INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-04 19:22 UTC

Five-Month Covert Mailbox Exfiltration at Stock Exchange via LOTL and Consumer Cloud APIs

THREAT CAMPAIGN | **HIGH** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0411
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	9.5
Affected Products	Microsoft Outlook (OST/PST files), Microsoft OneDrive, Dropbox, Windows (SYSTEM-level privilege); tooling: Aspose .NET library, FRPC, Secretsdump, SharpDecryptPwd
Published	2026-06-04T05:33:57
Discovery Source	Rss

Executive Summary

An unattributed threat actor maintained covert access to a senior stock exchange executive's email account for at least five months, continuously copying inbox contents to personal cloud storage accounts on Dropbox and OneDrive. The operation used only legitimate software tools and cloud services, no exploitable vulnerability was involved, making it invisible to most perimeter and signature-based defenses. The assessed purpose is espionage: the actor sought sensitive communications, and the dwell time indicates the organization lacked sufficient visibility into mailbox access patterns and cloud egress behavior.

Technical Analysis

A covert espionage campaign targeting a stock exchange executive's Microsoft Outlook mailbox achieved a minimum five-month dwell time with no CVE exploitation. The intrusion relied entirely on living-off-the-land (LOTL) tradecraft. Credential access was achieved via Secretsdump (T1003.001, LSASS memory dumping) and SharpDecryptPwd (T1555, credentials from password stores), enabling SYSTEM-level privilege and lateral movement (T1021). Local email collection (T1114.001) used the Aspose .NET library to parse OST/PST files and package them for exfiltration. Exfiltration traversed Dropbox and OneDrive consumer APIs using curl-based HTTP calls (T1071.001, T1567.002), bypassing perimeter controls that do not inspect legitimate cloud service traffic. FRPC provided protocol tunneling (T1572) to obscure command-and-control traffic. Persistence was maintained via scheduled tasks masquerading as Adobe, Lenovo, and OneDrive processes (T1053.005, T1036.004). Obfuscation techniques (T1027) reduced static detection fidelity. No patch is applicable, the attack surface is behavioral and architectural. Relevant weaknesses: CWE-284 (improper access control on mailbox),

CWE-778 (insufficient logging enabling five-month dwell), CWE-522 (insufficiently protected credentials enabling initial credential dumping). Assessment source: Symantec and Carbon Black Threat Hunter Team, reported via The Hacker News (T3 source, human validation of original vendor reports recommended).

