INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-03 13:57 UTC

Living-off-the-Land Email Compromise Targets Stock Exchange Executive via Native Windows Tools

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0400
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Microsoft Windows (native tooling), unspecified email platform, global stock exchange environment
Published	2026-06-03T06:01:00
Discovery Source	Rss

Executive Summary

An unattributed threat actor maintained persistent access to a senior finance executive's email account at a global stock exchange for several months, using only native Windows tools to evade detection. The intrusion exploited weak authentication and misconfigured access controls; no custom malware or known CVE was involved. The business risk is severe: executive email at a stock exchange may contain material non-public information, creating direct exposure to insider trading liability, market manipulation, and regulatory sanction.

Technical Analysis

This campaign represents a living-off-the-land (LotL) business email compromise (BEC) targeting a senior finance executive at an unnamed global stock exchange. The threat actor used exclusively native Windows utilities, mapped to T1218 (System Binary Proxy Execution) and T1036 (Masquerading), to avoid triggering signature-based detection. Initial access is assessed via valid account abuse (T1078) and credential compromise consistent with CWE-522 (Insufficiently Protected Credentials). Sustained email access was achieved through Exchange remote mailbox access (T1114.002), email forwarding rule manipulation (T1114.003), and account manipulation including additional cloud role grants (T1098.003). Defense evasion involved disabling or modifying security tooling (T1562.001) and use of email hiding rules (T1564.008). Cookie or token reuse (T1550.001) may have enabled session persistence without repeated credential entry. No CVE has been assigned; the root weaknesses are CWE-284 (Improper Access Control), CWE-287 (Improper

Authentication), and CWE-522 (Insufficiently Protected Credentials). No patch exists because no software vulnerability was exploited; remediation is entirely configuration and control-based. Primary reporting source is Dark Reading (T3); no vendor advisory directly addresses this specific campaign. A Microsoft Tech Community post references CVE-2026-42897 affecting Exchange Server (May 2026); however, no evidence links this CVE to the observed campaign activity. Campaign success relied on configuration weakness and credential compromise, not software vulnerability exploitation.

