INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-11 14:23 UTC

APT32 Turns Inward: OceanLotus Uses Supply Chain and Long-Haul Espionage to Target Vietnam's Own Financial and Infrastructure Sectors

THREAT CAMPAIGN | **HIGH** | CVSS 5.0

SCC Item ID	SCC-CAM-2026-0442
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	5.0
Affected Products	FireAnt Metakit (stock investor software platform, Vietnam, update mechanism); Microsoft SQL Server (suspected initial access vector); OneDrive.Sync.Service.exe (process injection target)
Published	2026-06-11T05:45:58
Discovery Source	Rss

Executive Summary

APT32 (OceanLotus), a threat actor assessed with medium-high confidence as Vietnam state-directed, conducted two overlapping espionage campaigns between mid-2024 and March 2026 targeting domestic Vietnamese financial and infrastructure organizations. The first campaign compromised the FireAnt Metakit stock investor platform's update mechanism to deliver the SPECTRALVIPER backdoor; the second maintained undetected access inside a Vietnamese transport construction firm for over a year. The campaigns signal a documented strategic shift by APT32 toward insider surveillance of Vietnam's own financial sector and critical infrastructure, elevating risk for any organization operating in or connected to those sectors.

Technical Analysis

APT32/OceanLotus executed two overlapping campaigns exploiting complementary weaknesses. Campaign 1: The FireAnt Metakit software update mechanism lacked code signing (CWE-494: Download of Code Without Integrity Check; CWE-345: Insufficient Verification of Data Authenticity), enabling selective delivery of the SPECTRALVIPER backdoor to stock investors via a tampered supply chain update channel (MITRE T1195.002: Compromise Software Supply Chain). Campaign 2: Initial access to a Vietnamese transport construction firm is

suspected via Microsoft SQL Server exploitation (T1190: Exploit Public-Facing Application), though the specific vulnerability has not been publicly identified and no CVE has been assigned. Both campaigns share a common post-exploitation pattern: DLL side-loading (CWE-427: Uncontrolled Search Path Element; T1574.002: DLL Side-Loading) and process injection into OneDrive.Sync.Service.exe (T1055: Process Injection) for defense evasion and persistence. Additional observed TTPs include C2 via application-layer protocols (T1071, T1071.001), local data collection (T1005), file and directory discovery (T1083), data archiving (T1560), obfuscation (T1027), system creation/modification for persistence (T1543), and network configuration discovery (T1016). SPECTRALVIPER attribution is supported by overlapping tooling, infrastructure, and tradecraft previously documented by ESET. No CVE identifiers have been assigned to the specific vulnerabilities exploited in either campaign. CWE references: CWE-494, CWE-345, CWE-427.

Action Checklist

1. Step 1: Containment, Organizations using FireAnt Metakit should immediately suspend the automatic software update mechanism and block the update channel at the network perimeter until integrity of the update pipeline can be verified with the vendor. Isolate any host that received a FireAnt Metakit update between mid-2024 and March 2026 for forensic review. Organizations running Microsoft SQL Server in environments connected to Vietnamese financial or infrastructure networks should restrict SQL Server's external network exposure and review service account privileges per NIST AC-6 (Least Privilege) and CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts).
2. Step 2: Detection, Hunt for the following behavioral indicators: (a) OneDrive.Sync.Service.exe spawning unexpected child processes or loading non-Microsoft DLLs from user-writable directories (T1055, T1574.002); (b) DLL side-loading activity, specifically DLLs loaded from non-standard paths alongside legitimate signed executables; (c) SPECTRALVIPER artifacts, review endpoint telemetry for unknown PE files injected into OneDrive.Sync.Service.exe. Enable and review Windows Security Event Log event IDs 4688 (process creation with command line), 7045 (new service installed), and 4657 (registry value modification) for persistence indicators (T1543). Query for outbound C2 over HTTP/HTTPS to low-reputation or newly registered domains (T1071.001). Audit SQL Server logs for anomalous authentication attempts, unusual stored procedure execution, and xp_cmdshell invocations (T1190). Apply NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs) to ensure logging is enabled and reviewed across affected systems.
3. Step 3: Eradication, Contact FireAnt Metakit's vendor to obtain a verified, integrity-checked installer and confirm the update channel has been secured with code signing. Do not reinstall from cached update packages. Remove any DLLs identified as side-loaded via forensic review. For SQL Server environments, apply all current Microsoft security updates, disable xp_cmdshell if not operationally required, and rotate all SQL Server service account credentials per NIST AC-2 (Account Management). Re-image compromised hosts where SPECTRALVIPER injection is confirmed; do not rely on antivirus removal alone given the process injection technique. Reference CIS 7.3 (Perform Automated Operating System Patch Management) and CIS 7.4 (Perform Automated Application Patch Management) for patch hygiene baseline.
4. Step 4: Recovery, Before returning affected systems to production, validate: (a) FireAnt Metakit update mechanism now enforces code-signed updates (CWE-494/CWE-345 remediated); (b) OneDrive.Sync.Service.exe process baseline is clean and no injected modules persist; (c) SQL Server service accounts have been rotated and privileges are scoped to least privilege (NIST AC-6); (d) all new DLL load events on recovered hosts are monitored for a minimum of 30 days post-recovery. Enable