Action Checklist

1. Step 1: Containment, Audit active Outlook mailbox delegate permissions and application access tokens for all executive and privileged accounts immediately. Revoke any OAuth tokens granted to personal Dropbox or OneDrive consumer applications from corporate endpoints. Block or alert on outbound API calls to consumer Dropbox (api.dropboxapi.com) and personal OneDrive (onedrive.live.com) endpoints at the proxy or firewall layer. Isolate any endpoint where Aspose .NET components, FRPC binaries, Secretsdump, or SharpDecryptPwd artifacts are detected. Reference: NIST AC-2 (account management), NIST AC-3 (access control), NIST SI-3 (malicious code protection at system entry/exit points).
2. Step 2: Detection, Query endpoint telemetry for presence of FRPC, Secretsdump, SharpDecryptPwd, and Aspose .NET wrapper binaries. Audit Windows scheduled tasks for entries masquerading as Adobe, Lenovo, or OneDrive, inspect task names, executable paths, and creation timestamps. Review Microsoft 365 Unified Audit Log and Exchange mailbox audit logs for OST/PST file access patterns, delegated mailbox access, and high-volume mail read events against executive accounts. Alert on curl or PowerShell processes making outbound HTTPS connections to Dropbox or OneDrive consumer API endpoints. Check for SYSTEM-level process trees spawning mail-parsing or archiving activity. Reference: NIST AU-2 (event logging), NIST AU-6 (audit record review and analysis), NIST SI-4 (system monitoring), CIS 8.2 (collect audit logs). D3FEND: System File Analysis (SFA), Local Account Monitoring (LAM), System Init Config Analysis (SICA).
3. Step 3: Eradication, Remove all identified LOTL tooling (FRPC, Secretsdump, SharpDecryptPwd, Aspose wrapper) from affected endpoints. Delete masquerading scheduled tasks and restore legitimate task configurations. Rotate all credentials on affected systems, prioritize service accounts and any account that authenticated to the targeted executive mailbox. Force re-authentication and token revocation across Microsoft 365 and any connected cloud services. Reference: NIST SI-2 (flaw remediation), NIST IR-4 (incident handling). D3FEND: Credential Rotation (CRO), Credential Hardening (CH).
4. Step 4: Recovery, Verify mailbox audit logging is enabled and capturing the full event set (MailItemsAccessed, Send, HardDelete) for all executive-tier accounts before declaring remediation complete. Confirm scheduled task inventory matches approved baselines. Monitor outbound cloud API traffic for 30 days post-remediation for recurrence. Validate SYSTEM-level process activity on previously affected endpoints. Reference: NIST IR-5 (incident monitoring), NIST AU-9 (protection of audit information), NIST AU-11 (audit record retention).
5. Step 5: Post-Incident, Conduct a formal review of mailbox audit logging gaps that permitted five-month dwell time without detection, map findings to NIST AU-2 (event logging completeness) and NIST AU-6 (review frequency). Implement cloud egress controls that inspect or restrict outbound traffic to consumer cloud storage APIs, particularly from endpoints handling sensitive communications. Establish behavioral detection rules for OST/PST file access outside normal Outlook process trees. Update incident response plan to address LOTL-specific indicators. Reference: NIST IR-8 (incident response plan), CIS 8.2 (audit log collection), CIS 7.1 (vulnerability management process). D3FEND: System File Analysis (SFA), User Account Permissions (UAP).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to executive leadership, legal counsel, and relevant financial regulators (e.g., SEC under Regulation SCI, or applicable national securities authority) if forensic analysis confirms the exfiltrated mailbox content included material non-public information (MNPI), merger/acquisition communications, or regulatory filings — stock exchange context creates mandatory breach notification and market integrity obligations that the IR team cannot assess unilaterally.
Recovery Notes	Before declaring the incident closed, verify via `Get-Mailbox | Select AuditEnabled,AuditOwner` that MailItemsAccessed, Send, and HardDelete auditing is active on all executive-tier M365 accounts, and confirm that E3/E5 licensing is applied where required for full audit log fidelity. Monitor outbound DNS resolution and HTTPS traffic to api.dropboxapi.com, onedrive.live.com, and all known FRPC relay infrastructure for a minimum of 30 days, as LOTL campaigns of this sophistication frequently maintain secondary persistence mechanisms not discovered during initial eradication. Given the five-month dwell time, treat any credential that was valid on the affected endpoint during the window as fully compromised and track rotation completion — particularly Outlook profile credentials, cached Windows credentials recoverable by SharpDecryptPwd, and any service account that authenticated to the executive mailbox via EWS or Graph API.
Forensic Artifacts	Microsoft 365 Unified Audit Log — MailItemsAccessed, FolderBind, and SyncFolderItems operations for the targeted executive mailbox covering the full five-month window: these are the primary evidence of continuous Aspose .NET EWS-based mailbox harvesting and establish the scope and cadence of exfiltration. | Windows Prefetch files at C:\Windows\Prefetch\ for FRPC.EXE, SECRETSDUMP.EXE, SHARPDECRYPTPWD.EXE, and any Aspose wrapper executable — prefetch timestamps establish first and last execution of each LOTL tool and are critical for timeline reconstruction in a campaign with no exploitable CVE. | Scheduled task XML files exported from C:\Windows\System32\Tasks\ — masquerading tasks (Adobe, Lenovo, OneDrive impersonation) contain creation author, trigger configuration, and executable path fields that define the persistence mechanism and may contain actor-controlled strings useful for attribution or hunting across other endpoints. | Sysmon Event ID 3 (Network Connection) logs showing outbound connections from FRPC.EXE or PowerShell.exe to api.dropboxapi.com and onedrive.live.com, with full process ancestry — these logs document the exfiltration channel, upload frequency, and data volume transferred to personal cloud accounts. | OST file at %LOCALAPPDATA%\Microsoft\Outlook\ — file size history (recoverable from VSS shadow copies if available) and modification timestamps document the scope of mailbox content staged locally by the Aspose .NET parsing component before upload, corroborating the M365 audit log evidence.

Per-Action IR Details

Step 1: Containment — Audit active Outlook mailbox delegate permissions and application access tokens for all executive and privileged accounts immediately. Revoke any OAuth tokens granted to personal Dropbox or OneDrive consumer applications from corporate endpoints. Block or alert on outbound API calls to consumer Dropbox (api.dropboxapi.com) and personal OneDrive (onedrive.live.com) endpoints at the proxy or firewall layer. Isolate any endpoint where Aspose .NET components, FRPC binaries, Secretsdump, or SharpDecryptPwd artifacts are detected. Reference: NIST SI-3 (malicious code protection at system entry/exit points).

