INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-14 06:03 UTC

W3LL Phishing-as-a-Service Platform Dismantled After $20M in BEC Fraud Attempts and 17,000+ Victims

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0176
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Microsoft 365
Published	2026-04-13T10:46:00
Discovery Source	Rss

Executive Summary

Law enforcement dismantled W3LL, a Phishing-as-a-Service platform that enabled business email compromise fraud attempts totaling approximately $20 million across more than 17,000 victims worldwide. W3LL sold ready-made phishing kits capable of bypassing multi-factor authentication on Microsoft 365 accounts by intercepting session tokens in real time, serving roughly 500 affiliated threat actors. The enforcement action removed the primary infrastructure, but organizations should treat this as a trigger to audit MFA configurations and email security controls, as the techniques W3LL commercialized remain widely available and continue to enable AiTM attacks across the threat landscape.

Technical Analysis

W3LL operated an adversary-in-the-middle (AiTM) phishing platform purpose-built to compromise Microsoft 365 accounts protected by standard MFA. The platform intercepted session tokens in real time, defeating time-based one-time passwords and push-based MFA by proxying authentication between the victim and Microsoft's legitimate login infrastructure. Relevant CWEs: CWE-287 (Improper Authentication), CWE-940 (Improper Verification of Source of a Communication Channel), CWE-384 (Session Fixation). MITRE ATT&CK coverage includes T1539 (Steal Web Session Cookie), T1557 (Adversary-in-the-Middle), T1566.002 (Spearphishing Link), T1114/T1114.003 (Email Collection/Email Forwarding Rule), T1078 (Valid Accounts), T1656 (Impersonation), T1583.001/T1583.006 (Acquire Infrastructure: Domains/Web Services), and T1586.002 (Compromise Accounts: Email Accounts). No CVE applies, this is a technique-based campaign, not a software vulnerability. W3LL's public storefront closed in 2023, but operations continued via encrypted messaging

channels under a rebranded identity until the recent arrest. The kit was sold at approximately $500 per license to roughly 500 affiliated actors, making the TTPs broadly distributed beyond the arrested developer.