enhanced process creation logging and DLL load auditing on recovered endpoints. Verify MFA is enforced on all remote access and administrative paths per CIS 6.4 (Require MFA for Remote Network Access) and CIS 6.5 (Require MFA for Administrative Access).

5. Step 5: Post-Incident, This campaign exposed three control gaps: (a) absence of software supply chain integrity controls (no enforced code signing on third-party update mechanisms, address via NIST SI-7: Software, Firmware, and Information Integrity and CIS 2.2: Ensure Authorized Software is Currently Supported); (b) insufficient process and DLL load monitoring on endpoints, enabling long-dwell-time intrusion (over one year undetected, address via NIST AU-2: Audit Events and AU-12: Audit Record Generation); (c) over-privileged service accounts enabling lateral movement post-initial access (address via NIST AC-6: Least Privilege and CIS 5.4). Initiate a supply chain risk review for all third-party software with auto-update mechanisms. Consider deploying NIST-aligned system file integrity monitoring and local account detection as ongoing detective controls.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to CIRT leadership and legal/compliance if memory forensics confirm SPECTRALVIPER injection in OneDrive.Sync.Service.exe on any host with access to financial transaction data or critical infrastructure control systems, as this constitutes an active, state-directed espionage intrusion with potential regulatory notification obligations under Vietnamese cybersecurity law (Circular 20/2017/TT-BTTTT) and warrants engagement of national CERT-VN.
Recovery Notes	Post-containment recovery must not begin until memory forensics have confirmed SPECTRALVIPER is absent from all OneDrive.Sync.Service.exe instances across the environment, as process injection leaves no on-disk artifact that antivirus will detect. Recovered hosts should be monitored via Sysmon EID 7 DLL load diffing against a clean baseline for a minimum of 30 days, with particular attention to any re-appearance of unsigned DLLs in user-writable directories loaded by Microsoft-signed host processes. Given APT32's documented capability for long-dwell re-entry and the supply chain vector remaining potentially active until FireAnt Metakit's update pipeline is independently verified, treat any new FireAnt Metakit update as untrusted until the vendor provides a signed attestation of pipeline integrity.

Forensic Artifacts	OneDrive.Sync.Service.exe process memory image (winpmem/DumpIt): primary artifact for SPECTRALVIPER — the injected PE backdoor resides entirely in memory of this process and will be destroyed on reboot; must be captured before any system shutdown or remediation action | Sysmon Event ID 7 (ImageLoad) logs filtered to OneDrive.Sync.Service.exe: will reveal the specific unsigned or mispathed DLL side-loaded by APT32 as part of T1574.002, including the full DLL path, load timestamp, and signing status | Windows Security Event Log Event ID 4688 (Process Creation) with command-line auditing enabled: captures any child processes spawned by OneDrive.Sync.Service.exe post-SPECTRALVIPER injection, documenting APT32's post-compromise execution chain | SQL Server ERRORLOG (%ProgramFiles%\Microsoft SQL Server\\MSSQL\Log\ERRORLOG) and default trace (fn_trace_gettable): documents xp_cmdshell invocations and anomalous service account authentications consistent with APT32's suspected SQL Server initial access vector | FireAnt Metakit installation directory file system timeline (%ProgramFiles% or %APPDATA% path): forensic timeline of file creation/modification events during the mid-2024 to March 2026 window will identify trojanized update packages delivered via the compromised update mechanism, including any DLLs substituted or added by APT32