NIST Phase: Containment

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

Controls: NIST AC-3 (Access Enforcement), NIST AC-4 (Information Flow Enforcement), NIST AC-17 (Remote Access), NIST AC-20 (Use Of External Systems)

Compensating: Use PowerShell with Microsoft Graph API (no license cost beyond M365 tenant access) to enumerate and revoke OAuth tokens: `Get-MgUserOauth2PermissionGrant -UserId | Where-Object { $_.ResourceId -match 'dropbox|onedrive.live' } | Remove-MgOauth2PermissionGrant`. For network blocking without a next-gen firewall, add Windows Firewall rules via GPO or a local PowerShell script to DROP outbound TCP 443 to Dropbox and personal OneDrive IP ranges (publish from Dropbox's official IP list). Deploy Sysmon Event ID 22 (DNS Query) to alert on resolution of api.dropboxapi.com and onedrive.live.com from endpoints designated as executive workstations.

Evidence: BEFORE isolating any endpoint, image or collect: (1) Windows scheduled task XML exports from `C:\Windows\System32\Tasks\` — specifically any task masquerading as Adobe, Lenovo, or OneDrive with creation timestamps in the suspected dwell window; (2) FRPC binary and configuration file (typically frpc.ini) from all user-writable and temp directories; (3) Prefetch files (`C:\Windows\Prefetch\`) for FRPC.EXE, SECRETSDUMP.EXE, SHARPDECRYPTPWD.EXE, and any Aspose wrapper executable to establish first-execution timestamps; (4) Microsoft 365 Unified Audit Log entries (MailItemsAccessed events) for the executive mailbox covering the full five-month window before any token revocation — token revocation will not retroactively remove log entries but confirms scope; (5) Current Windows Security Event Log for Event ID 4648 (explicit credential use) and 4672 (special privilege logon at SYSTEM level) on the affected endpoint.

Step 2: Detection — Query endpoint telemetry for presence of FRPC, Secretsdump, SharpDecryptPwd, and Aspose .NET wrapper binaries. Audit Windows scheduled tasks for entries masquerading as Adobe, Lenovo, or OneDrive — inspect task names, executable paths, and creation timestamps. Review Microsoft 365 Unified Audit Log and Exchange mailbox audit logs for OST/PST file access patterns, delegated mailbox access, and high-volume mail read events against executive accounts. Alert on curl or PowerShell processes making outbound HTTPS connections to Dropbox or OneDrive consumer API endpoints. Check for SYSTEM-level process trees spawning mail-parsing or archiving activity. Reference: NIST AU-2 (event logging), NIST AU-6 (audit record review and analysis), NIST SI-4 (system monitoring), CIS 8.2 (collect audit logs). D3FEND: D3-SFA (system file analysis), D3-LAM (local account monitoring).

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), CIS 8.2 (Collect Audit Logs), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Without a SIEM, run these steps manually on a two-person schedule: (1) Use `schtasks /query /fo LIST /v > tasks_export.txt` and pipe through `findstr /i 'adobe lenovo onedrive'` to surface masquerading tasks — compare creation time against known-good baselines; (2) Deploy a Sigma rule targeting Sysmon Event ID 1 (Process Create) where ParentImage matches the vulnerable service or Outlook process and CommandLine contains 'dropbox' or 'onedrive.live' — run sigma-cli against collected Sysmon EVTX exports offline; (3) Query M365 Unified Audit Log via PowerShell `Search-UnifiedAuditLog -RecordType ExchangeItem -Operations MailItemsAccessed -StartDate -EndDate -UserIds ` — export to CSV and filter for RecordCount spikes or off-hours access; (4) Use osquery `SELECT * FROM scheduled_tasks WHERE action LIKE '%frpc%' OR action LIKE '%aspose%';` for rapid binary-to-task correlation.