Action Checklist

1. Step 1: Containment. Immediately audit all active email forwarding rules and delegate access grants on executive and privileged finance accounts (T1114.003, T1098.003). Revoke any unrecognized forwarding rules, external delegates, and OAuth application grants. Per NIST AC-2 (Account Management) and AC-3 (Access Enforcement), suspend suspect sessions and force re-authentication for affected accounts.
2. Step 2: Detection. Query mail audit logs for forwarding rule creation events, delegate additions, and mailbox access from unfamiliar IPs or user agents. Hunt for T1218 indicators: execution of LOLBins (e.g., mshta.exe, regsvr32.exe, certutil.exe) in process telemetry correlated with email platform access events. Enable and review Unified Audit Log (UAL) in Microsoft 365 or equivalent. Reference NIST AU-2 (Event Logging) and AU-6 (Audit Record Review). Apply behavioral analytics and LOLBin detection to process-level anomalies.
3. Step 3: Eradication. Enforce phishing-resistant MFA (FIDO2 or certificate-based) on all executive accounts per NIST IA-5 (Authenticator Management) and CIS 6.3 (Require MFA for Externally-Exposed Applications) and CIS 6.5 (Require MFA for Administrative Access). Rotate all credentials for affected accounts per NIST IA-5. Revoke and reissue any active session tokens to eliminate T1550.001 (Use Alternate Authentication Material, Application Access Token) persistence. Apply credential hardening controls across privileged mail-enabled accounts.
4. Step 4: Recovery. Validate that no unauthorized forwarding rules, inbox rules, or delegate permissions remain on targeted accounts. Confirm MFA enrollment is complete and legacy authentication protocols (Basic Auth, SMTP AUTH where not required) are disabled per NIST AC-17 (Remote Access) and AC-20 (Use of External Systems). Monitor mailbox access logs for 30 days post-remediation for anomalous access patterns. Require MFA verification gates before restoring full executive account access.
5. Step 5: Post-Incident. Conduct a privileged access review against NIST AC-6 (Least Privilege) and AC-5 (Separation of Duties) to confirm executive mail accounts are not over-provisioned. Implement behavioral analytics to detect LotL activity (LOLBin execution chains) per NIST SI-4 (System Monitoring) and CIS 8.2 (Collect Audit Logs). Establish a mailbox rule change alerting policy. Review whether CIS 1.1 (Enterprise Asset Inventory) and CIS 5.1 (Account Inventory) are current; LotL campaigns exploit gaps in asset and account visibility.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate immediately to legal counsel and compliance if UAL analysis confirms the threat actor accessed the executive mailbox during any period when material non-public information (MNPI) was present — such as pre-announcement earnings data, M&A discussions, or regulatory filings — as this creates direct SEC Rule 10b-5 insider trading liability and may trigger mandatory breach notification obligations under applicable financial sector regulations.
Recovery Notes	Before restoring the executive account to full operational status, require in-person (or video-verified) FIDO2 hardware key enrollment with IT — do not allow self-service re-enrollment, as the threat actor may have registered attacker-controlled authenticator devices under T1098.005 that survive credential rotation. Monitor the executive mailbox UAL daily for a minimum of 30 days post-remediation, specifically watching for `MailboxLogin` events with legacy `ClientAppUsed` values or `ClientIPAddress` entries outside the executive's verified locations, as BEC actors frequently attempt re-entry after remediation using previously harvested session artifacts. Given the stock exchange context, retain all forensic artifacts under legal hold and coordinate with compliance on whether regulatory disclosure to the SEC or relevant exchange authority is required before the 30-day monitoring window closes.
Forensic Artifacts	M365 Unified Audit Log (UAL) — Operations: New-InboxRule, Set-InboxRule, Add-MailboxPermission, Add-RecipientPermission, MailboxLogin — these are the exact UAL write operations produced by T1114.003 email forwarding configuration and T1098.003 delegate access grants; export the full 90-day (or 180-day if licensed) window before any remediation actions alter the audit trail | Azure AD Sign-In Logs — filter on ClientAppUsed values of IMAP4, POP3, SMTP, and 'Other clients' combined with riskDetail and authenticationMethodsUsed fields — legacy auth sign-ins without MFA in the authenticationMethodsUsed field confirm the weak authentication initial access vector specific to this campaign | Sysmon Event ID 1 (Process Creation) logs from the executive's Windows endpoint — filter on Image paths matching mshta.exe, regsvr32.exe, certutil.exe, wscript.exe, cscript.exe with ParentImage values of outlook.exe, msedge.exe, or chrome.exe — a mail client spawning a LOLBin is the host-based signature of T1218 activity in a LotL campaign with no custom malware | Windows Security Event Log Event ID 4688 (Process Creation with command-line auditing enabled) — filter on certutil.exe invocations containing -urlcache, -decode, or -f flags, and regsvr32.exe invocations with /s /u /i flags pointing to remote URLs — these are the specific command-line patterns that distinguish malicious LOLBin use from legitimate administrative activity in this attack class | Azure AD Registered Authentication Methods snapshot (Get-MgUserAuthenticationMethod output) and OAuth2 Permission Grants (Get-MgUserOauth2PermissionGrant output) for the affected executive account — attacker-registered authenticator apps or phone numbers (T1098.005) and persisted OAuth application tokens scoped to Mail.Read or Mail.ReadWrite (T1550.001) are the persistence mechanisms specific to this BEC campaign and will survive password reset if not explicitly audited and revoked

Per-Action IR Details

Step 1: Containment — Immediately audit all active email forwarding rules and delegate access grants on executive and privileged finance accounts (T1114.003, T1098.003). Revoke any unrecognized forwarding rules, external delegates, and OAuth application grants. Per NIST AC-2 (Account Management) and AC-3 (Access Enforcement), suspend suspect sessions and force re-authentication for affected accounts.

NIST Phase: Containment

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

Controls: NIST AC-2 (Account Management), NIST AC-3 (Access Enforcement), NIST AC-12 (Session Termination), CIS 6.2 (Establish an Access Revoking Process), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

Compensating: Without an enterprise CASB or M365 Compliance Center, use the Exchange Online PowerShell module (free) to enumerate all forwarding rules: `Get-Mailbox -ResultSize Unlimited | Get-InboxRule | Where-Object {$_.ForwardTo -ne $null -or $_.RedirectTo -ne $null} | Select-Object MailboxOwnerID, Name, ForwardTo, RedirectTo`. Export results to CSV and diff against a known-good baseline. For OAuth grants, run `Get-MgUserOauth2PermissionGrant` via the free Microsoft Graph PowerShell SDK. A 2-person team can complete the executive account sweep in under two hours using these commands before SIEM tooling is available.