Action Checklist

1. Containment: Enforce phishing-resistant MFA (FIDO2/hardware security keys or certificate-based authentication) on all Microsoft 365 accounts, particularly privileged and finance roles.
2. Containment: Standard TOTP and push MFA do not stop AiTM attacks. Review and enforce Microsoft Entra ID Conditional Access policies requiring compliant devices and restricting legacy authentication protocols immediately.
3. Detection: Query Microsoft Entra ID sign-in logs for impossible travel events, sign-ins from unexpected IP geolocation, and token refresh activity without corresponding interactive sign-in.
4. Detection: Review Microsoft Defender for Office 365 alerts for suspicious email forwarding rules (T1114.003) and inbox rule creation by non-standard user agents.
5. Detection: Search unified audit logs for 'New-InboxRule' and 'Set-InboxRule' operations created by users who recently authenticated from anomalous locations.
6. Eradication: Audit and remove unauthorized inbox forwarding rules across all mailboxes using PowerShell (Get-InboxRule) or Microsoft Purview audit search.
7. Eradication: Revoke active sessions and force re-authentication for any account showing anomalous sign-in patterns.
8. Eradication: Rotate credentials for accounts where session token theft cannot be ruled out.
9. Recovery: Validate that phishing-resistant MFA is active and enforced via Conditional Access, not simply enabled, for all users.
10. Recovery: Confirm legacy authentication protocols (Basic Auth, SMTP AUTH where not required) are blocked.
11. Recovery: Monitor Entra ID sign-in logs for 30 days post-remediation for recurrence of anomalous token refresh patterns.
12. Post-Incident: Document gaps in MFA enforcement and Conditional Access policy coverage.
13. Post-Incident: Evaluate whether Microsoft Entra ID token protection (binding tokens to device) is configured.
14. Post-Incident: Conduct tabletop or simulation exercise against AiTM phishing scenarios.
15. Post-Incident: Review whether finance, executive, and IT admin accounts have additional controls beyond standard MFA.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to executive leadership, legal counsel, and potentially law enforcement if Unified Audit Log evidence confirms successful BEC fund transfers, if PII or financial account data was accessed via compromised M365 mailboxes (triggering breach notification obligations under GDPR, state data breach statutes, or PCI DSS Requirement 12.10), or if the IR team lacks capability to execute tenant-wide session revocation and Conditional Access enforcement within the 4-hour window required to prevent W3LL actors from monetizing a stolen session.
Recovery Notes	Before declaring recovery complete, validate via Conditional Access What-If tool in Entra ID that a test sign-in from a non-compliant device without FIDO2 authentication is blocked for all user accounts — particularly finance, executive, and IT admin roles targeted by W3LL BEC campaigns. Monitor Entra ID non-interactive sign-in logs daily for 30 days post-remediation filtering on token refresh events from IP addresses not associated with Microsoft's own services (i.e., not in Microsoft's published IP range list), as W3LL-affiliated actors may attempt to replay any tokens stolen prior to revocation that were not fully invalidated. If any new anomalous token refresh or inbox rule creation is detected during the monitoring window, treat it as a new incident rather than a residual artifact and re-initiate containment.
Forensic Artifacts	Microsoft Entra ID Non-Interactive Sign-in Logs (retained 30 days): The definitive artifact for W3LL AiTM token replay — a successful W3LL attack produces non-interactive token refresh events from data-center IP ranges (the W3LL proxy) without a corresponding interactive sign-in from the victim, because the victim authenticated against the W3LL reverse proxy rather than directly against Microsoft; export immediately as these expire and cannot be recovered. | Microsoft 365 Unified Audit Log — 'New-InboxRule' and 'Set-InboxRule' operations: W3LL-affiliated actors create inbox forwarding rules to external attacker-controlled addresses within minutes of session takeover to intercept BEC-relevant communications; the ClientInfoString field will show a non-human user agent (automation tool or headless browser) inconsistent with the victim's normal email client. | Microsoft Entra ID Risky Sign-ins and Risk Detections report: W3LL proxy infrastructure IPs are frequently listed in Microsoft's threat intelligence, causing Identity Protection to generate 'unfamiliar sign-in properties' or 'anonymous IP address' risk detections — these detections pre-date analyst awareness and establish the earliest confirmed indicator of W3LL targeting in the tenant. | Exchange Online Message Trace (Get-MessageTrace, 30-day retention): Reveals whether W3LL-created forwarding rules successfully exfiltrated BEC-relevant emails (invoice requests, wire transfer approvals, executive impersonation threads) to external addresses before detection; essential for determining BEC fraud exposure scope and regulatory breach notification obligations. | Microsoft Defender for Office 365 — Threat Explorer or Email & Collaboration audit (URL click events and delivery actions): W3LL phishing kits deliver a convincing M365 login page via URL; Threat Explorer records the original phishing URL that directed victims to the W3LL AiTM proxy, the delivery timestamp, and whether Microsoft's detonation detected the kit — this establishes the initial access vector and can be used to identify additional victims within the same tenant who clicked but whose sessions may not yet show anomalous behavior.

Per-Action IR Details

Containment — Enforce phishing-resistant MFA (FIDO2/hardware security keys or certificate-based authentication) on all Microsoft 365 accounts, particularly privileged and finance roles. Standard TOTP and push MFA do not stop AiTM attacks. Review Microsoft Entra ID Conditional Access policies to require compliant devices and restrict legacy authentication protocols immediately.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: Short-term containment to prevent ongoing session token harvesting by W3LL AiTM infrastructure; long-term containment via policy enforcement to eliminate the MFA bypass

vector W3LL kits exploited against M365 TOTP and push-based MFA.