Evidence: Prior to tuning or alerting changes: (1) Export the complete Microsoft 365 Unified Audit Log for MailItemsAccessed, FileDownloaded, and Send operations on the executive account for the full five-month suspected dwell period — this is the primary evidence of continuous exfiltration scope; (2) Collect Sysmon Event ID 3 (Network Connection) logs filtered on destination hostnames api.dropboxapi.com and onedrive.live.com, with full process ancestry (ParentImage, ParentCommandLine) to identify the FRPC or PowerShell upload mechanism; (3) Extract Windows Event ID 4698 (Scheduled Task Created) and 4702 (Scheduled Task Updated) from the Security event log on affected endpoints — correlate creation timestamps with earliest Aspose or FRPC prefetch timestamps to establish initial access timeline; (4) Retrieve OST file metadata from `%LOCALAPPDATA%\Microsoft\Outlook\` — file modification timestamps and size delta over the dwell window corroborate continuous mailbox harvesting; (5) Pull

Exchange Online mailbox audit log entries specifically for the 'SyncFolderItems' and 'FolderBind' operations which Aspose .NET EWS-based access would generate.

Step 3: Eradication — Remove all identified LOTL tooling (FRPC, Secretsdump, SharpDecryptPwd, Aspose wrapper) from affected endpoints. Delete masquerading scheduled tasks and restore legitimate task configurations. Rotate all credentials on affected systems — prioritize service accounts and any account that authenticated to the targeted executive mailbox. Force re-authentication and token revocation across Microsoft 365 and any connected cloud services. Reference: NIST SI-2 (flaw remediation), NIST IR-4 (incident handling). D3FEND: D3-CRO (credential rotation), D3-CH (credential hardening).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), NIST IA (Identification), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: For credential rotation without an enterprise PAM tool: (1) Use `net user /domain` or `Set-ADAccountPassword` for AD accounts; for M365, use `Update-MgUserPassword` via Graph PowerShell; (2) Force immediate M365 token invalidation with `Revoke-MgUserSignInSession -UserId ` — this invalidates all refresh tokens and forces reauthentication within hours; (3) Enumerate and delete FRPC persistence using `schtasks /delete /tn '' /f` and verify removal with a follow-up `schtasks /query`; (4) For SharpDecryptPwd artifacts, check `%APPDATA%`, `%TEMP%`, and `C:\ProgramData\` directories and delete — use `icacls` to verify no ACL modifications were left behind; (5) Run `reg query HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks` to confirm no orphaned task registry keys remain after scheduled task deletion.

Evidence: Before deleting any artifact: (1) Hash (SHA-256) and quarantine copies of FRPC binary, frpc.ini configuration file, Aspose wrapper DLLs, Secretsdump output files (typically NTDS.dit extracts or SAM hashes in local directories), and SharpDecryptPwd executables — these are chain-of-custody evidence for attribution and legal hold; (2) Export the full scheduled task XML for each masquerading task (`Export-ScheduledTask -TaskName "`) before deletion — the XML contains creation metadata, author fields, and trigger configurations that may identify the actor's operational pattern; (3) Collect Windows Security Event ID 4624 (successful logon) and 4648 (explicit credential logon) logs covering the dwell period to document which accounts were accessed under SYSTEM context from the exfiltration process tree; (4) Preserve a memory image (via WinPmem or equivalent free tool) from the affected endpoint if it has not been rebooted — FRPC and Aspose processes may have injected or hooked network stack components visible only in memory.

Step 4: Recovery — Verify mailbox audit logging is enabled and capturing the full event set (MailItemsAccessed, Send, HardDelete) for all executive-tier accounts before declaring remediation complete. Confirm scheduled task inventory matches approved baselines. Monitor outbound cloud API traffic for 30 days post-remediation for recurrence. Validate SYSTEM-level process activity on previously affected endpoints. Reference: NIST IR-5 (incident monitoring), NIST AU-9 (protection of audit information), NIST AU-11 (audit record retention).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-9 (Protection Of Audit Information), NIST AU-11 (Audit Record Retention), NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-4 (Audit Storage Capacity), CIS 8.2 (Collect Audit Logs), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: Without a SIEM for 30-day monitoring: (1) Schedule a daily PowerShell cron-equivalent (Task Scheduler) to run `Search-UnifiedAuditLog -Operations MailItemsAccessed,FileDownloaded -UserIds -StartDate (Get-Date).AddDays(-1)` and email results to the IR team; (2) Enable and verify mailbox auditing is on for all executive accounts: `Set-Mailbox -Identity -AuditEnabled $true -AuditOwner MailItemsAccessed,HardDelete,Send` — confirm with `Get-Mailbox -Identity | Select AuditEnabled,AuditOwner`; (3) Use a Sysmon Event ID 1 filter with a SYSTEM-context rule watching for Outlook.exe, FRPC.exe, or PowerShell.exe process creation under SYSTEM token

— forward Sysmon EVTX to a central Windows Event Collector via WEF (Windows Event Forwarding, free and native) rather than a commercial SIEM; (4) Diff current `schtasks /query /fo CSV` output weekly against the approved baseline CSV captured post-eradication to detect re-establishment of persistence.