Per-Action IR Details

Step 1: Containment — Organizations using FireAnt Metakit should immediately suspend the automatic software update mechanism and block the update channel at the network perimeter until integrity of the update pipeline can be verified with the vendor. Isolate any host that received a FireAnt Metakit update between mid-2024 and March 2026 for forensic review. Organizations running Microsoft SQL Server in environments connected to Vietnamese financial or infrastructure networks should restrict SQL Server's external network exposure and review service account privileges per NIST AC-6 (Least Privilege) and CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts).

NIST Phase: Containment

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

Controls: NIST AC-6 (Least Privilege), NIST AC-4 (Information Flow Enforcement), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Use Windows Firewall (netsh advfirewall) to block outbound traffic from the FireAnt Metakit update process: 'netsh advfirewall firewall add rule name="Block FireAnt Update" dir=out action=block program="". For SQL Server isolation, disable the TCP/IP protocol in SQL Server Configuration Manager and restrict port 1433/1434 via host firewall. Use PowerShell 'Get-LocalGroupMember -Group "Administrators"' on each affected host to enumerate over-privileged service accounts immediately.

Evidence: Before isolating hosts, capture: (1) full memory image from any host that received a FireAnt Metakit update between mid-2024 and March 2026 using winpmem or DumpIt — SPECTRALVIPER lives in memory via process injection into OneDrive.Sync.Service.exe and may not persist to disk; (2) prefetch files from C:\Windows\Prefetch\ for evidence of the FireAnt updater executable and any processes it spawned; (3) network flow logs or firewall logs capturing outbound connections from the FireAnt update process to confirm whether C2 callbacks occurred post-update; (4) SQL Server error log at %ProgramFiles%\Microsoft SQL Server\\MSSQL\Log\ERRORLOG for authentication anomalies and xp_cmdshell execution timestamps.

Step 2: Detection — Hunt for the following behavioral indicators: (a) OneDrive.Sync.Service.exe spawning unexpected child processes or loading non-Microsoft DLLs from user-writable directories (T1055, T1574.002); (b) DLL side-loading activity, specifically DLLs loaded from non-standard paths alongside legitimate signed executables; (c) SPECTRALVIPER artifacts — review endpoint telemetry for unknown PE files injected into OneDrive.Sync.Service.exe. Enable and review Windows Security Event Log event IDs 4688 (process creation with command line), 7045 (new service installed), and 4657 (registry value modification) for persistence indicators (T1543). Query for outbound C2 over HTTP/HTTPS to low-reputation or newly registered domains

(T1071.001). Audit SQL Server logs for anomalous authentication attempts, unusual stored procedure execution, and xp_cmdshell invocations (T1190). Apply NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs) to ensure logging is enabled and reviewed across affected systems.

NIST Phase: Detection Analysis

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

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with a configuration tuned to log Event ID 7 (ImageLoad) — this will capture every DLL loaded by OneDrive.Sync.Service.exe and flag loads from user-writable paths such as %APPDATA% or %TEMP%. Use the following PowerShell to search Sysmon logs for suspicious DLL loads by OneDrive.Sync.Service.exe: 'Get-WinEvent -LogName "Microsoft-Windows-Sysmon/Operational" | Where-Object {$_.Id -eq 7 -and $_.Message -like "*OneDrive.Sync.Service.exe*"} | Export-Csv sysmon_dll_loads.csv'. For SQL Server xp_cmdshell hunting without a SIEM, query the SQL Server default trace: 'SELECT * FROM fn_trace_gettable(CONVERT(VARCHAR(150),(SELECT TOP 1 path FROM sys.traces WHERE is_default=1)),DEFAULT) WHERE EventClass=46 AND TextData LIKE "%xp_cmdshell%"'. Apply a Sigma rule targeting Sysmon EID 1 (Process Create) where ParentImage ends in 'OneDrive.Sync.Service.exe' to detect SPECTRALVIPER's post-injection child process spawning.