Evidence: Before revoking any rules, export and preserve: (1) the full output of `Get-InboxRule` for all targeted mailboxes, capturing rule name, creation timestamp, ForwardTo/RedirectTo addresses, and the identity of the account that created each rule; (2) M365 Unified Audit Log entries filtered for operation types `New-InboxRule`, `Set-InboxRule`, `Add-MailboxPermission`, and `Add-RecipientPermission` within the suspected compromise window — these are the exact UAL operations written when T1114.003 forwarding and T1098.003 delegate access are configured; (3) Azure AD sign-in logs for the affected executive accounts, specifically entries with `clientAppUsed` values of `IMAP4`, `POP3`, or `SMTP` (legacy auth indicators) and any sign-ins from IP ranges not matching the organization's known egress or the executive's travel history; (4) OAuth application consent grants from the M365 Entra ID portal showing third-party app permissions scoped to `Mail.Read` or `Mail.ReadWrite` on the executive's mailbox.

Step 2: Detection — Query mail audit logs for forwarding rule creation events, delegate additions, and mailbox access from unfamiliar IPs or user agents. Hunt for T1218 indicators: execution of LOLBins (e.g., mshta.exe, regsvr32.exe, certutil.exe) in process telemetry correlated with email platform access events. Enable and review Unified Audit Log (UAL) in Microsoft 365 or equivalent. Reference NIST AU-2 (Event Logging) and AU-6 (Audit Record Review). Apply D3-LAM (Local Account Monitoring) and D3-SFA (System File Analysis) for process-level anomalies.

NIST Phase: Detection Analysis

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

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, use two free query surfaces in parallel: (1) For M365 UAL, run `Search-UnifiedAuditLog -StartDate -EndDate -Operations 'New-InboxRule','Set-InboxRule','Add-MailboxPermission','MailboxLogin' -ResultSize 5000 | Export-Csv` via Exchange Online PowerShell — filter results for `ClientIPAddress` values outside known corporate IP ranges and `UserAgent` strings matching non-standard mail clients or scripted access patterns (e.g., `python-requests`, `curl`). (2) For LOLBin detection on the executive's Windows endpoint, deploy Sysmon (free, Sysinternals) with the SwiftOnSecurity Sysmon config; query the resulting Windows Event Log (channel: `Microsoft-Windows-Sysmon/Operational`) for Event ID 1 (Process Create) where `ParentImage` matches `outlook.exe` or `msedge.exe` and `Image` matches `mshta.exe`, `regsvr32.exe`, `certutil.exe`, `wscript.exe`, or `cscript.exe` — a LOLBin spawned by the mail client is a high-confidence T1218 indicator in this campaign context.

Evidence: Capture before analysis concludes: (1) M365 UAL export for the full suspected compromise window (this campaign involved months of access — pull the maximum 90-day UAL window immediately, then request longer retention from Microsoft if available); (2) Azure AD Conditional Access and sign-in logs showing every authentication event for the executive account, including `riskDetail`, `riskLevelAggregated`, and `authenticationMethodsUsed` fields — absence of MFA in `authenticationMethodsUsed` confirms the weak authentication initial access vector; (3) on the executive's Windows endpoint, collect Sysmon Event ID 1 and 3 logs (Process Create and Network Connection) for any process in the `%TEMP%`, `%APPDATA%`, or `C:\Users\\Downloads` paths that made outbound connections — LotL actors using native tools often stage payloads or exfil scripts in user-writable directories; (4) Windows Security Event Log Event ID 4688 (Process Creation, with command-line auditing enabled) filtered on `certutil.exe` with `-decode`, `-urlcache`, or `-f` flags, which are the most common certutil LOLBin invocation patterns for download or decode operations in this attack class.

Step 3: Eradication — Enforce phishing-resistant MFA (FIDO2 or certificate-based) on all executive accounts per NIST IA-5 and CIS 6.3 (Require MFA for Externally-Exposed Applications) and CIS 6.5 (Require MFA for Administrative Access). Rotate all credentials for affected accounts (D3-CRO — Credential Rotation). Revoke

and reissue any active session tokens to eliminate T1550.001 (Use Alternate Authentication Material — Application Access Token) persistence. Apply D3-CH (Credential Hardening) across privileged mail-enabled accounts.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IA-5 (Authenticator Management), NIST AC-17 (Remote Access), NIST AC-2 (Account Management), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 5.2 (Use Unique Passwords)

Compensating: Without an enterprise identity platform, execute token revocation for all active M365 sessions using: `Revoke-MgUserSignInSession -UserId ` (Microsoft Graph PowerShell, free) — this invalidates all refresh tokens and forces re-authentication. Immediately follow with: `Set-MsolUser -UserPrincipalName -StrongPasswordRequired $true` to enforce complexity. For FIDO2 rollout without budget, Microsoft Entra ID free tier supports FIDO2 security keys (hardware keys such as YubiKey 5 series cost approximately $25–$50 each); prioritize executive and finance accounts for the first procurement cycle. As an interim gap-filler only, enable Microsoft Authenticator number matching (free, in-tenant setting) while FIDO2 keys are procured — this directly counters MFA fatigue, which is the most common bypass against push-based MFA in BEC campaigns.