Evidence: During the recovery monitoring window: (1) Continuously capture Sysmon Event ID 3 (Network Connection) for outbound connections to api.dropboxapi.com and onedrive.live.com — any recurrence within 30 days indicates either a second persistence mechanism was missed or the actor reestablished access via a different OAuth application; (2) Monitor OST file modification timestamps at `%LOCALAPPDATA%\Microsoft\Outlook\` on executive endpoints — unexpected size increases or modification events outside Outlook.exe process context indicate renewed harvesting; (3) Collect and retain M365 Unified Audit Logs for the full 30-day window to a tamper-evident export location (encrypted, access-controlled file share or write-once S3-equivalent) to satisfy NIST AU-11 (Audit Record Retention) requirements and support any subsequent regulatory inquiry given the stock exchange context.

Step 5: Post-Incident — Conduct a formal review of mailbox audit logging gaps that permitted five-month dwell time without detection — map findings to NIST AU-2 (event logging completeness) and NIST AU-6 (review frequency). Implement cloud egress controls that inspect or restrict outbound traffic to consumer cloud storage APIs, particularly from endpoints handling sensitive communications. Establish behavioral detection rules for OST/PST file access outside normal Outlook process trees. Update incident response plan to address LOTL-specific indicators. Reference: NIST IR-8 (incident response plan), CIS 8.2 (audit log collection), CIS 7.1 (vulnerability management process). D3FEND: D3-SFA (system file analysis), D3-UAP (user account permissions).

NIST Phase: Post Incident

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

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST IR-4 (Incident Handling), NIST AC-4 (Information Flow Enforcement), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For teams without commercial DLP or CASB tools: (1) Write a Sigma rule targeting Sysmon Event ID 1 (Process Create) where Image is NOT `C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE` and CommandLine or ParentCommandLine references `.ost` or `.pst` file paths — this catches any non-Outlook process reading mailbox data files, which is the core Aspose attack pattern; (2) Deploy a Windows Firewall GPO rule blocking outbound TCP 443 to Dropbox and personal OneDrive IP ranges on all endpoints classified as handling sensitive communications — publish the block list as a scheduled script that pulls current IP ranges from Dropbox's official published list; (3) Create a free YARA rule matching the Aspose.Email .NET library assembly GUIDs and known FRPC binary strings, then run weekly via ClamAV in offline scan mode against endpoint file systems; (4) Use `auditpol /set /subcategory:'Process Creation' /success:enable /failure:enable` plus Sysmon to ensure process creation audit coverage is not dependent on a SIEM being present — route via WEF to a dedicated log collection server.

Evidence: For the lessons-learned review: (1) Reconstruct the full attack timeline from earliest Prefetch timestamp (FRPC first execution) through last MailItemsAccessed event in the M365 Unified Audit Log — this documents the exact five-month dwell window and every log source that either fired or failed to fire; (2) Document which M365 audit log operations were disabled or not subscribed to during the dwell period — specifically whether MailItemsAccessed was enabled (it requires E3/E5 licensing and is not on by default in all configurations) — this finding directly drives the AU-2 gap remediation; (3) Retrieve proxy or firewall logs for the dwell period and reconstruct the volume and cadence of outbound HTTPS traffic to api.dropboxapi.com and onedrive.live.com — the pattern of regular, high-volume uploads during business hours from an executive endpoint is the behavioral signature this campaign would have produced, and its absence from alerting defines the detection gap to remediate.

