzureADOAuth2PermissionGrant`) capturing any malicious app registrations made during the compromise window with `Mail.Read`, `Mail.ReadWrite`, or `Files.ReadWrite` scopes — indicates whether VENOM operators established token-independent persistent access | Microsoft 365 Unified Audit Log `FileAccessed` and `FileDownloaded` events in SharePoint for executive accounts filtered by IP addresses inconsistent with normal work locations — documents exfiltration of sensitive documents accessed using stolen M365 session tokens | Exchange Online Message Trace (`Get-MessageTrace`) for outbound mail from executive accounts to external recipients during the compromise window, cross-referenced against mail forwarding rules — identifies data exfiltration and BEC email activity conducted via the hijacked executive mail sessions

Per-Action IR Details

Containment — Immediately enable Microsoft Entra ID Conditional Access policies requiring compliant or Hybrid Azure AD-joined devices for all C-suite accounts. Restrict or disable the OAuth 2.0 device authorization grant flow for your tenant unless operationally required (Microsoft Entra admin center > Identity > Applications > App registrations > Authentication flows). Block legacy authentication protocols that do not support modern token binding.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST AC-17 (Remote Access), NIST SI-10 (Information Input Validation), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: For teams without Entra ID P1/P2 licensing required for Conditional Access, use PowerShell to immediately block device-code flow at the tenant level: `Set-AuthenticationPolicy -AllowBasicAuthDeviceCode $false` and disable legacy auth per-protocol via Exchange Online: `Set-TransportConfig -SmtpClientAuthenticationDisabled $true`. Use the free Microsoft 365 Security Defaults toggle (Entra admin center > Properties > Manage Security Defaults) to enforce baseline MFA and block legacy auth across the tenant if Conditional Access is unavailable.

Evidence: Before modifying any Conditional Access or authentication flow policies, export the current Entra ID Sign-In Logs for all C-suite UPNs for the preceding 30 days via Microsoft Graph API (`GET /auditLogs/signIns?$filter=userPrincipalName eq '[exec@domain.com]'`) and archive them to immutable storage. Capture current Conditional Access policy state via PowerShell (`Get-AzureADMSConditionalAccessPolicy`) to establish pre-containment baseline. Document all OAuth app consent grants currently in place (`Get-AzureADOAuth2PermissionGrant`) before revoking, as VENOM operators may have registered persistent OAuth apps during the compromise window.

Detection — Review Microsoft Entra ID Sign-In Logs (Azure Portal > Entra ID > Monitoring > Sign-in logs) for C-suite accounts. Filter for: sign-ins from unexpected geographic locations or ASNs, device-code flow authentication events (token grant type = 'urn:ietf:params:oauth:grant-type:device_code'), sign-ins immediately followed by inbox rule creation or mail forwarding changes, and session token reuse from IP addresses inconsistent with the authenticated device. Correlate with Microsoft 365 Unified Audit Log for mail delegation and forwarding rule events.

NIST Phase: Detection Analysis

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

Controls: NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-3 (Content of Audit Records), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: For teams without a SIEM, use PowerShell with the ExchangeOnlineManagement and AzureAD modules. Run: `Search-UnifiedAuditLog -StartDate (Get-Date).AddDays(-30) -EndDate (Get-Date) -Operations 'New-InboxRule','Set-InboxRule','Add-MailboxPermission' -UserIds '[exec@domain.com]'` to detect post-compromise persistence. For device-code flow detection, run: `Get-AzureADAuditSignInLogs | Where-Object {$_.AuthenticationDetails -match 'device_code'}` — pipe output to CSV and manually sort by C-suite UPNs. Cross-reference source IPs against a free threat intelligence feed such as AbuseIPDB via their free API to flag known proxy/VPN exit nodes used by phishing infrastructure.

Evidence: The specific forensic signatures of a VENOM AiTM or device-code phishing attack in Entra ID Sign-In Logs are: (1) `clientAppUsed` field showing 'Browser' or 'Mobile Apps and Desktop clients' with `tokenIssuerType` = 'AzureAD' and `grantType` = 'urn:ietf:params:oauth:grant-type:device_code' for device-code attacks; (2) `ipAddress` fields showing a mismatch between the authentication IP and subsequent API call IPs — indicative of stolen session token replay from a different origin; (3) in the Microsoft 365 Unified Audit Log (Operations: `New-InboxRule`, `UpdateInboxRules`), look for rules created within minutes of a device-code grant event that redirect or delete mail matching keywords like 'invoice', 'wire', 'payment', or 'urgent' — a classic post-compromise BEC staging pattern consistent with C-suite targeting campaigns.