Controls: NIST IR-4 (Incident Handling) — execute containment as part of the incident handling capability, NIST AC-17 (Remote Access) — enforce managed, policy-compliant remote access to M365 via Conditional Access requiring compliant devices, NIST IA-5 (Authenticator Management) — replace TOTP/push authenticators with phishing-resistant FIDO2 credentials that cannot be intercepted by a W3LL reverse proxy, NIST SC-8 (Transmission Confidentiality and Integrity) — block legacy authentication protocols (Basic Auth, SMTP AUTH) that bypass modern auth controls and are a known W3LL initial-access vector, CIS 6.3 (Require MFA for Externally-Exposed Applications) — enforce MFA on all externally exposed M365 services; upgrade to phishing-resistant methods immediately, CIS 6.5 (Require MFA for Administrative Access) — apply FIDO2 or certificate-based MFA to all M365 admin and privileged roles without exception

Compensating: For teams without Entra ID P2 licensing: use Microsoft Entra ID free-tier Security Defaults to block legacy auth universally, then use the free Microsoft Authenticator passwordless phone sign-in (not push MFA) as a stepping stone. Run the following PowerShell to audit which Conditional Access policies currently permit legacy auth: Connect-MgGraph; Get-MgIdentityConditionalAccessPolicy | Where-Object {$_.Conditions.ClientAppTypes -contains 'exchangeActiveSync' -or $_.Conditions.ClientAppTypes -contains 'other'} | Select DisplayName, State. For finance and exec accounts with no FIDO2 hardware available, enforce named-location Conditional Access restricting sign-in to corporate IP ranges as an interim block against W3LL proxy infrastructure originating from offshore IPs.

Evidence: Before changing any Conditional Access policies, export the current policy state and sign-in log baseline: (1) Microsoft Entra ID Sign-in Logs — export all interactive and non-interactive sign-ins from the 30 days prior to discovery, filtered on 'Authentication Method' to identify which accounts are still using TOTP or push MFA and are therefore retroactively exposed to W3LL AiTM token theft. (2) Entra ID Audit Logs — capture all Conditional Access policy create/modify/delete events to establish whether an attacker with M365 admin access (post-compromise) tampered with policies to re-enable legacy auth. (3) Microsoft 365 Unified Audit Log — export 'UserLoggedIn' operations with 'ResultStatus: Success' where 'AuthenticationMethod' does not include FIDO2 or certificate, as these represent sessions that could have been hijacked by W3LL's reverse proxy intercepting the session cookie post-MFA.

Detection — Query Microsoft Entra ID sign-in logs for impossible travel events, sign-ins from unexpected IP geolocation, and token refresh activity without a corresponding interactive sign-in. Review Microsoft Defender for Office 365 alerts for suspicious email forwarding rules (T1114.003) and inbox rule creation by non-standard user agents. Search unified audit logs for 'New-InboxRule' and 'Set-InboxRule' operations created by users who recently authenticated from anomalous locations.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Correlate Entra ID non-interactive token refresh events — the behavioral signature of a W3LL-stolen session cookie being replayed — against interactive sign-in absence, impossible travel, and downstream mailbox rule creation to confirm AiTM compromise rather than benign anomaly.

Controls: NIST IR-5 (Incident Monitoring) — track and document each anomalous sign-in and inbox rule event as a discrete incident indicator, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — systematically review Entra ID and M365 unified audit logs at increased frequency during active W3LL campaign window, NIST AU-2 (Event Logging) — verify that non-interactive sign-in logs, token refresh events, and mailbox audit logs are enabled for all M365 accounts, as these are disabled by default for some license tiers, NIST SI-4 (System Monitoring) — monitor M365 environment for indicators of W3LL post-compromise behavior including AiTM token replay and BEC-preparatory inbox rule creation, CIS 8.2 (Collect Audit Logs) — ensure M365 unified audit logging is active across the tenant; W3LL actors rely on log gaps to persist undetected, MITRE ATT&CK T1114.003 (Email Collection: Email Forwarding Rule) — detect W3LL post-compromise persistence mechanism used to intercept BEC-relevant communications after session takeover, MITRE ATT&CK T1539 (Steal Web Session Cookie) — the core W3LL AiTM mechanism; token refresh without interactive sign-in is the primary detection signal