Detection Guidance

No signature-based detection is reliable for this campaign, all tools used are legitimate or commonly available. Detection depends on behavioral telemetry. Key indicators: (1) Scheduled tasks with display names matching Adobe, Lenovo, or OneDrive but with executable paths outside expected system or program file directories,

query Windows Event ID 4698 (scheduled task creation) and 4702 (task modification). (2) LSASS memory access events from non-system processes, Windows Event ID 10 (Sysmon) or equivalent EDR telemetry targeting lsass.exe. (3) OST or PST file reads by processes other than OUTLOOK.EXE, monitor file system access telemetry on %LOCALAPPDATA% and %APPDATA%\Microsoft\Outlook paths. (4) Outbound HTTPS to api.dropboxapi.com or onedrive.live.com from endpoints where such access is not business-justified, particularly from non-browser processes (curl, PowerShell, cmd.exe). (5) FRPC binary execution, detect by process name or hash if available; look for unusual TCP tunneling behavior on non-standard ports. (6) Microsoft 365 Unified Audit Log: MailItemsAccessed operations at high volume against executive mailboxes, especially outside business hours or from unexpected IP addresses. Ensure mailbox auditing is set to E3/E5 tier logging, default audit settings may not capture MailItemsAccessed. Reference: NIST SI-4 (system monitoring), NIST AU-6 (audit record review). D3FEND: System File Analysis (SFA), Local Account Monitoring (LAM), System Init Config Analysis (SICA).

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`api.dropboxapi.com`	Consumer Dropbox API endpoint used for covert email exfiltration; flag non-browser processes connecting to this domain	HIGH
DOMAIN	`onedrive.live.com`	Personal OneDrive consumer endpoint used as secondary exfiltration channel; distinct from enterprise OneDrive (sharepoint.com) — flag from corporate endpoints	HIGH

Framework Mappings

MITRE-ATTACK

- **T1567.002** — Exfiltration to Cloud Storage
- **T1027** — Obfuscated Files or Information
- **T1572** — Protocol Tunneling
- **T1036.004** — Masquerade Task or Service
- **T1560.001** — Archive via Utility
- **T1071.001** — Web Protocols
- **T1090** — Proxy
- **T1548** — Abuse Elevation Control Mechanism
- **T1114** — Email Collection
- **T1078** — Valid Accounts
- **T1003.001** — LSASS Memory
- **T1114.001** — Local Email Collection
- **T1555** — Credentials from Password Stores

- **T1071** — Application Layer Protocol
- **T1021** — Remote Services
- **T1053.005** — Scheduled Task
- **T1567** — Exfiltration Over Web Service
- **T1003** — OS Credential Dumping
- **T1548.002** — Bypass User Account Control

NIST-800-53R5

- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **AC-6** — Least Privilege
- **CM-6** — Configuration Settings
- **AC-2** — Account Management
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **AC-17** — Remote Access
- **AC-3** — Access Enforcement
- **CM-7** — Least Functionality

OWASP-TOP10-2021

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

CIS-V8

- **5.2** — Use Unique Passwords
- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **6.3** — Require MFA for Externally-Exposed Applications
- **8.2** — Collect Audit Logs

HIPAA-SECURITY

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

SOC2-TSC

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

NIST-CSF-2

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

ISO-27001-2022

- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1567.002	Exfiltration to Cloud Storage	Exfiltration
T1027	Obfuscated Files or Information	Defense-Evasion
T1572	Protocol Tunneling	Command-And-Control
T1036.004	Masquerade Task or Service	Defense-Evasion
T1560.001	Archive via Utility	Collection
T1071.001	Web Protocols	Command-And-Control
T1090	Proxy	Command-And-Control
T1548	Abuse Elevation Control Mechanism	Privilege-Escalation
T1114	Email Collection	Collection
T1078	Valid Accounts	Defense-Evasion
T1003.001	LSASS Memory	Credential-Access
T1114.001	Local Email Collection	Collection
T1555	Credentials from Password Stores	Credential-Access
T1071	Application Layer Protocol	Command-And-Control
T1021	Remote Services	Lateral-Movement
T1053.005	Scheduled Task	Execution
T1567	Exfiltration Over Web Service	Exfiltration
T1003	OS Credential Dumping	Credential-Access
T1548.002	Bypass User Account Control	Privilege-Escalation

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/06/hackers-spied-on-stock-exchange.html	T3
Repair Outlook Data Files (.pst and .ost)	https://support.microsoft.com/en-us/office/repair-outlook-data-file...	T1
Proven Methods to Prevent Outlook Data Corruption and ...	https://www.examcollection.com/blog/proven-methods-to-prevent-outlo...	T3
Microsoft Outlook CVE-2023-23397 - Elevation of Privilege ...	https://www.reddit.com/r/sysadmin/comments/11rssg1/microsoft_outloo...	T3
Microsoft patches Windows zero-day & risky Office flaws	https://securitybrief.com.au/story/microsoft-patches-windows-zero-d...	T3

Generated 2026-06-04 19:22 UTC by TJS Security Command Center