Evidence: Capture before completing detection sweep: (1) Sysmon Event ID 7 (ImageLoad) logs filtered to OneDrive.Sync.Service.exe — specifically any DLL loaded from a path outside C:\Program Files\Microsoft OneDrive\ or lacking a valid Microsoft Authenticode signature; (2) Windows Security Event Log Event ID 4688 entries where the creator process is OneDrive.Sync.Service.exe, with full command-line auditing enabled (confirm via 'auditpol /get /subcategory:"Process Creation"'); (3) SQL Server ERRORLOG and SQL Audit logs for xp_cmdshell invocations and logins from service accounts at unusual hours; (4) Autoruns output (Sysinternals) from affected hosts capturing all persistence locations — HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, scheduled tasks, and services — to identify T1543 persistence artifacts dropped by APT32 post-SPECTRALVIPER injection.

Step 3: Eradication — Contact FireAnt Metakit's vendor to obtain a verified, integrity-checked installer and confirm the update channel has been secured with code signing. Do not reinstall from cached update packages. Remove any DLLs identified as side-loaded via forensic review. For SQL Server environments, apply all current Microsoft security updates, disable xp_cmdshell if not operationally required, and rotate all SQL Server service account credentials per NIST CM controls and D3-CRO (Credential Rotation). Re-image compromised hosts where SPECTRALVIPER injection is confirmed; do not rely on antivirus removal alone given the process injection technique. Reference CIS 7.3 (Perform Automated Operating System Patch Management) and CIS 7.4 (Perform Automated Application Patch Management) for patch hygiene baseline.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-6 (Least Privilege), NIST AC-2 (Account Management), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 5.2 (Use Unique Passwords)

Compensating: Verify FireAnt Metakit installer integrity by computing SHA-256 of the vendor-provided binary and comparing against the vendor's published hash: 'certutil -hashfile SHA256'. For side-loaded DLL removal, use Sysinternals Sigcheck to enumerate all unsigned DLLs in the FireAnt Metakit installation directory: 'sigcheck -u -e C:\\'. Disable xp_cmdshell on SQL Server with: 'EXEC sp_configure "xp_cmdshell", 0; RECONFIGURE;'. Rotate SQL Server service account passwords using a randomly generated 25+ character credential stored in a local password manager (KeePass) and update the service logon via 'services.msc' — do not reuse any credential present during the compromise window.

Evidence: Before re-imaging, preserve: (1) a full forensic disk image of each confirmed SPECTRALVIPER-injected host using FTK Imager or dc3dd — SPECTRALVIPER's injected PE payload within OneDrive.Sync.Service.exe process memory is the primary artifact and will be destroyed on shutdown; (2) export the full list of DLLs loaded by

OneDrive.Sync.Service.exe at time of imaging via a live memory acquisition (Volatility 'dlllist' plugin targeting the OneDrive.Sync.Service.exe process); (3) collect all files in %TEMP%, %APPDATA%\Microsoft\, and the FireAnt Metakit installation directory that were created or modified during the compromise window (mid-2024 to March 2026) using 'forfiles /p /s /d +2024-06-01 /c "cmd /c echo @path @fdate @ftime"'; (4) copy SQL Server ERRORLOG and Windows Application Event Log before credential rotation destroys audit trail linkage.

Step 4: Recovery — Before returning affected systems to production, validate: (a) FireAnt Metakit update mechanism now enforces code-signed updates (CWE-494/CWE-345 remediated); (b) OneDrive.Sync.Service.exe process baseline is clean and no injected modules persist; (c) SQL Server service accounts have been rotated and privileges are scoped to least privilege (NIST AC-6); (d) all new DLL load events on recovered hosts are monitored for a minimum of 30 days post-recovery. Enable enhanced process creation logging and DLL load auditing on recovered endpoints. Verify MFA is enforced on all remote access and administrative paths per CIS 6.4 (Require MFA for Remote Network Access) and CIS 6.5 (Require MFA for Administrative Access).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-6 (Least Privilege), NIST AC-17 (Remote Access), NIST AU-2 (Event Logging), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access)