Eradication — Revoke all active Microsoft 365 sessions and refresh tokens for C-suite accounts using the Microsoft Entra admin center or PowerShell (Revoke-AzureADUserAllRefreshToken). Audit and remove any OAuth application consents granted during the suspected window. Inspect and remove suspicious inbox rules and mail forwarding configurations in Exchange Online. Rotate credentials for affected accounts after session revocation.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST AC-17 (Remote Access), NIST IA-5 (Authenticator Management), CIS 5.3 (Disable Dormant Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: For teams without automated identity governance tooling, execute session revocation via free PowerShell: `Get-AzureADUser -Filter "jobTitle eq 'CEO' or jobTitle eq 'CFO' or jobTitle eq 'VP'" | ForEach-Object { Revoke-AzureADUserAllRefreshToken -ObjectId $_.ObjectId }`. For OAuth consent audit, run: `Get-AzureADOAuth2PermissionGrant | Where-Object {$_.StartTime -gt (Get-Date).AddDays(-30)} | Select-Object ClientId, ConsentType, Scope` and manually cross-reference ClientId values against your known authorized application inventory. Remove suspicious inbox rules with: `Get-InboxRule -Mailbox '[exec@domain.com]' | Where-Object {$_.ForwardTo -ne $null -or $_.DeleteMessage -eq $true} | Remove-InboxRule`.

Evidence: Before executing token revocation, capture a full snapshot of active refresh token sessions via: `Get-AzureADAuditSignInLogs -Filter "userPrincipalName eq '[exec@domain.com]'" | Select-Object CreatedDateTime, IPAddress, ClientAppUsed, TokenIssuerType` — this preserves the evidence of stolen session replay. Export all inbox rules and mail forwarding configurations pre-removal: `Get-InboxRule -Mailbox '[exec@domain.com]' | Export-Csv -Path 'C:\IR\[exec]_inboxrules_$(Get-Date -f yyyyMMdd).csv'`. Document all OAuth apps granted consent during the VENOM compromise window before revocation — these may represent persistent access mechanisms (e.g., a malicious OAuth app with `Mail.Read` or `Mail.ReadWrite` scope registered to exfiltrate executive communications silently after session tokens expire).

Recovery — After session revocation and credential rotation, re-enroll executive accounts under phishing-resistant MFA (FIDO2 security keys or Windows Hello for Business). Validate Conditional Access policy enforcement by testing sign-in behavior from unmanaged devices. Monitor Entra ID sign-in logs for the following 30 days for recurrence of device-code flow authentication events targeting previously affected accounts.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST IA-5 (Authenticator Management), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: For teams that cannot procure FIDO2 hardware keys immediately, implement Microsoft Authenticator in numberless matching mode (not push-notification) as a temporary phishing-resistant step — this does not fully defeat AiTM but significantly raises the attack cost compared to standard TOTP. Document this as a temporary compensating control with a 30-day remediation deadline. To validate Conditional Access enforcement without enterprise MDM tooling, use a personal unmanaged device to attempt sign-in as a test account and confirm the policy blocks or restricts access; log the test result with screenshots as evidence of control validation.

Evidence: Before returning executive accounts to production use, verify no residual VENOM-linked persistence exists by running a final audit of: (1) Entra ID registered devices for the executive accounts (`Get-AzureADUserRegisteredDevice -ObjectId [exec_objectid]`) — remove any unrecognized device registrations that may have been added during the device-code phishing attack to establish persistent access; (2) Microsoft 365 Unified Audit Log for `Add member to role` or `Consent to application` operations occurring during the compromise window; (3) Exchange Online mail forwarding rules (`Get-Mailbox -Identity '[exec@domain.com]' | Select-Object ForwardingAddress, ForwardingSmtpAddress, DeliverToMailboxAndForward`) to confirm all forwarding was removed during eradication.

Post-Incident — This campaign exposes three control gaps: (1) reliance on TOTP/push-notification MFA as a sufficient control against session token theft; (2) unrestricted OAuth device-code flow availability; (3) absence of executive account behavioral baselines in SIEM. Implement phishing-resistant MFA (FIDO2) for all privileged and C-suite accounts, enforce continuous access evaluation (CAE) in Microsoft Entra, and build detection rules for device-code grant type authentication events in your SIEM against executive account identities.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-2 (Flaw Remediation), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For teams without a commercial SIEM, build a free detection pipeline using Sigma rules converted to PowerShell or KQL: use the community Sigma rule `win_azure_device_code_phishing.yml` (available in the SigmaHQ GitHub repository) as the detection basis, adapted to query Microsoft 365 Unified Audit Logs via scheduled PowerShell (`Search-UnifiedAuditLog -Operations 'UserLoggedIn' -FreeText 'device_code'`) running on a daily cron job. Output alerts to email or a free webhook-capable channel. For behavioral baselining of executive accounts without a SIEM, maintain a monthly CSV export of Entra ID sign-in logs per executive UPN and use PowerShell's `Compare-Object` to

diff against the prior month's baseline for new ASNs, countries, or client app types.