Compensating: Without Microsoft Sentinel or a commercial SIEM: (1) Run the following PowerShell to export non-interactive sign-ins and flag token refreshes with no paired interactive sign-in — requires AzureAD or Microsoft.Graph module: Get-MgAuditLogSignIn -Filter "isInteractive eq false and tokenIssuerType eq 'AzureAD'" | Select UserPrincipalName, IPAddress, Location, CreatedDateTime, AuthenticationRequirement | Export-Csv noninteractive_signins.csv. Cross-reference that CSV against Get-MgAuditLogSignIn -Filter "isInteractive eq true" to identify UPNs present only in non-interactive logs — these are the W3LL session-replay candidates. (2) For inbox rule

hunting without Defender for Office 365 Plan 2, use the Unified Audit Log via PowerShell: Search-UnifiedAuditLog -StartDate (Get-Date).AddDays(-30) -EndDate (Get-Date) -Operations 'New-InboxRule','Set-InboxRule' -ResultSize 5000 | ConvertFrom-Json | Where-Object {$_.Parameters -match 'ForwardTo|RedirectTo|DeleteMessage'} | Export-Csv inboxrules_audit.csv. (3) Apply the free Sigma rule 'microsoft_365_inbox_forwarding_rule_enabled' (SigmaHQ community rules) against exported UAL data using sigma-cli with the csv backend.

Evidence: Preserve the following before any remediation that would overwrite or expire evidence: (1) Microsoft Entra ID Non-Interactive Sign-in Logs — these contain the token refresh events generated when W3LL's infrastructure replays the stolen M365 session cookie; logs are retained only 30 days in Entra ID and will be lost without export. (2) Microsoft 365 Unified Audit Log entries for 'New-InboxRule' and 'Set-InboxRule' — W3LL-affiliated actors create forwarding rules to BEC-external addresses immediately after session takeover; the 'ClientInfoString' field will show the user agent used (often anomalous or automation-based). (3) Entra ID Risky Sign-ins report (Identity Protection) — if licensed, export all 'high risk' and 'medium risk' sign-in events; W3LL proxy IPs frequently appear in Microsoft's threat intelligence feed and trigger these alerts. (4) Microsoft Defender for Office 365 'Email & Collaboration' audit — capture any phishing simulation bypass events or ZAP (Zero-hour Auto Purge) actions that indicate W3LL-kit emails reached inboxes before detection. (5) Browser or email client user-agent strings from Entra ID sign-in logs — W3LL kits authenticate using the stolen cookie server-side, resulting in sign-ins from data-center IP ranges with headless browser or atypical user-agent strings that differ from the victim's legitimate client.

Eradication — Audit and remove unauthorized inbox forwarding rules across all mailboxes using PowerShell (Get-InboxRule) or Microsoft Purview audit search. Revoke active sessions and force re-authentication for any account that shows anomalous sign-in patterns. Rotate credentials for accounts where session token theft cannot be ruled out.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: Remove all W3LL-established persistence mechanisms — stolen session tokens and inbox forwarding rules — from the M365 tenant before recovery; failure to revoke tokens first allows W3LL-affiliated actors to re-establish forwarding rules even after password reset, because the cookie remains valid.

Controls: NIST IR-4 (Incident Handling) — execute eradication as part of the structured incident handling process, documented per IR-5, NIST AC-2 (Account Management) — disable or reset accounts where W3LL session token theft is confirmed or cannot be ruled out; revoke all active sessions, NIST IA-5 (Authenticator Management) — rotate credentials and re-enroll authenticators for compromised accounts, specifically replacing any TOTP/push MFA enrollment that was active during the W3LL AiTM attack window, NIST SI-2 (Flaw Remediation) — remove the unauthorized inbox rules that W3LL actors use to silently redirect BEC-target communications, CIS 5.3 (Disable Dormant Accounts) — review whether any compromised accounts are candidates for suspension pending full forensic review, CIS 6.2 (Establish an Access Revoking Process) — execute the access revocation process for all confirmed or suspected W3LL-compromised sessions and credentials, MITRE ATT&CK T1114.003 (Email Collection: Email Forwarding Rule) — eradicate W3LL persistence by removing all forwarding rules to external domains created during or after the anomalous sign-in window