Compensating: Establish a clean OneDrive.Sync.Service.exe DLL baseline on the first recovered host using Sysinternals ListDLLs: 'listdlls.exe OneDrive.Sync.Service.exe > baseline_dlls.txt' — diff against this baseline weekly on all recovered hosts using a scheduled PowerShell task. For 30-day post-recovery DLL load monitoring without EDR, configure Sysmon EID 7 to write to a dedicated log file and run a nightly PowerShell diff against the captured baseline. For MFA enforcement on a zero-budget team, enable Windows Hello for Business or deploy Duo Security's free tier on VPN and RDP gateway entry points.

Evidence: Before returning any host to production, document and retain: (1) Sysmon EID 7 baseline export showing all DLLs loaded by OneDrive.Sync.Service.exe on the clean re-imaged system — this becomes the integrity reference for 30-day monitoring; (2) output of 'sigcheck -tv' (Sysinternals) against the recovered FireAnt Metakit installation directory confirming all executables and DLLs carry valid Authenticode signatures from the expected publisher; (3) SQL Server sys.server_principals query output showing current service account privilege scope post-rotation, retained as evidence of least-privilege compliance; (4) screenshot or exported policy confirming MFA enforcement on all administrative and remote access paths, timestamped at production return.

Step 5: Post-Incident — This campaign exposed three control gaps: (a) absence of software supply chain integrity controls (no enforced code signing on third-party update mechanisms — address via NIST SI-class supply chain risk management and CIS 2.2: Ensure Authorized Software is Currently Supported); (b) insufficient process and DLL load monitoring on endpoints, enabling long-dwell-time intrusion (over one year undetected — address via NIST AU-2: Event Logging and AU-12: Audit Record Generation); (c) over-privileged service accounts enabling lateral movement post-initial access (address via NIST AC-6: Least Privilege and CIS 5.4). Initiate a supply chain risk review for all third-party software with auto-update mechanisms. Consider deploying D3-SFA (System File Analysis) and D3-LAM (Local Account Monitoring) as ongoing detective controls.

NIST Phase: Post Incident

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

Controls: NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation), NIST AC-6 (Least Privilege), NIST AU-11 (Audit Record Retention), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For supply chain integrity monitoring on a zero-budget team: build a weekly scheduled task using PowerShell and certutil to hash all executables and DLLs in the installation directories of every third-party application with an auto-update mechanism, comparing against a known-good baseline stored in a write-protected share. For

ongoing DLL load monitoring mapped to the SPECTRALVIPER injection technique, write a Sigma rule targeting Sysmon EID 7 where ImageLoaded path does not begin with expected vendor paths and the process is any Microsoft-signed host process (OneDrive.Sync.Service.exe, explorer.exe, svchost.exe) — publish the rule to the team's shared Sigma repository. For local account monitoring (D3-LAM equivalent), run 'net localgroup administrators' via a daily scheduled task and diff output against the previous day, alerting on any delta.

Evidence: Retain and archive for lessons-learned and future threat hunting: (1) the full timeline of FireAnt Metakit update events reconstructed from Windows Update logs (%WINDIR%\SoftwareDistribution\ReportingEvents.log), prefetch, and Sysmon — this documents the exact delivery window for SPECTRALVIPER and supports supply chain forensic review; (2) all Sysmon EID 7 and EID 1 logs from the transport construction firm's affected hosts covering the full 12-month dwell period, to reconstruct APT32's lateral movement and persistence chain for the lessons-learned report; (3) SQL Server audit logs covering the compromise window, preserved per NIST AU-11 (Audit Record Retention) policy, as evidence of the initial access vector and any data exfiltration staging; (4) YARA rules developed during this investigation targeting SPECTRALVIPER's PE injection signature, retained in the team's threat intelligence repository for proactive hunting against future APT32 intrusions.