Evidence: Before rotating credentials, preserve: (1) a snapshot of all current Azure AD registered authentication methods for the affected account (`Get-MgUserAuthenticationMethod -UserId `) — this documents whether any attacker-registered authenticator devices (phone numbers, authenticator apps) were added to the account as a persistence mechanism under T1098.005 (Account Manipulation: Device Registration); (2) the full list of active refresh tokens and their associated application IDs from Azure AD sign-in logs, specifically `appId` values — any `appId` mapping to a non-standard or unrecognized OAuth application indicates a persisted application access token (T1550.001) that credential rotation alone will not revoke; (3) the `lastPasswordChangeDateTime` attribute from Azure AD for the affected account to establish the timeline anchor for when the attacker first had valid credentials.

Step 4: Recovery — Validate that no unauthorized forwarding rules, inbox rules, or delegate permissions remain on targeted accounts. Confirm MFA enrollment is complete and legacy authentication protocols (Basic Auth, SMTP AUTH where not required) are disabled per NIST AC-17 (Remote Access) and AC-20 (Use of External Systems). Monitor mailbox access logs for 30 days post-remediation for anomalous access patterns. Apply D3-MFA (Multi-factor Authentication) verification gates before restoring full executive account access.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-17 (Remote Access), NIST AC-20 (Use of External Systems), NIST AC-7 (Unsuccessful Logon Attempts), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access)

Compensating: Block legacy authentication at the tenant level using an Azure AD Conditional Access policy (available in Entra ID free tier) that targets `Other clients` and `Exchange ActiveSync` with a `Block` grant control — this is a single policy that eliminates the SMTP AUTH and Basic Auth vectors exploited in this campaign without requiring a paid license. Validate the block is effective by querying UAL for `ClientAppUsed` values of `IMAP4`, `POP3`, `SMTP`, or `Other clients` post-policy-enforcement; any successful authentication using those client types indicates a Conditional Access gap. For the 30-day monitoring window without SIEM, schedule a daily 10-minute PowerShell task: `Search-UnifiedAuditLog -Operations 'MailboxLogin' -UserIds -StartDate (Get-Date).AddDays(-1) -EndDate (Get-Date)` and pipe output to a running CSV for human review.

Evidence: Before declaring recovery complete, produce a written attestation checklist capturing: (1) output of `Get-InboxRule` and `Get-MailboxPermission` post-remediation confirming zero unauthorized rules or delegates remain — this is your eradication verification artifact; (2) a Conditional Access policy export from Entra ID showing legacy auth block policies are in `Report-only` → `On` state (not left in report-only, which does not enforce); (3) re-run the Azure AD sign-in log query filtering `authenticationMethodsUsed` for the executive account — all successful logins post-recovery must show a phishing-resistant method (FIDO2 or CBA), not SMS or push; (4) confirm UAL retention is extended to the maximum available period (180 days with M365 E3/E5, 90 days otherwise) so the 30-day monitoring window has sufficient log depth.

Step 5: Post-Incident — Conduct a privileged access review against NIST AC-6 (Least Privilege) and AC-5 (Separation of Duties) to confirm executive mail accounts are not over-provisioned. Implement behavioral analytics to detect LotL activity (LOLBin execution chains) per NIST SI-4 (System Monitoring) and CIS 8.2 (Collect Audit Logs). Establish a mailbox rule change alerting policy. Review whether CIS 1.1 (Enterprise Asset Inventory) and CIS 5.1 (Account Inventory) are current — LotL campaigns exploit gaps in asset and account visibility.

NIST Phase: Post Incident

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

Controls: NIST AC-6 (Least Privilege), NIST AC-5 (Separation of Duties), NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For ongoing LotL behavioral detection without EDR, deploy the Sigma rule set (free, SigmaHQ GitHub repository) targeting LOLBin chains — specifically load the rules under `rules/windows/process_creation/` matching `mshta`, `certutil`, `regsvr32`, and `wscript` with suspicious parent processes; convert to Windows Event Log queries using `sigma convert -t windows-audit` and schedule them as hourly PowerShell tasks against the Sysmon log. For the mailbox rule alerting policy, create a free M365 Alert Policy in the Compliance Center (Purview) with the built-in `Email forwarding/redirect rule` activity type — this fires a native alert on any new `New-InboxRule` or `Set-InboxRule` operation that includes a `ForwardTo` or `RedirectTo` parameter, directly closing the detection gap this campaign exploited. Document the lessons-learned meeting output as a formal after-action report referencing NIST 800-61r3 §4.1 requirements and retain it as evidence of NIST IR-4 (Incident Handling) process maturity.