Compensating: Without Microsoft Purview or Defender for Office 365 Plan 2 for bulk rule auditing: (1) Run across all mailboxes using Exchange Online PowerShell — requires ExchangeOnlineManagement module: Get-Mailbox -ResultSize Unlimited | ForEach-Object { Get-InboxRule -Mailbox $_.UserPrincipalName } | Where-Object { $_.ForwardTo -ne $null -or $_.RedirectTo -ne $null -or $_.DeleteMessage -eq $true } | Select MailboxOwnerID, Name, ForwardTo, RedirectTo, DeleteMessage | Export-Csv suspicious_inboxrules.csv. Review the CSV, then remove confirmed malicious rules with: Remove-InboxRule -Mailbox 'victim@domain.com' -Identity 'RuleName'. (2) Revoke all active M365 sessions for suspected accounts using: Revoke-MgUserSignInSession -UserId 'victim@domain.com' — this invalidates all current refresh tokens, forcing W3LL's infrastructure to lose the replayed session. (3) After revocation, immediately enforce a password reset via Set-MgUserPassword or the M365 admin portal so that even if a token was cached outside Microsoft's revocation scope, the credential is invalid. (4) Document each rule removed and each session revoked with timestamps for the incident record per NIST IR-5 (Incident Monitoring).

Evidence: Before revoking sessions or removing rules, snapshot the following: (1) Full output of Get-InboxRule for each affected mailbox including RuleIdentity, ForwardTo, RedirectTo, ForwardAsAttachmentTo, and CreationTime — this establishes exactly when W3LL actors created the rule relative to the anomalous sign-in, confirming the attack

chain. (2) Microsoft 365 Message Trace (Get-MessageTrace) for the 30 days prior — identify whether any emails matching BEC-typical subjects (wire transfer, invoice, payment) were silently forwarded to external addresses by the W3LL-created rules before detection. (3) Entra ID sign-in log for the specific compromised UPN showing the non-interactive token refresh chain — export before revocation because revocation may clear the active session state visible in the portal. (4) Screenshot or export of Entra ID 'Active Sessions' for affected accounts before Revoke-MgUserSignInSession is executed, preserving the session metadata (IP, device, start time) for forensic record.

Recovery — Validate that phishing-resistant MFA is active and enforced via Conditional Access — not simply enabled — for all users. Confirm legacy authentication protocols (Basic Auth, SMTP AUTH where not required) are blocked. Monitor Entra ID sign-in logs for 30 days post-remediation for recurrence of anomalous token refresh patterns.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: Restore M365 to a verified secure state by confirming that Conditional Access enforcement — not just MFA enablement — closes the W3LL AiTM bypass path; monitor for 30 days because W3LL-affiliated actors are known to reattempt against the same targets after initial disruption.

Controls: NIST IR-4 (Incident Handling) — execute recovery as part of the incident handling plan with documented validation steps, NIST CA-7 (Continuous Monitoring) — implement ongoing monitoring of Entra ID sign-in logs post-recovery to detect W3LL re-targeting or residual stolen tokens not captured during eradication, NIST SC-8 (Transmission Confidentiality and Integrity) — verify that legacy auth protocols (Basic Auth, SMTP AUTH) remain blocked after recovery operations, as these are frequently re-enabled inadvertently by service account reconfiguration, NIST SI-6 (Security and Privacy Function Verification) — verify correct operation of Conditional Access policies enforcing phishing-resistant MFA after policy changes made during containment, CIS 7.2 (Establish and Maintain a Remediation Process) — validate that all remediation steps completed during eradication are confirmed effective before declaring recovery complete, CIS 6.3 (Require MFA for Externally-Exposed Applications) — confirm enforcement, not just enablement, of phishing-resistant MFA on all externally exposed M365 services post-recovery