Detection Guidance

Primary detection focus is behavioral, given no CVE-assigned signatures exist. Key indicators: (1) Process anomalies, OneDrive.Sync.Service.exe loading DLLs from user-writable or temp directories, or spawning cmd.exe, powershell.exe, or network utilities; monitor via Sysmon Event ID 7 (ImageLoad) and Event ID 10 (ProcessAccess). (2) DLL side-loading, legitimate signed binaries loading unsigned or low-reputation DLLs from non-standard paths; cross-reference against known-good DLL load baselines (T1574.002). (3) SPECTRALVIPER behavioral pattern, in-memory payload execution with no corresponding file on disk; detect via EDR process memory scanning and anomalous module loads into OneDrive.Sync.Service.exe. (4) Persistence mechanisms, new services or scheduled tasks with non-standard names or paths (Event ID 7045, 4698); registry run key modifications (Event ID 4657) (T1543). (5) C2 traffic, periodic beaconing over HTTP/HTTPS to low-reputation domains; look for consistent jitter-based intervals, unusual user-agent strings, or HTTP POST to domains with low DNS history (T1071.001). (6) SQL Server indicators, xp_cmdshell execution, bulk data access by service accounts outside business hours, or authentication from unexpected source IPs (T1190). (7) Data staging and exfiltration precursors, archive file creation (RAR, ZIP, 7z) in temp or user directories (T1560), followed by outbound transfer activity (T1005). Apply NIST AU-6 and AU-12 to ensure all relevant log sources (endpoint, network, application) feed into centralized analysis. NIST-aligned system file integrity and local account monitoring controls are directly applicable countermeasures.

Framework Mappings

MITRE-ATTACK

- **T1071** — Application Layer Protocol
- **T1055** — Process Injection
- **T1543** — Create or Modify System Process
- **T1574.002** — DLL Side-Loading
- **T1005** — Data from Local System
- **T1083** — File and Directory Discovery
- **T1560** — Archive Collected Data
- **T1027** — Obfuscated Files or Information

- **T1195.002** — Compromise Software Supply Chain
- **T1190** — Exploit Public-Facing Application
- **T1016** — System Network Configuration Discovery
- **T1071.001** — Web Protocols

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **AC-6** — Least Privilege
- **SI-3** — Malicious Code Protection
- **CM-7** — Least Functionality
- **SA-9** — External System Services
- **SR-3** — Supply Chain Controls and Processes
- **SI-7** — Software, Firmware, and Information Integrity
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **CM-3** — Configuration Change Control
- **SR-2** — Supply Chain Risk Management Plan

OWASP-TOP10-2021

- **A08:2021** — Software and Data Integrity Failures

CIS-V8

- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **15.1** — Establish and Maintain an Inventory of Service Providers
- **8.2** — Collect Audit Logs

NIST-CSF-2

- **GV.SC-01** — Cybersecurity supply chain risk management program
- **DE.CM-01** — Networks and network services are monitored

ISO-27001-2022

- **A.5.21** — Managing information security in the ICT supply chain

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1071	Application Layer Protocol	Command-And-Control
T1055	Process Injection	Defense-Evasion
T1543	Create or Modify System Process	Persistence
T1574.002	DLL Side-Loading	Persistence
T1005	Data from Local System	Collection
T1083	File and Directory Discovery	Discovery
T1560	Archive Collected Data	Collection
T1027	Obfuscated Files or Information	Defense-Evasion
T1195.002	Compromise Software Supply Chain	Initial-Access
T1190	Exploit Public-Facing Application	Initial-Access
T1016	System Network Configuration Discovery	Discovery
T1071.001	Web Protocols	Command-And-Control

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/06/oceanlotus-hits-vietnam-investors...	T3
OceanLotus: From external espionage to domestic targeting	https://www.welivesecurity.com/en/eset-research/oceanlotus-external...	T3
Microsoft Security Response Center Blog	https://www.microsoft.com/en-us/msrc/blog	T1
Fire Ant: A Deep-Dive into Hypervisor-Level Espionage - Sygnia	https://www.sygnia.co/blog/fire-ant-a-deep-dive-into-hypervisor-lev...	T3
Vulnerabilities Index - Huntress	https://www.huntress.com/threat-library/vulnerabilities	T3

Generated 2026-06-11 14:23 UTC by TJS Security Command Center