Evidence: Post-incident artifacts to retain for regulatory, legal, and lessons-learned purposes in a stock exchange context: (1) the complete UAL export covering the full compromise window, preserved in immutable storage — at a regulated financial institution, this constitutes potential evidence for SEC market manipulation or insider trading investigation and must be handled under legal hold protocols; (2) a timeline reconstruction document mapping each UAL event (forwarding rule creation, anomalous login, delegate grant) to calendar dates, establishing when the threat actor first had access to material non-public information (MNPI) — this timeline is the core artifact for any regulatory disclosure assessment; (3) the final access review output comparing pre-incident delegate permissions and OAuth grants against post-remediation state, signed off by the CISO or equivalent — this demonstrates due care for NIST AC-6 (Least Privilege) compliance; (4) Sysmon and Windows Security Event Log archives from the executive's endpoint covering the compromise window, preserved before any re-imaging, as LOLBin execution artifacts in these logs are the only host-based forensic evidence this campaign would leave in the absence of malware.

Detection Guidance

Focus detection on email platform audit logs and endpoint process telemetry. In Microsoft 365, query the Unified Audit Log for: operation types 'New-InboxRule', 'Set-InboxRule', 'Add-MailboxPermission', 'UpdateInboxRules', and 'MailItemsAccessed' from IP addresses outside established baselines. Flag any mailbox access by user agents inconsistent with the executive's known devices. On the endpoint, hunt for LOLBin execution (mshta.exe, certutil.exe, regsvr32.exe, wmic.exe, powershell.exe) spawned from unusual parent processes or at unusual hours; correlate with mail access timestamps (T1218, T1036). Look for disabled or modified security tooling in Windows Event Log (Event ID 7045, new service; Event ID 4719, audit policy change) consistent with T1562.001. Check for token reuse anomalies: multiple geographic access events within short windows using the same session token (T1550.001). Reference NIST AU-6 (Audit Record Review) for audit log analysis scope. Apply behavioral and file integrity monitoring to detect unauthorized modification of mail client configuration files or authentication stores consistent with CWE-522.

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1114** — Email Collection
- **T1562.001** — Disable or Modify Tools
- **T1114.002** — Remote Email Collection
- **T1098.003** — Additional Cloud Roles
- **T1218** — System Binary Proxy Execution
- **T1564.008** — Email Hiding Rules
- **T1550.001** — Application Access Token
- **T1036** — Masquerading
- **T1114.003** — Email Forwarding Rule

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-3** — Access Enforcement
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **SI-4** — System Monitoring

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control
- **A07:2021** — Identification and Authentication Failures
- **A04:2021** — Insecure Design

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **5.2** — Use Unique Passwords
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management
- **8.2** — Collect Audit Logs

SOC2-TSC

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

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(5)(ii)(D)** — Password Management

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

NIST-CSF-2

- **DE.CM-01** — Networks and network services are monitored

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1114	Email Collection	Collection
T1562.001	Disable or Modify Tools	Defense-Evasion
T1114.002	Remote Email Collection	Collection
T1098.003	Additional Cloud Roles	Persistence
T1218	System Binary Proxy Execution	Defense-Evasion
T1564.008	Email Hiding Rules	Defense-Evasion
T1550.001	Application Access Token	Defense-Evasion
T1036	Masquerading	Defense-Evasion
T1114.003	Email Forwarding Rule	Collection

Sources

Source	URL	Tier
Security News	https://www.darkreading.com/cyberattacks-data-breaches/global-stock...	T3
Addressing Exchange Server May 2026 vulnerability CVE-2026 ...	https://techcommunity.microsoft.com/blog/exchange/addressing-exchan...	T1

Source	URL	Tier
Stopping attacks against on-premises Exchange Server and ...	https://www.microsoft.com/en-us/security/blog/2025/04/09/stopping-a...	T1
Active Exploitation of Microsoft Exchange Vulnerabilities - update 4	https://www.cyber.gc.ca/en/alerts-advisories/active-exploitation-mi...	T3
Microsoft Exchange Zero-Day Under Attack, No Patch Available	https://www.darkreading.com/vulnerabilities-threats/microsoft-excha...	T3

Generated 2026-06-03 13:57 UTC by TJS Security Command Center