Compensating: Without Microsoft Sentinel for continuous monitoring: (1) Schedule a daily PowerShell task to export non-interactive sign-in anomalies for 30 days: $signins = Get-MgAuditLogSignIn -Filter "isInteractive eq false and createdDateTime gt $(Get-Date).AddDays(-1).ToString('yyyy-MM-ddTHH:mm:ssZ')" | Where-Object {$_.RiskLevelDuringSignIn -ne 'none' -or $_.IPAddress -notmatch '^(10\.|172\.(1[6-9]|2[0-9]|3[01])\.|192\.168\.)'} — pipe to a CSV and email to the security team. (2) To verify legacy auth blocking without Entra ID Workbooks: Search-UnifiedAuditLog -Operations 'UserLoggedIn' -ResultSize 5000 | Where-Object {$_.ClientInfoString -match 'BasicAuth|SMTP|IMAP|POP'} — any results indicate legacy auth is still active. (3) Use the free Microsoft tool 'Entra ID Sign-in Diagnostic' (available in the portal at no additional license cost) to spot-check specific accounts flagged during detection for ongoing anomalies.

Evidence: During the 30-day monitoring window, preserve: (1) Weekly exports of Entra ID non-interactive sign-in logs filtered to token refresh events — compare against the pre-remediation baseline to confirm the W3LL replay pattern has ceased. (2) Conditional Access policy audit log entries confirming no policy modifications occurred post-recovery (Entra ID Audit Log, category: Policy, activity: Update conditional access policy). (3) Any new 'New-InboxRule' operations in the Unified Audit Log during the monitoring window — W3LL re-compromise would likely re-establish forwarding rules as the first post-access action.

Post-Incident — Document any gaps in MFA enforcement and Conditional Access policy coverage. Evaluate whether Microsoft Entra ID token protection (binding tokens to device) is configured. Conduct tabletop or simulation exercise against AiTM phishing scenarios. Review whether finance, executive, and IT admin accounts have additional controls beyond standard MFA, given BEC fraud focus.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Conduct a lessons-learned review specifically against the W3LL AiTM attack chain to update detection playbooks, close Conditional Access coverage gaps, and validate that token protection and privileged account controls would stop a recurrence from the remaining ~500 W3LL-affiliated actors who were not arrested in the enforcement action.

Controls: NIST IR-4 (Incident Handling) — update the incident handling capability based on lessons learned from the W3LL campaign response, NIST IR-8 (Incident Response Plan) — revise the IR plan to include AiTM phishing as an explicit scenario with W3LL-specific indicators and detection queries, NIST RA-3 (Risk Assessment) — assess residual risk from W3LL-affiliated actors still active post-enforcement and from AiTM-capable kits redistributed from W3LL's platform, NIST PM-16 (Threat Awareness Program) — incorporate W3LL campaign TTPs into threat awareness training, specifically targeting finance and executive staff who are BEC fraud targets, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — update the vulnerability management process to include periodic Conditional Access policy review and MFA method coverage audits as standing controls against AiTM-capable phishing services, CIS 6.5 (Require MFA for Administrative Access) — confirm in post-incident review that IT admin accounts have phishing-resistant MFA enforced and are bound to Entra ID token protection, MITRE ATT&CK T1557 (Adversary-in-the-Middle) — incorporate AiTM detection logic into the permanent detection engineering backlog; W3LL's platform architecture is now documented and will inform successor kits

Compensating: For teams without a dedicated GRC or purple team capability: (1) Use the free CISA Tabletop Exercise Packages (CTEPs) — the BEC and phishing scenario package provides a structured 2-hour exercise template applicable to the W3LL AiTM scenario without requiring a facilitator; available at cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages. Label as a search-retrieved URL — recommend human validation before use. (2) To evaluate Entra ID token protection status without premium tooling, run: Get-MgPolicyTokenLifetimePolicy and Get-MgPolicyAuthenticationStrengthPolicy — confirm a policy exists requiring phishing-resistant authentication strength for Conditional Access assignments on privileged roles. (3) For finance and exec account additional controls with no PAM tooling budget: create a dedicated Conditional Access policy scoped to a 'High-Value Targets' Entra ID group that requires FIDO2 or certificate-based auth AND a compliant device AND a named corporate IP location — this three-factor Conditional Access condition cannot be satisfied by a W3LL AiTM proxy operating from an offshore data center.