Evidence: The lessons-learned documentation for this VENOM incident must capture: (1) the full timeline from first device-code phishing email delivery (sourced from Microsoft Defender for Office 365 Threat Explorer or Message Trace logs if available) to first session token use from attacker infrastructure; (2) a complete list of OAuth application consent grants made during the compromise window, with scope details, to identify what data was accessible to VENOM operators; (3) any evidence of downstream BEC activity — wire transfer requests, invoice modifications, or sensitive document access — sourced from Exchange Online message trace and SharePoint Unified Audit Log (`FileAccessed`, `FileDownloaded` operations by the compromised executive accounts from unexpected IPs).

Detection Guidance

Primary detection surface is Microsoft Entra ID Sign-In Logs and the Microsoft 365 Unified Audit Log. Key indicators: (1) Device-code authentication flow events, filter Entra sign-in logs for tokenProtocol or clientAppUsed values indicating device-code grant type against executive accounts. (2) AiTM proxy indicators, sign-in events from hosting provider or VPN ASNs inconsistent with the user's established location baseline, particularly when followed immediately by token issuance. (3) Post-compromise activity, Unified Audit Log events for New-InboxRule, Set-Mailbox (ForwardingSmtpAddress set), and Add-MailboxPermission within minutes of a suspicious sign-in. (4) QR code delivery, email gateway logs showing inbound messages with embedded images containing QR code patterns and no traditional URL-based links; double Base64-encoded URL fragments may appear as unusual character sequences in URL logs. (5) Behavioral baseline deviation, executive accounts accessing SharePoint or Teams from new device fingerprints or at unusual hours. Recommended SIEM query pattern (conceptual, adapt to your platform): alert on Entra sign-in events where account is in executive group AND grant_type = device_code AND IP ASN is not in known-good baseline, correlated with Unified Audit Log inbox rule creation within a 15-minute window.

Framework Mappings

MITRE-ATTACK

- **T1550.001** — Application Access Token
- **T1111** — Multi-Factor Authentication Interception
- **T1556.006** — Multi-Factor Authentication
- **T1557** — Adversary-in-the-Middle
- **T1583** — Acquire Infrastructure
- **T1566.001** — Spearphishing Attachment
- **T1539** — Steal Web Session Cookie
- **T1621** — Multi-Factor Authentication Request Generation
- **T1598.003** — Spearphishing Link
- **T1027** — Obfuscated Files or Information
- **T1528** — Steal Application Access Token
- **T1078** — Valid Accounts
- **T1566** — Phishing

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **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
- **CA-7** — Continuous Monitoring
- **IA-8** — Identification and Authentication (Non-Organizational Users)

OWASP-TOP10-2021

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

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.5.34** — Privacy and protection of personal information

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1550.001	Application Access Token	Defense-Evasion
T1111	Multi-Factor Authentication Interception	Credential-Access
T1556.006	Multi-Factor Authentication	Credential-Access
T1557	Adversary-in-the-Middle	Credential-Access
T1583	Acquire Infrastructure	Resource-Development

Technique ID	Technique Name	Tactic
T1566.001	Spearphishing Attachment	Initial-Access
T1539	Steal Web Session Cookie	Credential-Access
T1621	Multi-Factor Authentication Request Generation	Credential-Access
T1598.003	Spearphishing Link	Reconnaissance
T1027	Obfuscated Files or Information	Defense-Evasion
T1528	Steal Application Access Token	Credential-Access
T1078	Valid Accounts	Defense-Evasion
T1566	Phishing	Initial-Access

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/new-venom-phishing-a...	T3
Disrupting active exploitation of on-premises SharePoint ... - Microsoft	https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting...	T1
Customer guidance for SharePoint vulnerability CVE-2025-53770	https://www.microsoft.com/en-us/msrc/blog/2025/07/customer-guidance...	T1
Client advisory: Microsoft SharePoint vulnerabilities actively exploited	https://www.cfc.com/en-gb/knowledge/resources/advisories/2025/07/cl...	T3
Unauthenticated RCE Vulnerability in Microsoft SharePoint Server	https://www.avertium.com/flash-notices/critical-unauthenticated-rce...	T3

Generated 2026-04-10 06:15 UTC by TJS Security Command Center