Evidence: For the post-incident record and lessons-learned documentation, assemble: (1) The complete Entra ID Conditional Access policy state at time of incident discovery versus current state — delta analysis shows exactly which policy gaps W3LL-affiliated actors could have exploited. (2) The incident timeline mapping each confirmed or suspected victim account's anomalous sign-in to the corresponding inbox rule creation and any outbound BEC-related email activity — this establishes dwell time and the full attack chain for the after-action report. (3) MFA method enrollment report (Get-MgUserAuthenticationMethod for all users) from both before and after the incident — documents which accounts were exposed to AiTM bypass due to TOTP/push enrollment and confirms post-incident uplift to phishing-resistant methods.

Detection Guidance

Primary detection sources: Microsoft Entra ID sign-in logs and Microsoft Defender for Office 365. Key behavioral indicators: (1) Sign-in events followed immediately by token refresh with no subsequent interactive sign-in, indicative of stolen session token reuse. (2) Inbox rule creation (New-InboxRule/Set-InboxRule in unified audit log) shortly after an anomalous authentication event. (3) Sign-ins from IP addresses associated with known AiTM proxy infrastructure, cross-reference with current threat intelligence feeds. (4) Concurrent sessions from geographically separated locations within a short window (impossible travel). (5) Email forwarding rules pointing to external domains not previously seen in your environment. Microsoft Sentinel analytic rules for 'AiTM phishing' and 'suspicious inbox manipulation' cover several of these patterns natively. For environments without Sentinel, KQL queries against Entra ID SignInLogs filtering on ResultType, UserAgent anomalies, and LocationDetails provide equivalent coverage.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`Not available from provided sources`	W3LL infrastructure domains were not published in the supplied source material. Check FBI/CISA advisories and current threat intelligence feeds for confirmed W3LL-associated domains and IP ranges.	LOW

Framework Mappings

MITRE-ATTACK

- **T1539** — Steal Web Session Cookie
- **T1114** — Email Collection
- **T1078** — Valid Accounts
- **T1583.006** — Web Services
- **T1586.002** — Email Accounts
- **T1583.001** — Domains
- **T1557** — Adversary-in-the-Middle
- **T1114.003** — Email Forwarding Rule
- **T1656** — Impersonation
- **T1566.002** — Spearphishing Link

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AT-2** — Literacy Training and Awareness
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **SC-13** — Cryptographic Protection

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
- **164.312(e)(1)** — Transmission Security

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information
- **A.8.24** — Use of cryptography

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1539	Steal Web Session Cookie	Credential-Access
T1114	Email Collection	Collection
T1078	Valid Accounts	Defense-Evasion
T1583.006	Web Services	Resource-Development
T1586.002	Email Accounts	Resource-Development
T1583.001	Domains	Resource-Development
T1557	Adversary-in-the-Middle	Credential-Access
T1114.003	Email Forwarding Rule	Collection
T1656	Impersonation	Defense-Evasion
T1566.002	Spearphishing Link	Initial-Access

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/04/fbi-and-indonesian-police-dismant...	T3

Source	URL	Tier
Microsoft 365 vulnerability scanning and remediation	https://learn.microsoft.com/en-us/compliance/assurance/assurance-mi...	T1
Microsoft Defender Vulnerability Management	https://learn.microsoft.com/en-us/defender-vulnerability-management...	T1
Microsoft Defender Vulnerability Management | Microsoft Security	https://www.microsoft.com/en-us/security/business/threat-protection...	T1
Microsoft 365: The Complete Guide To Vulnerability Management	https://www.youtube.com/watch?v=r69wcxlLPqM	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-04-14 06:03 UTC by TJS Security Command Center